Administration of the
Avaya G350 Media Gateway

555-245-501
Issue 3
January 2005

Copyright 2005, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

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 may 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 Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

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

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Contacts* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Contacts* link. 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.

Standards Compliance

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

Product Safety Standards

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

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment - Immunity Characteristics - Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

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.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. 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.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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 G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

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. 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.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
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-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

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

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

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

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

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

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

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

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. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

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

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

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

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

Japan

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。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

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

Contents

About this Book 17
Overview 17
Audience 17
Downloading this book and updates from the Web 17
Downloading this book 17
Related resources 18
Technical assistance 19
Within the US. 19
International 19
Trademarks. 19
Sending us comments. 20

Chapter 1: Introduction 21

Chapter 2: Configuration overview. 23
Installation and setup overview. 23
Configuration using CLI. 25
Configuration using GUI applications 25
Saving configuration changes 26
Firmware version control 26

Chapter 3: Accessing the Avaya G350 Media Gateway 27
Accessing the CLI 27
CLI Overview 28
CLI contexts 28
CLI help. 28
Accessing the CLI locally 29
Accessing CLI via local network 29
Accessing CLI with a console device 29
Accessing CLI via modem 30
Accessing CLI via a USB modem. 30
Accessing CLI via a serial modem 31
Accessing CLI via a modem connection to the S8300 31
Accessing Avaya IW. 32
Accessing GIW. 34
Accessing Avaya Communication Manager 35

Managing login permissions 36
Security overview 36
Managing users and passwords 37
Privilege level 37
Configuring usernames 37
SSH protocol support 38
SSH Configuration 39
SCP protocol support 39
RADIUS authentication 40
802.1x protocol. 41
How port based authentication works 41
Configuring 802.1x. 42
Manual re-authentication 44
Optional 802.1x commands 44
Displaying 802.1x parameters. 45
Special security features 48
Enabling and disabling recovery password 48
Enabling and disabling telnet access 48

Chapter 4: Basic device configuration 49
Defining an interface 49
Configuring the Primary Management Interface (PMI) 50
Defining the default gateway 51
Configuring the Media Gateway Controller (MGC) 51
The Media Gateway Controller (MGC) 52
Configuring the MGC list 52
Setting reset times. 54
Accessing the registered MGC 54
Monitoring the ICC or LSP 55
Viewing the status of the device 55
Version management 56
File transfer 57
Software and firmware upgrades 57
Managing the firmware banks. 57
Upgrading software and firmware 58
Managing configuration files 60
Listing the files on the Avaya G350 Media Gateway 60

Chapter 5: Configuring Ethernet ports 61
Ethernet ports on the G350 61
Configuring switch Ethernet ports 62
Switch Ethernet port commands 62
Configuring the WAN Ethernet port 63
WAN Ethernet port traffic shaping 64
Backup interfaces 64
WAN Ethernet port commands 64

Chapter 6: Configuring logging 65
Logging overview 65
Syslog server 66
Logging file. 67
Logging session 67
Filters and severity levels 68

Chapter 7: Configuring VoIP QoS 71
VoIP overview 71
Configuring RTP and RTCP 72
Configuring RTP header compression 72
Configuring QoS parameters 74
Configuring RTCP QoS parameters 75
Configuring RSVP parameters 75
Configuring Weighted Fair VoIP Queuing (WFVQ) 76

Chapter 8: Configuring the G350 for modem use 77
Configuring the USB port for modem use 77
Configuring the console port for modem use 78

Chapter 9: Configuring a WAN Interface 81
WAN overview 81
Serial interface overview 83
Frame Relay multipoint topology support 84
Initial WAN configuration 85
Configuring the Avaya MM340 E1/T1 WAN media module 85
E1/T1 default settings 88
Configuring the Avaya MM342 USP WAN media module 88
USP default settings 90

Configuring PPP 90
Configuring PPPoE 91
PPPoE overview 91
PPPoE configuration 92
Configuring frame relay 95
Verifying the WAN configuration and testing connectivity 96
Backup interfaces 97
Backup commands 99
Extended keepalive 99
Dynamic CAC 101
Frame relay encapsulation 103
Priority DLCI 103
Traffic Shaping and Marking 104
Priority queuing 105
WAN configuration example 105
PPP VoIP configuration 106
Configuration Example for Site A. 107
Configuration Example for Site B. 109

Chapter 10: Configuring PoE 111
PoE overview. 111
Introduction 111
Load detection 112
How the G350 detects a powered device. 112
Plug and Play Operation. 113
Powering devices 113
PoE configuration CLI commands 114
PoE configuration examples 114

Chapter 11: Configuring Emergency Transfer Relay (ETR). 117
ETR overview 117
Setting ETR state 117
Viewing ETR state 118

Chapter 12: Configuring SNMP. 119
SNMP configuration overview 119
SNMP versions. 120
SNMPv1. 121
SNMPv2c 121

SNMPv3. 121
Users 122
Groups 123
Views 124
Configuring SNMP traps 125
Configuring SNMP access 127
Configuring dynamic trap manager 128
SNMP configuration examples 128

Chapter 13: Configuring advanced switching 131
Configuring VLANs 131
VLAN overview. 132
VLAN tagging 133
Multi VLAN binding 134
G350 VLAN table. 134
Ingress VLAN security. 135
ICC-VLAN. 135
VLAN CLI commands 135
VLAN configuration examples 136
Configuring port redundancy 139
Port redundancy overview 139
Secondary port activation. 139
Switchback 140
Port redundancy CLI commands 140
Port redundancy configuration examples 141
Configuring port mirroring 141
Port mirroring overview 142
Port mirroring constraints 142
Port mirroring CLI commands 142
Port mirroring configuration examples 142
Configuring spanning tree 143
Spanning tree overview 143
Spanning tree protocol 143
Spanning tree per port. 144
Rapid Spanning Tree Protocol (RSTP) 144
Spanning tree CLI commands 146
Spanning tree configuration examples. 147

Port classification 149
Port classification overview. 149
Port classification CLI commands 149
Port classification configuration examples 150

Chapter 14: Configuring contact closure 151
Contact closure overview 151
Contact closure hardware configuration. 152
Contact closure software configuration 152
Showing contact closure status 153

Chapter 15: Configuring RMON monitoring 155
RMON overview 155
RMON CLI commands 156
RMON configuration examples 156

Chapter 16: Configuring the router. 159
Overview of the G350 router 160
Configuring interfaces. 160
Router interface concepts. 161
Physical router interfaces 161
Layer 2 virtual interfaces 161
Layer 2 logical interfaces 162
IP Interface configuration commands 162
Interface configuration examples. 162
Configuring the routing table 163
Overview of the routing table 163
Via-interface static route 165
Permanent static route 165
Discard route. 165
Routing table commands 166
Configuring GRE tunneling 166
GRE tunneling overview. 167
Routing packets to a GRE tunnel 168
Preventing nested tunneling in GRE tunnels 168
Optional GRE tunnel features. 171
keepalive 171
Dynamic MTU discovery. 172
Setting up a GRE tunnel. 172

Additional GRE tunnel parameters 174
GRE tunnel application example 175
Configuring DHCP and BOOTP relay 177
DHCP 177
BOOTP 177
DHCP/BOOTP relay 178
DHCP/BOOTP relay commands 178
Configuring DHCP server 179
Application — G350 as a DHCP server and router 180
DHCP server CLI configuration 181
Configuring Options 182
Configuring vendor-specific options 183
DHCP pool configuration examples 183
Configuring broadcast relay 185
Directed broadcast forwarding 186
NetBIOS rebroadcast 186
Configuring the ARP table 187
Overview of ARP 187
The ARP table 187
ARP table commands 189
Enabling proxy ARP 189
Configuring ICMP errors 190
Configuring RIP 190
RIP overview 190
RIPv1 191
RIPv2 191
Preventing routing loops in RIP 191
RIP distribution access lists 192
RIP limitations 193
RIP commands 193
Configuring OSPF 194
Overview of OSPF 194
OSPF dynamic cost 195
OSPF limitations 195
OSPF commands 196
Route redistribution 197
Export default metric 198

Configuring VRRP 198
Overview of VRRP 198
VRRP configuration example 199
VRRP commands 200
Configuring fragmentation 201
Overview of fragmentation 201
Reassembly parameters. 202
Fragmentation commands 202

Chapter 17: Configuring IPSec VPN 203
Overview of IPSec VPN 203
Configuring a site-to-site IPSec VPN 204
Overview of IPSec VPN configuration 204
Prerequisite – coordinating with the VPN peer 208
Installing the VPN license file 208
Configuring ISAKMP policies 209
Configuring transform-sets 210
Configuring ISAKMP peer information 211
Configuring crypto maps 213
Configuring crypto-lists 214
Configuring interfaces. 216
Deactivating crypto lists to modify IPSec VPN parameters. 217
IPSec VPN maintenance. 218
Displaying IPSec VPN configuration 218
Displaying IPSec VPN status 218
IPSec VPN intervention 219
IPSec VPN logging. 219
Typical installations 221
Simple VPN topology: VPN hub and spokes. 221
Configuring the simple VPN topology 222
Full or partial mesh 226
Configuring the mesh VPN topology 227
Hub-and-spoke with hub redundancy/load sharing 238
Configuring the VPN hub redundancy/load sharing topologies 239
Full solution: hub-and-spoke with VPN for data and VoIP control backup . . 245
Configuring hub-and-spoke with VPN for data and VoIP control backup . 246

Chapter 18: Configuring policy 253
Policy overview 253
Access control lists 254
QoS lists 254
Policy-based routing 255
Managing policy lists 255
Defining policy lists 256
Creating and editing a policy list 256
Defining list identification attributes 257
Default actions 257
Deleting a policy list 257
Attaching policy lists to an interface 258
Device-wide policy lists 260
Defining global rules 260
Defining rules 261
Overview of rule criteria 261
Editing and creating rules 262
Rule criteria 262
IP protocol 262
Source and destination IP address 263
Source and destination port range 264
ICMP type and code 265
TCP Establish bit (access control lists only) 265
Operation 265
Composite operations 266
Overview of composite operations 266
Pre-configured composite operations for access control lists 266
Pre-configured composite operations for QoS lists 267
Configuring composite operations 268
Composite operation example 269
DSCP table 269
Displaying and testing policy lists 270
Displaying policy lists 270
Simulating packets 272

Chapter 19: Configuring policy-based routing 273
Policy-based routing overview 273
Applications 274
Separate routing of voice and data traffic 274
Backup 275
Configuring Policy-Based Routing 276
PBR Rules 279
Overview of rule criteria 279
Modifying rules 280
Rule criteria 280
Next Hop Lists 280
Next hop list overview 281
Modifying next hop lists 281
Editing and Deleting PBR lists 282
Displaying PBR lists 282
Application example 283

Chapter 20: Setting synchronization 287
Displaying synchronization status 288

Chapter 21: FIPS 289
Overview 289
Supported algorithms 292
Non-FIPS mode of operation 293
Security level 294
Operational environment 294
Assumptions of roles 294
Assumptions concerning user behavior 296
Critical security parameters and private keys 297
Public keys 299
CSP access rights within roles and services 300
Security rules 304
Password guidelines 306
Managing the module in FIPS-compliant mode 306
Prerequisites 307

Administration procedures 307
Entering FIPS mode 307
Failure scenarios and repair actions 319
Error states. 320
Recovering from an error state 320
Considerations. 322

Appendix A: Traps and MIBs 323
G350 traps 323
G350 MIBs 331

Appendix B: Configuring the G350 using the Avaya IW 389
Preliminary screens 389
MGC configuration and upgrade 391
Upgrading an existing MGC. 395
Gateway configuration 401
Firmware configuration 404
Modem configuration 406
Telephony configuration 408
Trunk configuration 412
Adding a trunk 414
Modifying trunk parameters. 415
Modifying IP route configuration 416
Displaying trunk status 417
Removing a trunk 418
Configuring a trunk media module 419
Endpoint installation. 420
Alarm configuration 421
Password and final screens. 423

Appendix C: Configuring the G350 using the GIW 427

Index 439

About this Book

Overview

Administration of the Avaya G350 Media Gateway describes how to configure and manage the G350 Media Gateway after it is already installed. For installation instructions, see *Installation and Upgrades for the Avaya G350 Media Gateway,* 03-300394.

Audience

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

Downloading this book and updates from the Web

You can download the latest version of the *Administration of the Avaya G350 Media Gateway* from the Avaya Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might contain new product information and updates to the information in this book. You can also download these updates from the Avaya Web site.

Downloading this book

To download the latest version of this book:

1. Access the Avaya web site at http://www.avaya.com/support.
2. On the left side of the page, click **Product Documentation**.

   The system displays the Welcome to Product Documentation page.
3. On the right side of the page, type 555-245-501, and then click **Search**.

   The system displays the Product Documentation Search Results page.

4. Scroll down to find the latest issue number, and then click the book title that is to the right of the latest issue number.
5. On the next page, scroll down and click one of the following options:
   - **PDF Format** to download the book in regular PDF format
   - **ZIP Format** to download the book as a zipped PDF file

Related resources

For more information on the Avaya G350 Media Gateway and related features, see the following books:

Title	Number
Overview of the Avaya G350 Media Gateway	555-245-201
Quick Start for Hardware Installation	03-300148
Installation and Upgrades for the Avaya G350 Media Gateway	03-300394
Maintenance of the Avaya G350 Media Gateway	555-245-105
Avaya G350 Media Gateway CLI Reference	555-245-202
Avaya G350 Media Gateway Glossary	555-245-301

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya DEFINITY Helpline at 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Trademarks

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.

  Product Documentation Group

  Room B3-H13

  1300 W. 120th Ave.

  Westminster, CO 80234 USA
- E-mail, send your comments to:

  document@avaya.com
- Fax, send your comments to:

  1-303-538-1741

Mention the name and number of this book, *Administration of the Avaya G350 Media Gateway*, 555-245-501.

Chapter 1: Introduction

The Avaya G350 Media Gateway is a high-performance converged networking and telephony device. The G350 provides networking and telephony services for up to 40 endpoint stations. The G350 contains:

- an advanced router
- a high-performance switch
- a Voice over IP (VoIP) engine
- a fax and modem over IP engine
- preservation of calls in progress when switching from one server to another (applicable to all connections except ISDN BRI)
- support for contact closure
- Virtual Private Networks (VPN)
- Emergency Transfer Relay (ETR)

When you add plug-in media modules to the G350, the G350 also supports:

- Power over Ethernet (PoE) IP telephones
- DCP digital telephones
- Analog telephones and trunks
- E1/T1 trunks
- ISDN PRI trunks
- ISDN BRI trunks
- E1/T1 WAN data lines
- on board ports
- USP ports

This guide explains how to configure the Avaya G350 Media Gateway and contains the following chapters:

- Chapter 2: Configuration overview — overview of G350 configuration tasks
- Chapter 3: Accessing the Avaya G350 Media Gateway — how to access the G350 CLI and manage login permissions
- Chapter 4: Basic device configuration — how to identify the G350 to other devices, view device status, configure event logging, and manage files
- Chapter 5: Configuring Ethernet ports — how to configure Ethernet ports on the G350
- Chapter 6: Configuring logging — how to configure G350 system logging

- Chapter 7: Configuring VoIP QoS — how to configure VoIP parameters and register call controllers on the G350
- Chapter 8: Configuring the G350 for modem use — how to configure the G350 console port and USB port for modem use
- Chapter 9: Configuring a WAN Interface — how to configure an E1/T1 or USP WAN line on the G350
- Chapter 10: Configuring PoE — how to configure PoE on the G350
- Chapter 11: Configuring Emergency Transfer Relay (ETR) — how to configure ETR on the G350
- Chapter 12: Configuring SNMP — how to configure SNMP on the G350
- Chapter 13: Configuring advanced switching — how to configure advanced switching features on the G350
- Chapter 14: Configuring contact closure — how to configure contact closure on the G350
- Chapter 15: Configuring RMON monitoring — how to configure RMON monitoring of the G350
- Chapter 16: Configuring the router — how to configure advanced features of the G350 router
- Chapter 17: Configuring IPSec VPN — how to configure IPSec VPN in the G350
- Chapter 18: Configuring policy — how to configure access control and QoS policy lists on the G350
- Chapter 19: Configuring policy-based routing — how to configure policy-based routing lists on the G350
- Chapter 20: Setting synchronization — how to configure synchronization for digital trunks
- Chapter 21: FIPS — information about the G350 cryptographic module's compliance with the Federal Information Processing Standard (FIPS-140-2) for cryptographic modules and how to configure the module to work in FIPS mode
- Appendix A: Traps and MIBs — SNMP traps and MIBs on the G350
- Appendix B: Configuring the G350 using the Avaya IW — how to configure the G350 using the Avaya IW
- Appendix C: Configuring the G350 using the GIW — how to configure the G350 using the GIW

Chapter 2: Configuration overview

This chapter provides an overview of the Avaya G350 Media Gateway configuration process and contains the following sections:

- Installation and setup overview — overview of the G350 installation and setup process
- Configuration using CLI — overview of CLI, a command prompt interface for entering configuration commands
- Configuration using GUI applications — overview of GUI applications that can be used for some configuration tasks
- Saving configuration changes — instructions on how to save configuration changes
- Firmware version control — overview of firmware version control

Installation and setup overview

A new Avaya G350 Media Gateway comes with default configuration settings. There are certain items that you must configure, according to your system specifications, before using the G350. Configuration of other items depends on the specifications of your network.

A new G350 has two IP interfaces for management (SNMP, telnet). These are the console interface and the USB interface. By default, the IP address of the console interface is 10.3.0.1 with a subnet mask of 255.255.255.0. The first thing you should do when configuring a new G350 is to assign a new IP address to the console interface. To do this:

1. Use the **`interface console`** command to enter the console context.
2. Use the **`ip address`** command to define a new IP address for the console interface.

Note:

For more detailed installation instructions, including information on obtaining IP addresses, refer to *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.

The following example assigns to the console interface an IP address of 10.3.3.1 with a subnet mask of 255.255.255.0:

```
G350-001(super)# interface console
G350-001(super-if:Console)# ip address 10.3.3.1 255.255.255.0
Done!
```

If you intend to use a USB modem to connect to the G350, you should also assign a new IP address to the USB interface. By default, the IP address of the USB interface is 10.3.0.3 with a subnet mask of 255.255.255.0. To assign a new IP address to the USB interface:

1. Use the **`interface USB`** command to enter the USB context.
2. Use the **`ip address`** command to define a new IP address for the USB interface.

The following example assigns to the USB interface an IP address of 10.3.3.2 with a subnet mask of 255.255.255.0:

```
G350-001(super)# interface USB
G350-001(super-if:USB)# ip address 10.3.3.2 255.255.255.0
Done!
```

You must also make sure the G350 is properly configured for whichever methods you intend to use for accessing the G350. For information on accessing the G350, see Accessing the Avaya G350 Media Gateway on page 27.

Your next step should be to define the other interfaces required by your system specifications. See Defining an interface on page 49.

Once you have defined your interfaces, you can define a Primary Management IP address (PMI). The PMI is the IP address which the G350 uses to identify itself when communicating with other devices, particularly the Media Gateway Controller (MGC). Management data intended for the G350 is routed to the interface defined as the PMI. You can use any interface as the PMI. For instructions on how to define the PMI, see Configuring the Primary Management Interface (PMI) on page 50.

Once you have defined a PMI, you must register the G350 with an MGC. The MGC is a media server that controls telephone services on the G350. The MGC can be internal or external. See The Media Gateway Controller (MGC) on page 52.

Once you have performed these steps, the G350 is ready for use. Other configuration tasks may also have to be performed, but these steps depend on the individual specifications of your G350 and your network.

Most G350 configuration tasks are performed using the Avaya G350 Media Gateway Command Line Interface (CLI). However, Avaya provides two GUI interfaces that are designed to perform the basic configuration tasks described in this section. These are the Avaya Installation Wizard (Avaya IW) and the Avaya Gateway Installation Wizard (GIW). You can use the Avaya IW or the GIW to set a PMI, enable the console or USB port for modem use, upgrade firmware, and register the G350 with an MGC. You can then use the CLI to perform ongoing administration.

Configuration using CLI

You can use the Avaya G350 Media Gateway Command Line Interface (CLI) to manage the G350. The CLI is a command prompt interface that enables you to type commands and view responses. For instructions on how to access the G350 CLI, see Accessing the CLI on page 27.

This guide contains information and examples about how to use CLI commands to configure the Avaya G350 Media Gateway. For more information about the G350 CLI and a complete description of each CLI command, see the *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

Configuration using GUI applications

Several Avaya GUI applications enable you to perform some configuration tasks on the Avaya G350 Media Gateway.

The Avaya Installation Wizard (Avaya IW) is a web-based installation wizard that leads the user through the key configuration steps of a G350 installation. The Avaya IW can be used for initial configuration of a G350 with an S8300 installed as the G350's primary (ICC) or backup (LSP) call controller. For instructions on how to access the Avaya IW, see Accessing Avaya IW on page 32. For step-by-step instructions on how to configure the G350 using the Avaya IW, see Configuring the G350 using the Avaya IW on page 389.

The Avaya Gateway Installation Wizard (GIW) is a standalone application that allows the user to perform certain basic G350 configuration tasks. The GIW can be used for initial configuration of a G350 that does not have an S8300 installed as either the G350's primary (ICC) or backup (LSP) call controller. For instructions on how to access the GIW, see Accessing GIW on page 34. For step-by-step instructions on how to configure the G350 using the GIW, see Configuring the G350 using the GIW on page 427.

You can also use the Avaya G350 Manager to configure most features of the G350. The Avaya G350 Manager is a GUI application. You can access the Avaya G350 Manager from Avaya Integrated Management software or from a web browser. Most of the commands that are available through the G350 CLI are also available through the Avaya G350 Manager. For more information about the Avaya G350 Manager, see the *Avaya G350 Manager User Guide*, 650-100-709.

Saving configuration changes

When you make changes to the configuration of the Avaya G350 Media Gateway, you must save your changes to make them permanent. The G350 has two sets of configuration information:

- Running configuration
- Startup configuration

The G350 operates according to the running configuration. When the G350 is reset, the G350 erases the running configuration and loads the startup configuration as the new running configuration. When you change the configuration of the G350, your changes affect only the running configuration. Your changes are lost when the G350 resets if you do not save your changes.

Use the **`copy running-config startup-config`** command to save changes to the configuration of the G350. A copy of the running configuration becomes the new startup configuration.

You can back up either the running configuration or the startup configuration to an FTP or TFTP server on your network. You can restore a backup copy of the configuration from the FTP or TFTP server. When you restore the backup copy of the configuration, the backup copy becomes the new running configuration on the G350. For more information, see Managing configuration files on page 60.

Firmware version control

Firmware is the software that runs the Avaya G350 Media Gateway. The Avaya G350 Media Gateway has two firmware banks:

- Bank A
- Bank B

Each firmware bank contains a version of the G350 firmware. These may be different versions. The purpose of this feature is to provide redundancy of firmware. You can save an old version of the firmware in case you need to use it later. If it becomes necessary to use the older version, you can reset the G350 using the older version. This is particularly important when uploading new versions.

For more information on using the two firmware banks, see Software and firmware upgrades on page 57.

Chapter 3: Accessing the Avaya G350 Media Gateway

This chapter provides information about the various ways of configuring the Avaya G350 Media Gateway and contains the following sections:

- Accessing the CLI — instructions on how to access the CLI
- Accessing Avaya IW — instructions on how to access the Avaya IW
- Accessing GIW — instructions on how to access the GIW
- Accessing Avaya Communication Manager — instructions on how to access the Avaya Communication Manager
- Managing login permissions — instructions on using and configuring usernames and passwords, and on configuring the G350 to use SSH, SCP, and RADIUS authentication
- Special security features — instructions on how to enable and disable the recovery password, and the G350's ability to establish incoming and outgoing telnet connections

Accessing the CLI

This section explains how to access the CLI and includes the following topics:

- CLI Overview — basic instructions on how to use the CLI
- Accessing the CLI locally — instructions on how to access the CLI locally via a local network or a console device
- Accessing CLI via modem — instructions on how to access the CLI from a remote location using a modem

CLI Overview

The CLI is a textual command prompt interface that you can use to configure the Avaya G350 Media Gateway and media modules. You can access the CLI with any of the following:

- Telnet through the network
- A console device
- Telnet through dialup:
  - Telnet through serial modem
  - Telnet through USB modem
  - Telnet through USB modem via the S8300

Log in to the CLI with a username and password that your system administrator provides. If your network has a RADIUS server, you can use RADIUS authentication. For more information, see Managing login permissions on page 36.

Note:

You can disconnect a telnet session by typing **<Ctrl>+]**. This is particularly useful if the normal telnet logout does not work.

CLI contexts

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

For example, in order to configure a Loopback interface, you must first enter the Loopback context from General context. Enter the Loopback context using the **`interface`** command with an interface identifier such as **`interface loopback 1`**. Once you are in the Loopback context, you can enter Loopback interface commands.

CLI help

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

If you type **`help`** or **`?`** before or after the first word or words of a command, the CLI displays a list of all commands in the current context that begin with this word or words. For example, to display a list of IP commands available in general context, type **`help ip`**, **`ip help`**, **`? ip`**, or **`ip ?`**.

If you type **help** or **?** before or after a full command, the CLI displays the command's syntax and parameters, and an example of the command. You must be in the command's context in order to use the **help** command to display information about the command. In the following example, the user enters the context of the Vlan 1 interface and displays help for the **bandwidth** command.

```
G350-001(super)# interface vlan 1
G350-001(super-if:Vlan 1)# bandwidth ?
Bandwidth commands:
-----------------------------------------------------------------------
Syntax: bandwidth <kilobytes size>
                  <kilobytes size> : integer (1-10000000)
Example: bandwidth 1000
```

Accessing the CLI locally

There are two ways you can access the CLI locally:

- Accessing CLI via local network
- Accessing CLI with a console device

Accessing CLI via local network

You can access the CLI from a computer on the same local network as the Avaya G350 Media Gateway by using any standard telnet program. For the host address, you can use the IP address of any G350 interface.

Accessing CLI with a console device

To access the CLI with a console device, use one of the following types of console devices:

- Serial terminal
- Laptop with serial cable and terminal emulator software

Connect the console device to the console port (CONSOLE) on the front panel of the Avaya G350 Media Gateway. Use only an approved Avaya serial cable. For more information about approved Avaya serial cables, see *Overview of the Avaya G350 Media Gateway,* 555-245-201.

For more information about the console port, see Configuring the console port for modem use on page 78.

Accessing CLI via modem

You can access the CLI from a remote location using any standard telnet program. Use a dialup PPP network connection from a modem at the remote location to either a USB or a serial modem connected to the console port on the front panel of the G350. Use only an approved Avaya serial cable. For more information about approved Avaya serial cables, see *Overview of the Avaya G350 Media Gateway,* 555-245-201.

Note:

You can disconnect a telnet session by typing **<Ctrl>**+**]**. This is particularly useful if the normal telnet logout does not work.

Accessing CLI via a USB modem

To access the CLI with telnet through dialup from a remote location using a USB modem:

1. Connect a modem to the USB port on the front panel of the Avaya G350 Media Gateway. Use a USB cable to connect the modem. It is recommended to use a Multitech MultiModem USB, MT5634ZBA-USB-V92.
2. Make sure the USB port is properly configured for modem use. For details, see Configuring the USB port for modem use on page 77.
3. From the remote computer, create a dialup network connection to the Avaya G350 Media 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 G350 uses PAP authentication. If your network has a RADIUS server, you can use RADIUS authentication for the PPP connection. For more information, see Managing login permissions on page 36.
4. Open any standard telnet program on the remote computer.
5. Open a telnet session to the IP address of the USB port on the G350. The default IP address of the USB port is 10.3.0.3 with subnet mask 255.255.255.0. For instructions on how to change the IP address of the USB port (i.e., the USB interface), see Configuring the USB port for modem use on page 77.
6. Configure the serial connection on the remote computer to match the configuration of the USB port on the G350. The USB port uses the following settings:
   - baud — 9600
   - data bits — 8
   - parity — none
   - stop bits — 1
   - flow control — hardware

Accessing CLI via a serial modem

To access the CLI with telnet through dialup from a remote location using a serial modem:

1. Connect a modem to the console port (CONSOLE) on the front panel of the Avaya G350 Media Gateway. Use an RJ-45 serial cable to connect the modem. It is recommended to use a Multitech MultiModem ZBA, MT5634ZBA-V92.
2. Make sure the console port is properly configured for modem use. For details, see Configuring the console port for modem use on page 78.
3. From the remote computer, create a dialup network connection to the Avaya G350 Media 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 G350 uses PAP authentication. If your network has a RADIUS server, you can use RADIUS authentication for the PPP connection. For more information, see Managing login permissions on page 36.
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 G350. The default IP address of the console port is 10.3.0.1 with subnet mask 255.255.255.0. For instructions on how to change the IP address of the console port (i.e., the console interface), see Configuring the console port for modem use on page 78.
6. Configure the serial connection on the remote computer to match the configuration of the console port on the G350. The console port uses the following settings:
   - baud — 9600
   - data bits — 8
   - parity — none
   - stop bits — 1
   - flow control — hardware

Accessing CLI via a modem connection to the S8300

If the Avaya G350 Media Gateway includes an S8300 Media Server, you can access the CLI from a remote location by establishing a PPP network connection from a modem at the remote location to a USB modem connected to the one of the USB ports on the front panel of the S8300.

Note:

In order to access the CLI via the S8300, the PMI of the G350 must be configured. See Configuring the Primary Management Interface (PMI) on page 50.

To access the G350 CLI via telnet through a dialup connection from a remote location via the S8300:

1. Connect a USB modem to either of the two USB ports on the Avaya S8300 Media Server. It is recommended to use a Multitech MultiModem USB, MT5634ZBA-USB-V92.
2. Use the Avaya Maintenance Web Interface (MWI) to configure the USB port on the S8300 for modem use. For instructions, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.
3. From a remote computer, create a dialup network connection to the S8300. Use the TCP/IP and PPP protocols to create the connection.
4. Open any standard telnet program on the remote computer.
5. Enter the command **`telnet`**, followed by the IP address of the S8300 USB port to which the modem is connected.
6. Enter the command **`telnet`**, followed by the PMI of the G350.

Accessing Avaya IW

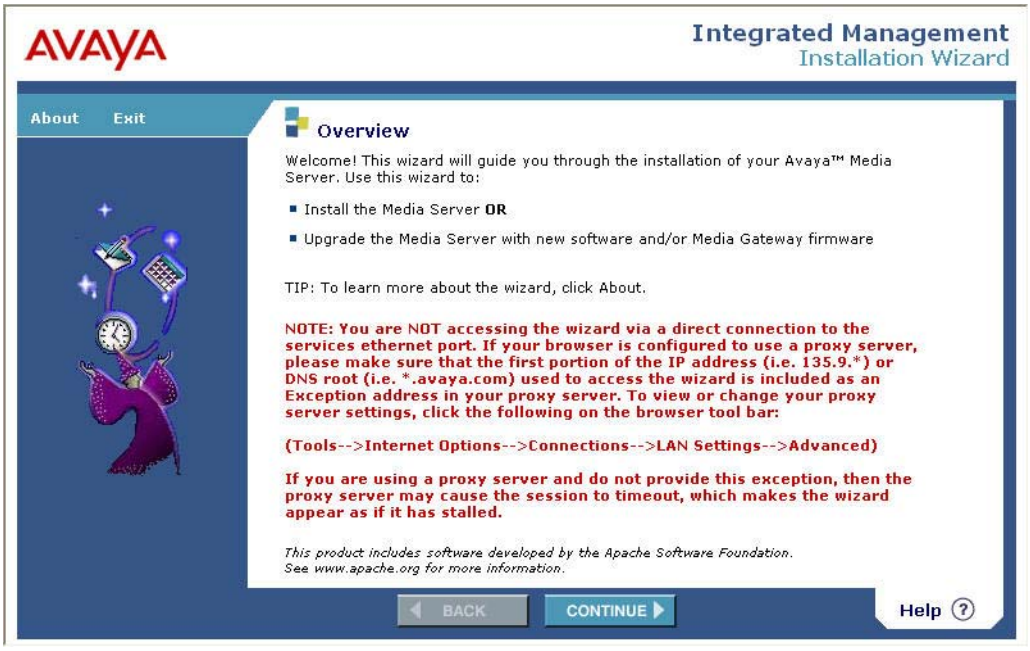
The Avaya Installation Wizard (Avaya IW) is a web-based installation wizard that is used with the Avaya G350 Media Gateway to perform initial configuration tasks and to upgrade software and firmware. The Avaya IW is designed for use with systems that include an S8300 Media Server, operating in either ICC or LSP mode. See The Media Gateway Controller (MGC) on page 52.

Specifically, you can perform the following tasks with the Avaya IW:

- Configure PMI information — see Configuring the Primary Management Interface (PMI) on page 50
- Configure SNMP information — see Configuring SNMP on page 119
- Configure Ethernet interfaces — see Configuring Ethernet ports on page 61
- Configure primary and secondary Media Gateway Controllers — see The Media Gateway Controller (MGC) on page 52
- Install license and password files
- Install software and firmware upgrades — see Software and firmware upgrades on page 57
- Enable and configure the USB ports of the S8300 for modem use
- Enable the G350 for modem use — see Configuring the G350 for modem use on page 77
- Configure G350 telephony and trunk parameters
- Configure alarms
- Change your password

When performing initial configuration of the G350, you can access and run the Avaya IW using a laptop computer. To access the Avaya IW:

1. Connect a laptop computer to the Services port of the S8300, using a crossover cable.
2. Make sure the laptop is configured as follows:
   - IP Address: 192.11.13.5
   - NetMask: 255.255.255.252
   - Disable DNS
   - Clear the primary WINS and secondary WINS IP Addresses
   - Disable the Proxy Server in the Internet Explorer
3. Launch Internet Explorer on the laptop and type the following URL to access the S8300 Media Server Home Page: http://192.11.13.6
4. Enter the appropriate login name and password.
5. Select the Launch Installation Wizard link from the home page. The Overview screen appears:



For step-by-step instructions how to configure the G350 using the Avaya IW, see Appendix B: Configuring the G350 using the Avaya IW.

Accessing GIW

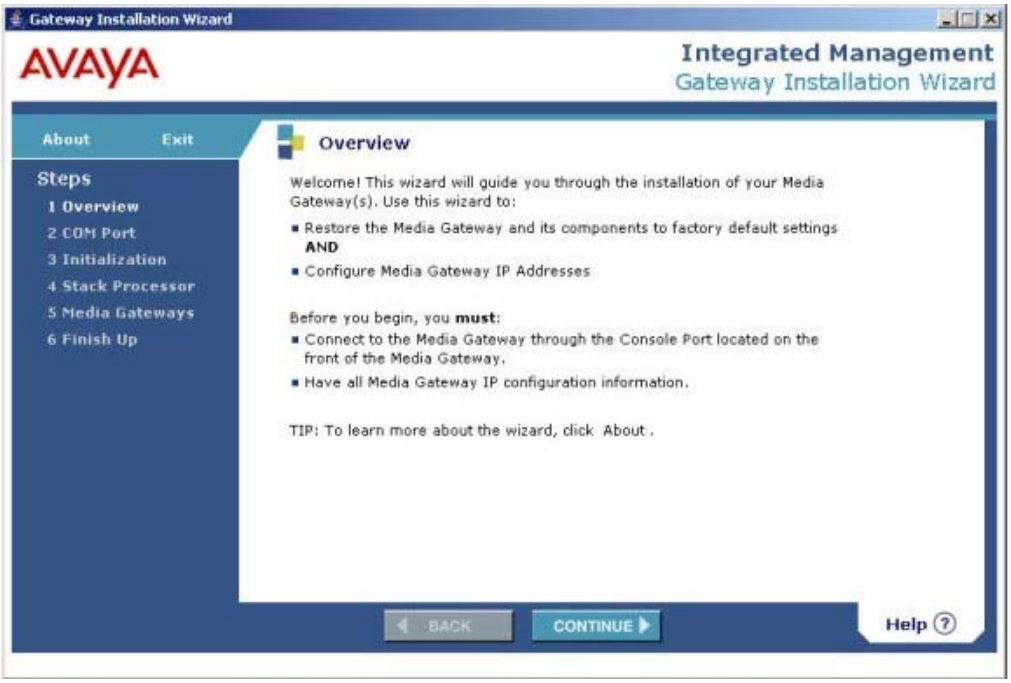
The Gateway Installation Wizard (GIW) is an automated tool that allows you to perform a streamlined installation and configuration of a G350 controlled by an internal S8300. You can use the GIW to perform initial configuration of the G350 and to upgrade software and firmware. Specifically, you can perform the following tasks with the GIW:

- Configure PMI information — see Configuring the Primary Management Interface (PMI) on page 50
- Configure SNMP information — see Configuring SNMP on page 119
- Configure primary and secondary Media Gateway Controllers — see The Media Gateway Controller (MGC) on page 52
- Check connectivity between the G350 and its Media Gateway Controller
- Display information on the G350 and media modules installed on the G350
- Enable the G350 for modem use — see Configuring the G350 for modem use on page 77
- Install software and firmware upgrades — see Software and firmware upgrades on page 57

To access the GIW:

1. Install GIW on a laptop computer from the CD provided by Avaya. The laptop should be running Windows 2000 or Windows XP.
2. Plug one end of an RJ-45 to RJ-45 cable into a DB-9 adapter.
3. Plug the RJ-45 connector at the other end of the cable into the console port (CONSOLE) of the G350.
4. Plug the DB-9 end of the cable into the COM port of the laptop computer.

5. From your laptop computer, double-click the GIW icon to run GIW. The Overview screen appears:



For step-by-step instructions on how to configure the G350 using the GIW, see Appendix C: Configuring the G350 using the GIW.

Accessing Avaya Communication Manager

Use Avaya Communication Manager software to control telephone services that the Avaya G350 Media Gateway provides. Avaya Communication Manager software runs on a media server. There might be several media servers on your network that can control the Avaya G350 Media Gateway. You can access Avaya Communication Manager on any media server that is a Media Gateway Controller (MGC) for the Avaya G350 Media Gateway. For more information, see The Media Gateway Controller (MGC) on page 52.

You can access Avaya Communication Manager with any of the following:

- Avaya Site Administration (ASA). ASA provides wizards and other tools that help you to use Avaya Communication Manager effectively. For more information, see *Administrator's Guide for Avaya Communication Manager*, 555-233-506.
- Telnet to port 5023 on the media server, using the following syntax: **`telnet <IP address of the media server> <5023>`**. For more information, see *Administrator's Guide for Avaya Communication Manager*, 555-233-506.
- Avaya G350 Media Gateway CLI. See Accessing the registered MGC on page 54.

Managing login permissions

This section explains how to manage login permissions and contains the following topics:

- Security overview — overview of the G350's internal security mechanism and how it can operate in conjunction with a RADIUS authentication system
- Managing users and passwords — explanation of the users, passwords, and access privileges, and instructions on how to define new users
- SSH protocol support — explanation of SSH authentication and instructions on how to configure SSH authentication parameters
- SCP protocol support — explanation of SCP authentication and instructions on how to configure SCP authentication parameters
- RADIUS authentication — instructions on how to configure the G350 to work with an external RADIUS server
- 802.1x protocol — instructions on how to configure 802.1x protocol

Security overview

The Avaya G350 Media Gateway includes a security mechanism through which the system administrator defines users and assigns each user and username and a password. Each user is assigned a privilege level. The user's privilege level determines which commands the user can perform.

In addition to its basic security mechanism, the G350 supports secure data transfer via SSH and SCP.

The G350 can be configured to work with an external RADIUS server to provide user authentication. When RADIUS authentication is enabled on the G350, the RADIUS server operates in conjunction with the G350 security mechanism. When the user enters a username, the G350 first searches its own database for the username. If the G350 does not find the username in its own database, it establishes a connection with the RADIUS server, and the RADIUS server provides the necessary authentication services.

The G350 also uses the 802.1x protocol in conjunction with EAP within EAPOL and over RADIUS to provide a means of authenticating and authorizing users attached to a LAN port, and of preventing access to that port in cases where the authentication process fails.

Managing users and passwords

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

- When you access the CLI. For more information, see Accessing the CLI on page 27.
- When you connect to the console port modem with dialup PPP. For more information, see Accessing CLI via modem on page 30.
- When you open Avaya G350 Manager.

When you use Avaya G350 Manager or the CLI, your username determines your privilege level. The commands that are available to you during the session depend on your privilege level.

If your network has a RADIUS server, you can use RADIUS authentication instead of a username and password. A RADIUS server provides centralized authentication service for many devices on a network. For more information, see RADIUS authentication on page 40.

Privilege level

When you start to use Avaya G350 Manager or the CLI, you must enter a username. The username that you enter sets your privilege level. The commands that are available to you during the session depend on your privilege level. If you use RADIUS authentication, the RADIUS server sets your privilege level.

The G350 provides the following three privilege levels:

- **Read-only** — You can use Read-only privilege level to view configuration parameters.
- **Read-write** — You can use Read-write privilege level to view and change all configuration parameters except those related to security. For example, you cannot change a password with Read-write privilege level.
- **Admin** — You can use Admin privilege level to view and change all configuration parameters, including parameters related to security. Use Admin privilege level only when you need to change configuration that is related to security, such as adding new user accounts and setting the device policy manager source.

The default username has Admin privilege level. For security reasons, the network administrator usually changes the password of the default username. For more information about privilege levels, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

Configuring usernames

To create a username, use the **`username`** command. To remove a username, use the **`no username`** command. To change the password or the privilege level for a username, remove the username and add it again. You need an Admin privilege level to use the **`username`** and **`no username`** commands.

When you create a new user, you must define the user's password and privilege level. The following example creates a user named John with the password johnny and a Read-write privilege level:

```
G350-001> username john password johnny access-type read-write
```

SSH protocol support

SSH (Secure Shell) protocol is a security protocol that enables you to establish a remote session over a secured tunnel, also called a remote shell. SSH accomplishes this by creating a transparent, encrypted channel between the local and remote devices. In addition to the remote shell, SSH provides secure file transfer between the local and remote devices. SSH is used for telnet file transfers. The G350 supports two concurrent SSH users.

There are two ways to establish an SSH session:

- RSA authentication
- Password authentication

Use the **`ssh enable`** command to determine which of these ways is used on the G350. See SSH Configuration on page 39.

RSA authentication works as follows:

- The G350 generates a key of variable length (512-2048 bits) using the DSA encryption method. This is the private key.
- The G350 calculates an MD5 Hash of the private key, called a fingerprint (the public key). The fingerprint is always 16 bytes long. This fingerprint is displayed.
- The G350 sends the public key (the fingerprint) to the client computer. This public key is used by the client to encrypt the data it sends to the G350. The G350 decrypts the data using the private key.
- Both sides negotiate and must agree on the same chipper type. The G350 only supports 3DES-CBC encryption. The user on the client side accepts the fingerprint. The client maintains a cache containing a list of fingerprints per server IP address. If the information in this cache changes, the client notifies the user.
- The client chooses a random number that is used to encrypt and decrypt the information sent.
- This random number is sent to the G350, after encryption based on the G350's public key.
- When the G350 receives the encrypted random number, it decrypts it using the private key. This random number is now used with the 3DES-CBC encryption method for all encryption and decryption of data. The public and private keys are no longer used.

Password authentication works as follows:

- Before any data is transferred, the G350 requires the client to supply a user name and password. This authenticates the user on the client side to the G350.

SSH Configuration

Use the **ip ssh enable** command to enable SSH authentication and set the SSH parameters. Use the **no** form of this command to disable the SSH server. Disabling the server disconnects all active SSH sessions. By default, SSH is enabled.

You can set the following SSH parameters using the **ssh enable** command:

- ***timeout*** — sets the time interval (in seconds) that the SSH server waits for the SSH client to respond. If this time elapses with no response, the session's SSH server disconnects. The timeout can be from 20 to 400 seconds. The default value is 120.

  Note:

  This parameter applies to the SSH negotiation phase. Once an SSH session is established, the CLI timeout applies.

- ***authentication-retries*** — the number of connection attempts after which the SSH server disconnects. This parameter can be from 1 to 5. The default value is 3.
- ***rsa-authentication*** — enables (yes) or disables (no) the public key authentication method. By default, public key authentication is disabled.
- ***password-authentication*** — enables (yes) or disables (no) the password authentication method. By default, password authentication is enabled.
- ***port*** — changes the default value of the SSH port. Changing the port number does not interrupt active connections. The default value is 22.

Use the **ssh-client known-hosts** command to clear the client's list of server fingerprints. Each client maintains a list of server fingerprints. If a key changes, the client's verification of the server's fingerprint will fail, thereby preventing the client's access to the server. If this happens, you can use the **ssh-client known-hosts** command to erase the client's server fingerprint list. This enables the client to access the server and begin to recreate its list of fingerprints with the server's new fingerprint.

Use the **crypto key generate dsa** command to generate an SSH host key pair.

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

Use the **show ip ssh** command to display a list of active SSH sessions.

SCP protocol support

In addition to data transfer via an SSH session, the SSH protocol is also used to support SCP for secure file transfer. When using SCP, the G350 is the client, and an SCP server must be installed on the management station. After users are defined on the SCP server, the G350 acts as an SCP client.

The process of establishing an SCP session is the same process as described in SSH protocol support on page 38, except that the roles of the G350 and the client computer are reversed.

To perform file transfers secured by SCP, the G350 launches a local SSH client via the CLI. This establishes a secured channel to the secured file server. The G350 authenticates itself to the server by providing a user name and password. With a Windows-based SSH server (WinSSHD), the user name provided must be a defined user on the Windows machine with read/write privileges. The files transferred via SCP are saved in the *C:\Documents and Settings\ username* directory.

The network element performs file transfer in unattended mode.

RADIUS authentication

If your network has a RADIUS server, you can configure the G350 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 G350. When you try to access the G350, the G350 searches for your username and password in its own database first. If it does not find them, it activates RADIUS authentication.

To use RADIUS authentication:

1. Configure your RADIUS server with the usernames, passwords, and privilege levels that you want to use on the G350.
2. Configure RADIUS authentication on the G350, as described below.

Use the following commands to configure RADIUS authentication on the G350. For more information about these commands, see the *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

1. Use the **`set radius authentication enable`** command to enable RADIUS authentication.
2. Use the **`set radius authentication secret`** command to set the shared secret for the authentication. This command must be followed by a text string. For example:

   `set radius authentication secret hush`
3. Use the **`set radius authentication server`** command to set the IP address of the primary or secondary RADIUS Authentication server.

You can use the following commands to change the RADIUS parameters. These commands are optional.

- Use the **`set radius authentication retry-number`** command to set the number of times to resend an access request when there is no response.
- Use the **`set radius authentication retry-time`** command to set the time to wait before resending an access request.
- Use the **`set radius authentication udp-port`** command to set the RFC 2138 approved UDP port number. Normally, the UDP port number should be set to its default value of 1812. Some early implementations of the RADIUS server used port number 1645.

To disable RADIUS authentication on the G350, use the **`set radius authentication disable`** command.

To display the RADIUS parameters, use the **`show radius authentication`** command. Shared secrets are not displayed.

For additional information on RADIUS configuration and authentication, go to the Avaya web site at http://www.avaya.com/support, and perform a search for the document *Avaya G700/ G350 RADIUS Configuration Overview*.

802.1x protocol

The 802.1x protocol is a method for performing authentication to obtain access to the G350's LAN ports. 802.1x provides a means of authenticating and authorizing users attached to a LAN port and of preventing access to that port in cases where the authentication process fails. You can enable 802.1x on the MM314 media module's 10/100 Ethernet ports.

Note:

You cannot enable 802.1x on the MM314 media module's Gigabit Ethernet port (port 51).

The 802.1x protocol defines an interaction between the following three entities:

- Supplicant — an entity (the host) at one end of a point-to-point LAN segment that is requesting authentication
- Authenticator — an entity (in this case the G350) at the other end of a point-to-point LAN segment that facilitates authentication of the Supplicant
- Authentication (RADIUS) Server — an entity that provides an authentication service to the Authenticator. The Authentication Server determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the Authenticator.

How port based authentication works

The authentication procedure is port-based, which means:

- access control is achieved by enforcing authentication on connected ports
- if an endpoint station that connects to a port is not authorized, the port state is set to "unauthorized", which closes the port to all traffic
- as a result of an authentication attempt, the port can be either in a "blocked" or a "forwarding" state

802.1x interacts with existing standards to perform its authentication operation. Specifically, it makes use of Extensible Authentication Protocol (EAP) messages, encapsulated within Ethernet frames (EAPOL), and EAP over RADIUS for the communication between the Authenticator and the Authentication Server.

Note:

The G350 only supports MD5 EAP type.

Configuring 802.1x

You can configure 802.1x on the G350's PoE module (MM314). You can configure 802.1x on any of the MM314 ports except the Gigabit Ethernet port (port 51).

To configure 802.1x:

1. Configure RADIUS authentication on the G350. For instructions, see RADIUS authentication on page 40.
2. Use the **`set port dot1x port-control`** command to change the 802.1x mode of an individual port. This command must be followed by the module and port number, and the 802.1x mode. The following are the possible modes:
   - *`force-unauthorize`* — the port is always blocked
   - *`auto`* — whether the port is blocked or open depends on the authentication outcome
   - *`force-authorize`* — the port is always open (in forwarding state)

   By default, all ports are in auto mode. In other words, all ports are configured to use 802.1x authentication if it is enabled on the G350. If a port is not in auto mode, you can use the following command to return the port to auto mode:

```
G350-001(super)# set port dot1x port-control 6/3 auto
Done !
G350-001(super)#
```

3. Use the **`set port dot1x port-control`** command to configure the authentication mode of the LAN port connected to the RADIUS server as force-authorize. This ensures that the port remains open at all times, so that it will be able to transmit authentication requests to the RADIUS server. For example, if port 2 is the port that connects to the RADIUS server, type the following command:

```
G350-001(super)# set port dot1x port-control 6/2 force-authorize
Done !
G350-001(super)#
```

4. Use the **`set dot1x system-auth-control enable`** command to enable 802.1x authentication on all ports set to auto mode. For example:

```
G350-001(super)# set dot1x system-auth-control enable
```

   To disable 802.1x authentication on the G350, use the command **`set dot1x system-auth-control disable`**.

   Once the authentication process is enabled, the process proceeds as follows:

   - The Supplicant is asked to supply a user name and password.
   - If 802.1x authentication is enabled on the port, the Authenticator initiates authentication when the link is up.
   - When authentication is completed, the Supplicant receives a Permit/Deny notification.
   - Authentication fails if:
     - the Supplicant fails to respond to requests from the Authenticator
     - Management controls prevent the port from being authorized
     - The link is down
     - The user supplied incorrect login information.

5. For additional security, use the **`set port dot1x re-authentication`** command, followed by the module and port number (or a range of ports) to enable re-authentication on a port or a group of ports. By default, re-authentication is disabled. For example:

```
G350-001(super)# set port dot1x re-authentication 6/4-6 enable
```

   To disable re-authentication, use this command **`set port dot1x re-authentication`** ***`module/port`*** **`disable`**.

6. By default, the re-authentication period is 3600 seconds. In other words, if re-authentication is enabled on a port, the port attempts to re-authenticate the host every 3600 seconds. To change the re-authentication period, use the **`set dot1x re-authperiod`** command, followed by the length of the new re-authentication period in seconds (0 to 65535). For example:

```
G350-001(super)# set port dot1x re-authperiod 6/4 400
```

Manual re-authentication

You can perform a manual re-authentication at any time. To perform a manual re-authentication, use the **`set prt dot1x re-authenticate`** command, followed by the module and port number (or range of ports). For example:

```
G350-001(super)# set port dot1x re-authenticate 6/5-10
```

When you perform a manual re-authentication, the port or ports attempt to re-authenticate the host immediately.

Optional 802.1x commands

You can use the following commands to modify 802.1x parameters:

- Use the **`clear dot1x config`** command to disable 802.1x on the G350 and return to default parameters.
- Use the **`set port dot1x initialize`** command, followed by the module and port number (or range of ports) to initialize a port or ports.
- Use the **`set dot1x quiet-period`** command, followed by a time period in seconds (0 to 65535), to set the minimum idle time between authentication attempts for all ports on which 802.1x is enabled.
- Use the **`set port dot1x quiet-period`** command, followed by the module and port number (or range of ports) and a time period in seconds (0 to 65535), to set the minimum idle time between authentication attempts for a specific port or ports.
- Use the **`set dot1x tx-period`** command, followed by a time period in seconds (1 to 65535), to set the time internal between attempts to access the Authenticated Station for all ports on which 802.1x is enabled.
- Use the **`set port dot1x tx-period`** command, followed by the module and port number (or range of ports) and a time period in seconds (0 to 65535), to set the time internal between attempts to access the Authenticated Station for a specific port or ports.
- Use the **`set dot1x supp-timeout`** command, followed by a time period in seconds (1 to 65535), to set the authenticator-to-supplicant retransmission timeout period (the time for the G350 to wait for a reply from the Authenticated Station) for all ports on which 802.1x is enabled.
- Use the **`set port dot1x supp-timeout`** command, followed by the module and port number (or range of ports) and a time period in seconds (0 to 65535), to set the authenticator-to-supplicant retransmission timeout period (the time for the G350 to wait for a reply from the Authenticated Station) for a specific port or ports.
- Use the **`set dot1x max-req`** command, followed by a number from 1 to 10, to set the maximum number of times the port tries to retransmit requests to the Authenticated Station before the session is terminated for all ports on which 802.1x is enabled.

- Use the **set port dot1x max-req** command, followed by the module and port number (or range of ports) and a number from 1 to 10, to set the maximum number of times the port tries to retransmit requests to the Authenticated Station before the session is terminated for a specific port or ports.
- Use the **set port dot1x server-timeout** command, followed by the module and port number (or range of ports) and a time period in seconds (1 to 65535) to set the server timeout (the time to wait for a reply from the Authentication Server) per port.

Displaying 802.1x parameters

You can use the following commands to display 802.1x parameters:

- Use the **show dot1x** command to display the system 802.1x parameters, including whether 802.1x is enabled or disabled on the G350.
- Use the **show port dot1x** command to display all the configurable values associated with the authenticator port access entity (PAE) and backend authenticator. To display values for a particular port, type the module and port numbers after the command. If you do not enter a module and port number, the command displays values for all ports on which 802.1x can be configured. For example:

```
G350-001(super)# show port dot1x
Port   Auth     BEnd   Port     Port   Re   Quiet ReAuth Server Supp   Tx    Max
Number State    State  Control  Status Auth Priod Priod  Tmeout Tmeout Priod Req
------ -------- ------ -------- ------ ---- ----- ------ ------ ------ ----- --
6/1    Authed   Idle   Auto     Disa   60   100   30     30     30     30    2
6/2    Authed   Idle   Auto     Disa   60   100   30     30     30     30    2
6/3    Authed   Idle   Auto     Disa   60   100   30     30     30     30    2
6/4    Authed   Idle   Auto     Disa   60   100   30     30     30     30    2
6/5    Authed   Idle   Auto     Disa   60   100   30     30     30     30    2
6/6    Authed   Idle   Auto     Disa   60   100   30     30     30     30    2
```

Table 1 lists and describes the columns in the **show port dot1x** display.

Table 1: 802.1x Show port output description *1 of 2*

Column	Description
Port Number	Number of the module and port
Auth State	The Port Access Entity state. Possible states are: • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuth • ForceUnauth
BEnd Stat	The current state of the Backend Authentication state machine. Possible states are: • Request • Response • Success • Fail • Timeout • Idle • Init
Port Control	Port control type. Valid values include: • force-authorized • force-unauthorized • auto
Port Status	The current value of the controlled port status. Possible states include: • Authorized • Unauthorized
Re Auth	The state of re-authentication on the port. Possible states include: • Enabled — The port connection is re-authenticated after the reAuthPeriod. • Disabled — The port connection is not re-authenticated. The reAuthPeriod is ignored.
Quiet Period	The amount of time, in seconds, between sending authentication requests.

1 of 2

Table 1: 802.1x Show port output description *2 of 2*

Column	Description
ReAuth Period	The time, in seconds, after which the port connection should be re-authenticated.
Server Tmout	The amount of time, in seconds, the G350 waits for a response from the RADIUS server.
Supp Tmeout	The amount of time, in seconds, before resending authentication requests.
Tx Priod	The amount of time, in seconds, in which an authentication request must be answered.
Max Req	The maximum number of times a request for authentication is sent before timing out.
	2 of 2

- Use the **`show port dot1x statistics`** command to display 802.1x statistics. To display statistics for a particular port, type the module and port numbers after the command. If you do not enter a module and port number, the command displays statistics for all ports on which 802.1x can be configured. For example:

```
G350-001(super)# show port dot1x statistics 6/1
Port   Tx_Req/Id  Tx_Req    Tx_Total   Rx_Start  Rx_Logff  Rx_Resp/Id  Rx_Resp
------ ---------  --------  ---------  --------  --------  ----------  ---------
6/1        2         5          0          0         0          0
Port   Rx_Invalid  Rx_Len_Err  Rx_Total   Last_Rx_Frm_Ver  Last_Rx_Frm_Src_Mac
------ ----------  ----------  ---------  ---------------  -------------------
6/1        0         0          0                0          1d-80-00-00-00-00
```

Special security features

This section describes the following special security features:

- Enabling and disabling recovery password — instructions on how to enable and disable the recovery password, which provides emergency access to the G350 via a direct connection to the console port
- Enabling and disabling telnet access — instructions on how to enable and disable telnet access to and from the G350

Enabling and disabling recovery password

The G350 includes a special recovery password. The purpose of the recovery password is to enable the system administrator to access the G350 in the event that the regular password is forgotten. You can only use the recovery password when accessing the G350 via a direct connection to the console port. See Accessing CLI with a console device on page 29.

You can use the **`set terminal recovery password`** command to enable or disable the recovery password. You can only use this command when accessing the G350 via a direct connection to the console port.

Enabling and disabling telnet access

You can enable and disable the G350's ability to establish incoming and outgoing telnet connections, using the following commands. You can only use these commands when accessing the G350 via a direct connection to the console port. See Accessing CLI with a console device on page 29.

- Use the **`ip telnet`** command to enable the G350 to establish an incoming telnet connection. Use the **`no`** form of this command to disable the G350's ability to establish an incoming telnet connection.
- Use the **`ip telnet client`** command to enable the G350 to establish an outgoing telnet connection. Use the **`no`** form of this command to disable the G350's ability to establish an outgoing telnet connection.

Chapter 4: Basic device configuration

This chapter provides information about basic configuration of the Avaya G350 Media Gateway and contains the following sections:

- Defining an interface — instructions on how to define a new interface and its IP address
- Configuring the Primary Management Interface (PMI) — instructions on how to configure parameters that identify the G350 to other devices
- Defining the default gateway — instructions on how to define a G350 interface as the G350's default gateway
- Configuring the Media Gateway Controller (MGC) — instructions on how to configure an MGC to work with the G350
- Viewing the status of the device — instructions on how to view the status of the G350
- Version management — instructions on how to manage and upgrade software, firmware, configuration, and other files on the G350

Defining an interface

In a new Avaya G350 Media Gateway, only the console and USB interfaces are defined. All other interfaces must be defined by the administrator, after installation of the G350.

To define an interface:

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 2/1
   ```

   For more information on the various types of interfaces, see Router interface concepts on page 161.

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.
4. For a list and descriptions of other interface configuration commands, see Configuring interfaces on page 160. For interface configuration examples, see WAN configuration example on page 105.

Configuring the Primary Management Interface (PMI)

The Primary Management Interface (PMI) address is the IP address of an interface that you can specify on the Avaya G350 Media Gateway. The first IP address you configure on the G350 automatically becomes the PMI. You can subsequently assign any IP interface to be the PMI.

The PMI is used as the IP address of the G350 for the following management functions:

- Registration of the G350 to an MGC
- Sending SNMP traps
- Opening telnet sessions from the G350
- Sending messages from the G350 using FTP and TFTP protocol

You can designate any of the G350's interfaces to serve as the G350's PMI. The PMI must be an IP address that the MGC recognizes. If you are not sure which interface to use as the PMI, check with your system administrator.

To set the PMI of the G350:

1. Use the **`interface`** command to enter the context of the interface to which you want to set the PMI. For example, to use the VLAN 1 interface as the PMI, type **`interface vlan 1`**.

   Note:

   If the interface has not been defined, you must define it now. See Defining an interface on page 49.

2. Type the **`pmi`** command.
3. Type **`exit`** to return to general context.
4. Type the **`copy running-config startup-config`** command. This saves the new PMI in the startup configuration file.
5. Use the **`reset`** command to reset the G350.

   Note:

   Most configuration changes take effect as soon as you make the change, but must be saved to the startup configuration file in order to remain in effect after you reset the G350. The PMI address is an exception. A change to the PMI does not take effect at all until you reset the G350.

6. To verify the new PMI, type the **`show pmi`** command in general context. If you use this command before you reset the G350, it displays two different PMIs:
   - **Active PMI** — the PMI the G350 is currently using, as defined in the running configuration file
   - **Configured PMI** — the PMI that the G350 is configured to use after reset, as defined in the startup configuration file

If you use this command after you reset the G350, both the Active and the Configured PMI should be the same IP address.

Use the following commands to configure other identification information:

- Use the **`set system contact`** command to set the contact information for the G350.
- Use the **`set system location`** command to set the location information for the G350.
- Use the **`set system name`** command to specify the name of the G350.

Defining the default gateway

The G350 uses a default gateway to connect to outside networks that are not listed on the G350'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.

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

ip default-gateway 132.55.4.45

The following example defines Serial interface 5/1:1 as the default gateway:

ip default-gateway Serial 5/1:1

Configuring the Media Gateway Controller (MGC)

This section provides information about configuring a Media Gateway Controller (MGC) to work with the G350 and includes the following topics:

- The Media Gateway Controller (MGC) — an overview of the types of MGCs that can be used with the G350
- Configuring the MGC list — instructions on how to register primary and backup MGCs for the G350
- Setting reset times — instructions on how to set time-outs for when the G350 has to reestablish a connection with its MGC
- Accessing the registered MGC — instructions on how to access the registered MGC using the CLI
- Monitoring the ICC or LSP — instructions on how to monitor the connection between the G350 and its registered MGC using the CLI

The Media Gateway Controller (MGC)

The Media Gateway Controller (MGC) controls telephone services on the Avaya G350 Media Gateway. You can use a media server with Avaya Communication Manager software as an MGC. The G350 supports both External Call Controllers (ECC) and Internal Call Controllers (ICC). An ICC is an Avaya S8300 Media Server that you install in the G350 as a media module. An ECC is an external media server that communicates with the G350 over the network.

Note:

When the G350 uses an ECC, it can use a local S8300 as a backup controller. The S8300 functions in Local Survivable Processor (LSP) mode. If the ECC stops serving the G350, the S8300 takes over the service.

Table 2: Media servers supported by the Avaya G350 Media Gateway on page 52 lists the media servers that can be used with the G350.

Table 2: Media servers supported by the Avaya G350 Media Gateway

Media server	Type	Usage
Avaya S8300 Media Server	Media module	ECC, ICC, or LSP
Avaya S8500 Media Server	External	ECC
Avaya S8700 Media Server	External	ECC

To register the G350 with an MGC, you need the G350's serial number. You can find this serial number in one of the following ways:

- Use the **`show system`** command.
- Look for a 12-character string located on a label on the back panel of the G350.

Configuring the MGC list

The G350 must be registered with an MGC in order to provide telephone service. Use the **`set mgc list`** command to set the G350's MGC. You can enter the IP addresses of up to four MGCs with the **`set mgc list`** command. The first MGC on the list is the primary MGC. The Avaya G350 Media Gateway searches for the primary MGC first. If it cannot connect to the primary MGC, it searches for the other MGCs on the list.

Note:

To register an S8500 or S8700 media server as the MGC, use the IP address of the media server's Control-LAN card (CLAN) rather than the IP address of the media server itself.

The following is an example of the **`set mgc list`** command:

```
G350-001> set mgc list 132.236.73.2, 132.236.73.3, 132.236,73.4,
132.236.73.5
```

If the media server with the IP address 132.236.73.2 is available, that media server becomes the G350's MGC. If that server is not available, the G350 searches for the next media server on the list, and so on.

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

- **Registered** — indicates whether or not the G350 is registered with an MGC (YES or NO).
- **Active Controller** — displays the IP address of the active MGC. If there is no active MGC (i.e., if the **`set mgc list`** command failed to configure an MGC), this field displays 255.255.255.255.
- **H248 Link Status** — indicates whether the communication link between the G350 and the MGC is up or down.
- **H248 Link Error Code** — if there is a communication failure between the G350 and the MGC, this field displays the error code.

To show the current MGC list, use the **`show mgc list`** command. This command shows the IP addresses of the MGCs on the MGC list.

To remove one or more MGCs from the MGC list, use the **`clear mgc list`** command. Type the IP address of the MGC you want to remove as an argument to remove that MGC. You can remove more than one MGC with one command by typing the IP addresses of all the MGCs you want to remove, separated by commas. To remove all the MGCs on the list, use the **`clear mgc list`** command with no arguments.

To change the G350's MGC list:

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

   Note:

   If you use the **`set mgc list`** command without first clearing the MGC list, the G350 simply adds the new MGCs to the end of the MGC list.

Setting reset times

If the connection between the G350 and its registered MGC is lost, the G350 attempts to recover the connection. Use the **set reset-times primary-search** command and the **set reset-times total-search** command to set the time-out for the G350's search for the primary MGC and the other MGC's on its MGC list, respectively. Use the **set reset-times transition-point** command to configure the point at which the primary MGCs in the list end and the LSPs begin. For example, if there are three IP addresses in the MGC list and the third address is the LSP, the transition point should be 2.

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

For example:

```
G350-001> set reset-times primary-search 20
G350-001> set reset-times total-search 40
350-001> set reset-times transition-point 1
```

In this example, in the event of a loss of connection with the registered MGC, the G350 searches for the primary MGC on its MGC list for 20 minutes. If the G350 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.

Use the **show recovery** command to show the status of MGC and ICC monitoring and recovery setup.

Accessing the registered MGC

To access the G350's registered MGC through the G350:

- If the MGC is an S8300 media server, use the **session mgc** command
- If the MGC is an S8500 or S8700 media server, use the **set mediaserver** command to manually define the MGC's IP address, then use the **session mgc** command to access the MGC

If the G350 includes an S8300, use the **session icc** command to access the S8300. You can use this command whether or not the local S8300 is the G350's registered MGC.

Note:

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

To open a connection directly to the Avaya Communication Manager System Access Terminal (SAT) application in the MGC, add **sat** to the command. For example:

```
G350-001> session mgc sat
```

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

```
G350-001> session mgc
```

Monitoring the ICC or LSP

When an MGC controls telephone services on the Avaya G350 Media Gateway in ICC or LSP mode, the G350 monitors the connection with the MGC. If the connection with the MGC is lost, the G350 starts a recovery process. Use the following commands to configure MGC monitoring:

- Use the **set icc-monitoring** command to control heartbeat monitoring of an ICC or LSP. 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/LSP monitoring process.

Viewing the status of the device

To view the status of the Avaya G350 Media Gateway, use the following commands. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **show faults** command to view information about currently active faults.
- Use the **show mgc** command to view information about the Media Gateway Controller with which the G350 is registered. For more information, see Configuring the Media Gateway Controller (MGC) on page 51.
- Use the **show mm** command to view information about media modules that are installed on the G350. 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

- Use the **`show module`** command or the **`show mg list`** command to view brief information about media modules that are installed in the G350. 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
- Use the **`show system`** command to display the serial number of the G350, the G350's uptime, the firmware version number, MAC addresses, and other system information.
- Use the **`show restart-log`** command to view information about the last time that the G350 was reset.
- Use the **`show temp`** command to view the temperature of the G350 CPU. This command also displays the high and low temperatures that will trigger a temperature warning.
- Use the **`show voltages`** command to view the power supply voltages of the G350.
- Use the **`show utilization`** command to display information about CPU and memory usage on the G350.

  Note:

  Before using this command, you must first use the **`set utilization cpu`** command to enable CPU utilization measurements.
- Use the **`test led`** command to test the system ALM and MDM and system CPU LEDs on the front panel of the G350. The CPU and media module LEDs blink for five seconds.

Version management

This section provides information about managing and upgrading software, firmware, configuration, and other files on the Avaya G350 Media Gateway and contains the following sections:

- File transfer — overview of transferring software and firmware files to the G350
- Software and firmware upgrades — instructions on how to upgrade software and firmware
- Managing configuration files — instructions on how to manage configuration files
- Listing the files on the Avaya G350 Media Gateway — instructions on how to display a list of G350 files and their version numbers

File transfer

The Avaya G350 Media Gateway can be a client for the FTP and TFTP protocols. Use the FTP or TFTP protocols to transfer files between the Avaya G350 Media Gateway and other devices. You can use file transfer to:

- Install software and firmware upgrades on the G350
- Install firmware upgrades on media modules
- Back up and restore configuration settings

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

Note:

If you use an FTP server, the G350 prompts you for a username and password when you enter a command to transfer a file. Also, when opening an FTP connection to the S8300, all anonymous FTP file transfers are restricted to the /pub directory. Permission for anonymous FTP users to create files in other directories is denied.

Software and firmware upgrades

You can upgrade software on the Avaya G350 Media Gateway. Software used to control the Avaya G350 Media Gateway itself and media modules installed on the G350 is called firmware. Use the FTP or TFTP protocol to upload a new version of software or firmware. You can upgrade the following types of software and firmware:

- Firmware for the Avaya G350 Media Gateway
- Java applet for Avaya G350 Manager
- Firmware for media modules

Note:

You can also use the G350 to upgrade the firmware and configuration files for IP phones. For details, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.

Managing the firmware banks

The G350 has two firmware banks:

- Bank A
- Bank B

Each firmware bank contains a version of the G350 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 G350 using the other version. This is particularly important when uploading new versions.

By default, when you turn on or reset the G350, the G350 loads firmware from Bank B. To change the default bank from which firmware is loaded during startup, type the **`set boot bank`** command. For example, to configure the G350 to load firmware from Bank A on startup, type **`set boot bank bank-A`**. After typing the **`set boot bank`** command, you must type the **`copy running-config startup-config`** command to save the change. Now, when you reset the G350, it will load firmware from Bank A.

You can use the ASB button on the G350 front panel to load firmware from the bank other than the default bank during startup:

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

For example, if the G350 is configured to load firmware from Bank B, use the steps listed above to reset the G350 to load the firmware from Bank A instead.

To display the bank from which the G350 is currently set to load its firmware upon startup or reset, type the **`show boot bank`** command.

Upgrading software and firmware

To upgrade software or firmware, you must obtain an upgrade file from Avaya. Place the file on your FTP or TFTP server. Then, use one of the following commands to upload the file to the G350. For each of these commands, include the full path of the file and the IP address of the FTP or TFTP host as parameters. When you enter the command, the CLI prompts you for a username and password.

Note:

In addition to using the CLI to upgrade software and firmware, you can use the Avaya IW and the GIW. See Configuring the G350 using the Avaya IW on page 389 and Configuring the G350 using the GIW on page 427.

- Use the **`copy ftp EW_archive`** command to upgrade the Java applet for Avaya G350 Manager software from an FTP server.
- Use the **`copy ftp module`** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an FTP server.
- Use the **`copy ftp SW_imageA`** command to upgrade the G350 firmware into Bank A from an FTP server.
- Use the **`copy ftp SW_imageB`** command to upgrade the G350 firmware into Bank B from an FTP server.

- Use the **`copy tftp EW_archive`** command to upgrade the Java applet for Avaya G350 Manager software from a TFTP server.
- Use the **`copy tftp module`** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from a TFTP server.
- Use the **`copy tftp SW_imageA`** command to upgrade the G350 firmware into Bank A from a TFTP server.
- Use the **`copy tftp SW_imageB`** command to upgrade the G350 firmware into Bank B from a TFTP server.
- Use the **`copy ftp EW_archive`** command to upgrade the Java applet for Avaya G350 Manager software from an FTP server.
- Use the **`copy ftp module`** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an FTP server.
- Use the **`copy ftp SW_imageA`** command to upgrade the G350 firmware into Bank A from an FTP server.
- Use the **`copy ftp SW_imageB`** command to upgrade the G350 firmware into Bank B from an FTP server.
- Use the **`copy tftp EW_archive`** command to upgrade the Java applet for Avaya G350 Manager software from a TFTP server.
- Use the **`copy tftp module`** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from a TFTP server.
- Use the **`copy tftp SW_imageA`** command to upgrade the G350 firmware into Bank A from a TFTP server.
- Use the **`copy tftp SW_imageB`** command to upgrade the G350 firmware into Bank B from a TFTP server.

When using FTP or TFTP commands, you must use the specific path to the file on the FTP or TFTP server according to the home directory of the service (FTP or TFTP) that you are using. For example, to upgrade the firmware of an MM312 media module in slot 3 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\mm312v51.fdl 192.1.1.10 3
```

Note:

When uploading firmware from the S8300, use only the file name, without the directory path, in the command line. Otherwise, the procedure will fail. For instance, in the example above, you must use the following command:
`copy tftp module mm312v51.fdl 192.1.1.10 3`

Note:

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

The following example uploads a firmware version with the path and file name C:\g350.net from an FTP server with the IP address 149.49.134.153 to Bank A of the G350:

```
copy ftp SW_imageA C:\g350.net 149.49.134.153
```

Managing configuration files

A configuration file is a data file that contains a complete set of configuration settings for the Avaya G350 Media Gateway. You can use configuration files to back up and restore the configuration of the G350. Use the FTP or TFTP protocol to transfer a configuration file between the G350 and a server on the network. You can back up either the running configuration or the startup configuration to the server as a configuration file. When you restore a configuration file from a server, it becomes the startup configuration on the G350. For more information about running configuration and startup configuration, see Configuration using GUI applications on page 25.

To transfer a configuration file between the G350 and a server on the network, use one of the following commands:

- Use the **`copy ftp startup-config`** command to restore a configuration file from an FTP server. The configuration file becomes the startup configuration on the G350.
- Use the **`copy tftp startup-config`** command to restore a configuration file from a TFTP server. The configuration file becomes the startup configuration on the G350.
- Use the **`copy running-config ftp`** command to back up the running configuration on the G350 to an FTP server.
- Use the **`copy running-config tftp`** command to back up the running configuration on the G350 to a TFTP server.
- Use the **`copy startup-config ftp`** command to back up the startup configuration on the G350 to an FTP server.
- Use the **`copy startup-config tftp`** command to back up the startup configuration on the G350 to a TFTP server.

Listing the files on the Avaya G350 Media Gateway

Use the **`dir`** command to list all G350 files. When you list the files, you can see the version numbers of the software components. The **`dir`** command also shows the booter file, which cannot be changed.

Chapter 5: Configuring Ethernet ports

This chapter provides information about configuring Ethernet ports on the Avaya G350 Media Gateway and contains the following sections:

- Ethernet ports on the G350 — a description of the Ethernet ports on the G350
- Configuring switch Ethernet ports — instructions on how to configure Ethernet ports on the G350 switch
- Configuring the WAN Ethernet port — instructions on how to configure the Ethernet port on the G350 router

Ethernet ports on the G350

The switch on the Avaya G350 Media Gateway has the following Ethernet ports:

- The 10/100 mbps fixed switch port on the front panel (port 10/3)
- The 10/100 mbps ports on the Avaya MM314 media module (ports 6/1 through 6/24)
- The Gigabit port on the Avaya MM314 media module (port 6/51)

Note:

The ports on the Avaya MM314 media module are only available if your G350 includes this media module.

The router on the Avaya G350 Media Gateway has the following Ethernet port:

- The 10/100 mbps fixed router port on the front panel (port 10/2)

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 G350, you can use either a standard network cable or a crossover network cable to connect any device.

Configuring switch Ethernet ports

For basic configuration of a switch Ethernet port, use the commands listed below. You can also configure the following features on a switch Ethernet port:

- Advanced switching features, including VLANs. For more information, see Chapter 13: Configuring advanced switching.
- VoIP queuing. To configure VoIP queuing on a switch port, configure a VLAN for the port. Then configure VoIP queuing on the VLAN. For more information about VoIP queuing, see Configuring QoS parameters on page 74.
- Access control policy lists and QoS policy lists. To configure policy lists on a switch port, configure a VLAN for the port. Then configure policy on the VLAN. For more information on policy lists, see Chapter 18: Configuring policy.
- SNMP Link Up and Link Down traps. For more information, see Configuring SNMP traps on page 125.

Switch Ethernet port commands

Use the following commands for basic configuration of switch Ethernet ports. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`set port auto-negotiation-flowcontrol-advertisement`** command to set the flowcontrol advertisement for the specified port when performing auto-negotiation. This command is only applicable to the Gigabit Ethernet port.
- Use the **`set port disable`** command to disable a port or range of ports.
- Use the **`set port duplex`** command to configure the duplex type of an Ethernet or Fast Ethernet port or range of ports.You can configure Ethernet and Fast Ethernet 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.
- Use the **`set port edge admin state`** command to set the administrative state the specified port is assumed to be in.
- Use the **`set port enable`** command to enable a port or a range of ports.
- Use the **`set port level`** command to determine the default packet priority level for untagged packets. Packets traveling through a port set at normal priority should be served only after packets traveling through a port set at high priority are served.
- Use the **`set port name`** command to configure a name for a port.

- Use the **`set port negotiation`** command to enable or disable the link negotiation protocol on the specified port. This command applies to Fast Ethernet or Gigabit Ethernet ports. When negotiation is enabled, the speed and duplex of the Fast Ethernet ports are determined by auto-negotiation. If negotiation is disabled, the user can set the speed and duplex of the Fast Ethernet ports.
- Use the **`set port point-to-point admin status`** command, followed by the module and port number of the port, to manage the connection type of the port. Use one of the following arguments with this command:
  - ***`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 G350 tries to automatically detect the connection type of the port
- Use the **`set port speed`** command to configure the speed of a port or range of ports. In auto-negotiation mode, the port's speed is determined by auto-negotiation. An error message is generated if you attempt to set the speed when auto-negotiation is enabled

Configuring the WAN Ethernet port

For basic configuration of the WAN Ethernet port:

1. Use the **`interface FastEthernet 10/2`** command to enter the context of the port interface.
2. Perform basic configuration of the interface. For more information, see Configuring interfaces on page 160.
3. Use the Ethernet WAN port configuration commands in the context of the port interface. See WAN Ethernet port commands on page 64.

You can also configure the following features on the WAN Ethernet port:

- Primary Management Interface (PMI). For more information, see Configuring the Primary Management Interface (PMI) on page 50.
- Advanced router features. For more information, see Chapter 16: Configuring the router.
- VoIP queuing. For more information, see Configuring QoS parameters on page 74.
- Access control policy lists and QoS policy lists. For more information, see Chapter 18: Configuring policy.
- SNMP Link Up and Link Down traps. For more information, see Configuring SNMP traps on page 125.

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. 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.

To disable traffic shaping, use the **no** form of the **traffic-shape rate** command.

For information on traffic shaping in general, see Configuring QoS parameters on page 74.

Backup interfaces

You can configure backup relations between a pair of any Layer 2 serial interfaces, including the Fast Ethernet interface. For instructions on how to configure backup interfaces, see Backup interfaces on page 97.

WAN Ethernet port commands

Use the following commands in FastEthernet 10/2 context for basic Ethernet configuration of the WAN Ethernet port:

- Use the **autoneg** command to set the port speed and duplex to auto-negotiation mode for the external FastEthernet port. Use the **no** form of this command to disable the auto-negotiation mode.
- Use the **duplex** command to control the duplex setting for the interface.
- Use the **shutdown** command to set the administrative status of the current interface to down. Use the **no** form of this command to restore the administrative status of the interface to up.
- Use the **speed** command to set the port speed.

Chapter 6: Configuring logging

This chapter provides information on G350 system logging and contains the following sections:

- Logging overview — overview of the G350 logging process
- Syslog server — instructions on how to enable and disable Syslog servers
- Logging file — instructions on how to enable and disable message logging to non-volatile memory, and how to display and delete the log file
- Logging session — instructions on how to enable and disable the display of logging messages to your screen
- Filters and severity levels — instructions on how to filter logging messages

Logging overview

The Avaya G350 Media 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. You can define filters for each sink to limit the types of messages the sink receives.

Table 3: Logging sinks

Sink	Description
Session	Logging messages are sent to the terminal screen. This sink is disabled whenever a session ends, and remains disabled until the user enables it.
Log file	Logging data is saved in the flash memory. These files serve as the system logging database.
Syslog	Logging messages are sent to up to three configured servers, using Syslog protocol.

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 you reset the G350, the Session sink is disabled, even if you enabled it during the session. The other sinks retain whatever setting they had before the reset, as long as you have saved the running configuring to the startup configuration using the **`copy running-config startup-config`** command. Filters are not disabled when you reset the G350.

Syslog server

A Syslog server is a remote server that receives logging messages using Syslog protocol. This enables storage of large log files, which you can use to generate reports. You can define up to three Syslog servers.

To define and configure a Syslog server:

1. To define the Syslog server, type the **`set logging server`** command, followed by the IP address of the server.
2. To enable the Syslog server, type the **`set logging server enable command`**, followed by the IP address of the Syslog server. When you define a new Syslog server, it is defined as disabled, so you must use this command in order to enable the server.
3. To define an output facility for the Syslog server, type the **`set logging server facility`** command, followed by the name of the output facility and the IP address of the Syslog server. (This step is optional.) The following is a list of possible facilities:

   auth (Authorization)
   daemon (Background System Process)
   clkd (Clock Daemon)
   clkd2 (Clock Daemon)
   mail (Electronic Mail)
   local0 – local7 (For Local Use)
   ftpd (FTP Daemon)
   kern (Kernel)
   alert (Log Alert)
   audi (Log Audit)
   ntp (NTP Subsystem)
   lpr (Printing)
   sec (Security)
   syslog (System Logging)
   uucp (Unix-to-Unix Copy Program)
   news (Usenet news)
   user (User Process)

   The following example defines the FTP Daemon as the output facility for Syslog reports generated by the Syslog server with the IP address 168.12.1.15:

   ```
   set logging server facility ftpd 168.12.1.15
   ```

4. To limit access to the Syslog server output, type the **`set logging server access-level`** command, followed by an access level (read-only, read-write, or admin). Only messages with the appropriate access level are sent to the Syslog output.

To disable a Syslog server, type the **`set logging server disable`** command, followed by the IP address of the Syslog server.

To delete a Syslog server from the Syslog server table, type the **`clear logging server`** command, followed by the IP address of the Syslog server you want to delete.

To display the status of a Syslog server, use the **`show logging server condition`** command, 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 G350. This command displays whether the server is enabled or disabled, and lists all filters defined on the server.

The Syslog sink has the following default settings:

- **Severity** — warning
- **Facility** — local 7
- **Access level** — read-write

Logging file

To enable the logging of system messages to a log file in the flash memory, type the **`set logging file enable`** command. To disable the logging of system messages to a log file, type the **`set logging file disable`** command.

To delete the current log file and open an empty log file, type the **`clear logging file content`** command.

To display messages in the log file, type the **`show logging file content`** command. You can filter this command by severity per application. See Filters and severity levels on page 68. You can also limit the number of messages to display. The following example displays the 50 most recent QoS messages with a severity level of Critical or higher:

```
show logging file content qos critical 50
```

Logging session

To start the display of system messages to the terminal screen, type the **`set logging session enable`** command. To discontinue the display of system messages to the terminal screen, type the **`set logging session disable`** command.

To display how session logging is configured, type the **`show logging session condition`** command. This command displays whether session logging is enabled or disabled, and lists all filters defined for session logging.

Filters and severity levels

You can use filtering options to reduce the number of collected and transmitted messages. The filtering options are based on message classification by application and severity. For a specified sink, you can define the threshold severity for message output for each application. Messages with a severity lower than the defined threshold are sent to the specified sink, and those with a higher severity than the defined threshold are not sent.

Table 4 lists the eight available severity levels.

Table 4: Severity levels

Severity level	Code	Description
Emergency	0	System is unusable
Alert	1	Immediate action required
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

To configure a filter that will eliminate all messages for the specified application, type **none** instead of a severity level.

The sinks have the following default severity levels:

- **Session** — warning
- **Log file** — informational
- **Syslog** — warning

Filters are defined per application. Table 5: Logging applications on page 69 lists the applications for which you can define filters.

Table 5: Logging applications *1 of 2*

Application	Description
boot	System startup failures
cascade	Stack CASCADE mechanism
cli	CLI
config	Configuration changes
console	Serial modem messages
dhcps	DHCP server package
fan	Cooling system
filesys	File system problem (flash)
ipsec	VPN package
isakmp	ISAKMP protocol
lag	Link Aggregation package
poe	Power over Ethernet
policy	Policy package
ppp	PPP protocol
pppoe	PPP over Ethernet
qos	QoS messages
router	Core routing system failures
snmp	SNMP agent
stp	Spanning tree package
supply	Power supply system
switchfabric	Switch fabric failures
system	Operating system failures
threshold	RMON alarms
usb-modem	USB modem messages
vlan	VLAN package
	1 of 2

Table 5: Logging applications *2 of 2*

Application	Description
voice	Voice failures
wan	WAN plugged-in expansion
	2 of 2

To define a filter that applies to every application, type **`all`** instead of the application.

Use the **`set logging file condition`** command to create a filter for system messages that are logged to a log file. The following example defines a filter in which QoS messages with a severity level of Critical or higher are sent to the log file:

```
set logging file condition qos critical
```

Use the **`set logging session condition`** command to create a filter for system messages that are displayed on the terminal screen. The following example defines a filter in which all messages with a severity level of Warning or higher are displayed on the screen:

```
set logging session condition all warning
```

Use the **`set logging server condition`** command to create a filter for system messages that are logged to the specified Syslog server. In addition to the application and severity level, you must specify the IP address of the Syslog server to which you want to apply the filter. The following example defines a filter in which no RIP messages are sent to the Syslog server with the IP address 175.5.16.33:

```
set logging server condition rip none 175.5.16.33
```

Chapter 7: Configuring VoIP QoS

This chapter provides information about configuring VoIP on the G350 and contains the following sections:

- VoIP overview — an overview of G350 VoIP configuration
- Configuring RTP and RTCP — instructions on how to configure RTP and RTCP protocols on the G350
- Configuring QoS parameters — instructions on how to configure MGP QoS parameters on the G350
- Configuring RTCP QoS parameters — instructions on how to configure RTP QoS parameters on the G350
- Configuring RSVP parameters — instructions on how to configure RSVP protocol on the G350
- Configuring Weighted Fair VoIP Queuing (WFVQ) — instructions on how to configure VoIP queueing.

VoIP overview

The Avaya G350 Media Gateway provides voice services over IP data networks using VoIP. VoIP is a group of protocols for transmitting and receiving various types of voice data over an IP network. VoIP includes protocols for transmitting and receiving the following types of information:

- Digitally encoded voice data
- Call signalling information
- Call routing information
- QoS information

VoIP uses the RTP and RTCP protocols to transmit and receive digitally encoded voice data. For more information about configuring RTP and RTCP on the Avaya G350 Media Gateway, see Configuring RTP and RTCP on page 72.

You can use many types of telephones and trunks that do not directly support VoIP. The Avaya G350 Media Gateway translates voice and signalling data between VoIP and the system used by the telephones and trunks.

Configuring RTP and RTCP

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.

Use the **`ip rtp port-range`** command to configure the range of UDP ports for RTP.

Note:

This range should match the range configured in the IP_network region to which the G350 is assigned in the ACM.

Configuring RTP header compression

Use RTP header compression to reduce the amount of bandwidth needed for voice data. The G350 RTP Header Compression process is based on the following:

- The packet order on a PPP and Frame Relay link is preserved.
- After transmitting full headers, usually only the deltas from the full packet's header need to be sent, and not the full header itself. This is due to the IP, UDP, and RTP header structure.
- Since the deltas are often constant, the second order delta is 0 and does not need to be transmitted.

You can configure how often the full header is transmitted, either as a function of time or transmitted compressed packets.

RTP Header Compression can reduce the size of all three headers (IP+UDP+RTP~40 bytes) to 2-4 bytes.

The G350 can only compress RTP packets. Any UDP packet with an even destination port within a user-configurable range of ports, is considered an RTP packet.

The G350 can decompress any type of compressed packets. Decompression is enabled whenever RTP compression is enabled.

Use the following commands to configure RTP header compression:

- Use the **`clear ip rtp header-compression`** command to clear RTP header compression statistics either 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. There is no renegotiation of parameters.
- Use the **`ip rtp compression-connections`** command to control the number of RTP connections supported on this interface. Use the **no** form of this command to restore the default. This command also sets the number of connections in the non-TCP space, not just RTP.

Note:

This command automatically enables TCP header decompression on this interface.

- Use the **`ip rtp max-period`** command to set the maximum number of compressed headers that can be sent between full headers.
- Use the **`ip rtp max-time`** command to set the maximum number of seconds between full headers.
- Use the **`ip rtp non-tcp-mode`** command to set the header compression mode. 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.

  Note:

  IETF mode is not compatible with non-IETF mode.

- Use the **`ip rtp port-range`** command to configure the range of UDP ports for RTP.
- By default, the G350 decompresses up to 16 compressed TCP connections. You can modify this number (within the range of 3-256) using the **`ip tcp decompression-connections`** command. Use the **`no`** form of this command to restore the default. This command only exists in a PPP encapsulated interface.

  Note:

  The G350 is currently not capable of actively compressing TCP connections. It decompresses TCP connections compressed on the other side of the link.

- Use the **`show ip rtp header-compression`** command to display the RTP header compression statistics for a specific interface. If no interface is specified, statistics for all interfaces are displayed.

Configuring QoS parameters

The G350 uses MGCP (H248) protocol for call signalling and call routing information. Use the following commands to configure QoS for signalling and VoIP traffic. For more information about these commands, including parameters and default settings, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`set qos control`** command to define the source for QoS control parameters. The source can be either **`local`** where the user configures the values locally on the G350, or **`remote`** in which case the values are obtained from the G350's registered MGC.
- Use the **`set qos bearer`** command to provide the means to set up QoS parameters for the VoIP bearer.

  Note:

  The parameters you define using the **`set qos bearer`** command may conflict with the default QoS list (400). This causes the 801.2p for VoIP packets to differ from settings configured in the QoS list. To avoid this problem, perform the following steps:

  1. Create a new QoS list.
  2. In the new QoS list, either
     - Set the default IP rule composite operation to No Change, OR
     - Configure the DSCP map according to the QoS parameters you defined using the **`set qos bearer`** command. For instructions on creating a QoS list, see QoS lists on page 254.
- Use the **`set qos signal`** command to provide the means to set up QoS parameters for MGCP (H248) communication with the MGC.
- Use the **`voip-queue-delay`** command to set the maximum queue delay for which to estimate the high priority queue size necessary to meet the queuing delay for a specific VoIP codec. To determine the queue size you currently have, use the **`show queueing`** command.
- Use the **`show qos`** command to display the local and downloaded QoS parameters.

Configuring RTCP QoS parameters

Use the following commands to configure QoS monitoring for RTCP:

- Use the **`set qos rtcp`** command to permit the setup of RTCP parameters. The parameters that can be set are enabling or disabling RTCP reporting capability, setting the IP address of the monitor, setting the reporting period (the default is 5 sec.), and defining the listening port number.
- Use the **`show qos-rtcp`** command to display QoS, RSVP, and RTCP parameters.

Configuring RSVP parameters

VoIP uses the RSVP protocol to reserve network resources for voice data while communicating with other media gateways and other VoIP entities, such as IP phones and Softphones.

- Use the **`set qos rsvp`** command to set the current values for the RSVP parameters of the VoIP engines. The parameters that can be set are enabled/disabled, refresh rate (seconds), failure retry (y or n), and service profile (Guaranteed or Controlled).
- Use the **`show qos-rtcp`** command to display QoS, RSVP, and RTCP parameters.

Configuring Weighted Fair VoIP Queuing (WFVQ)

Weighted Fair VoIP Queuing (WFVQ) combines weighted fair queuing (WFQ) for data streams and priority VoIP queuing to provide the real-time response time that is required for VoIP.

WFQ is applied to data streams to provide fair bandwidth distribution among different data streams, with faster response times for shorter packets that are typical for interactive applications such as telnet. Priority VoIP queuing is applied to VoIP bearer and signaling traffic.

WFVQ is the default queuing mode for all Serial interfaces and all Fast Ethernet interfaces for which traffic-shaping is enabled. To disable WFVQ, you must enable another queuing mode, using either the **`voip-queue`** or the **`priority-queue`** command in interface context. To re-enable WFVQ, use the **`fair-voip-queue`** command in interface context. WFVQ is the recommended queuing mode.

Note:

There is no **`no`** form of the **`fair-voip-queue`** command. If you enter the command **`no fair-voip-queue`**, it will actually enable WFVQ if WFVQ is not already enabled.

Use the following commands to set the WFVQ queuing parameters.

- Use the **`voip-queue-delay`** command to set the maximum query delay. To determine the queue size you currently have, use the **`show queueing`** command.
- Use the **`fair-queue-limit`** command to 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.

  Note:

  This command should generally be used only for troubleshooting.

Chapter 8: Configuring the G350 for modem use

You can connect either a USB or a serial modem to the Avaya G350 Media Gateway. A USB modem must be connected to the USB port on the G350 chassis. A serial modem must be connected to the console port (CONSOLE) on the G350 chassis.

Both the USB port and the CONSOLE port require configuration for modem use. You can configure the ports for modem use via the Avaya IW (see Configuring the G350 using the Avaya IW on page 389) or the GIW (see Configuring the G350 using the GIW on page 427). For details on using a modem with the G350, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.

This chapter explains how to use the CLI to configure the console and USB ports for modem use.

Configuring the USB port for modem use

By default, the USB port is not enabled. To enable the USB port, you must enable the USB interface. Use the **`interface usb-modem`** command to enable the USB interface. Use the **`no`** form of this command to disable the USB interface. The **`no`** form of the **`interface usb-modem`** command also resets the interface to its default parameter values. These values are:

- **Interface status** — down
- **IP address** — 10.3.0.3
- **Netmask** — 255.255.255.0
- **PPP timeout** — None
- **PPP speed** — 38,400 bps

To set the USB port's parameters, use the following commands in USB interface context:

- Use the **`async reset-modem`** command to reset the connected modem. You can use this command from within an active PPP session over the USB modem.
- Use the **`speed`** command to set the PPP baud rate to be used by the USB port when connected to a modem (in bits per second). Options are 9600, 19200, and 38400.
- Use the **`ip address`** command to assign an IP address and mask to the USB port. This is the IP address to which a remote user can connect using telnet. For example, to assign the IP address 192.168.22.33 with mask 255.255.255.0 to the USB port, use the following command:

  ```
  G350-001(if:USB)# ip address 192.168.22.33 255.255.255.0
  ```

  The default IP address of the USB port is 10.3.0.3 with the mask 255.255.255.0.

- Use the **`ppp authentication`** command to decide the authentication method used when starting a client session on the PPP server. Use this command with one 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.
  - ***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 interface context.
- Use the **`shutdown`** command to disconnect a session.
- Use the **`timeout absolute`** command to set the number of minutes until the system automatically disconnects an idle PPP incoming session. By default, there is no timeout.
- Use the **`show interface usb-modem`** command to display the USB interface parameters, the current status of the USB port, and the identity of any USB modem connected to the USB port.

Configuring the console port for modem use

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. For more information, see Accessing the CLI on page 27.

You can set the console port so that it automatically detects whether a console device or a modem is connected to it. Use the **`async mode interactive`** command 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, use the **`async mode terminal`** command to disable interactive mode.

Note:

By default, async mode is set to ***`terminal`***.

Use the following commands to configure the console port for use with a modem:

- Use the **`async reset-modem`** command to reset the connected modem.
- Use the **`speed`** command to set the PPP baud rate to be used by the console port when connected to a modem (in bits per second). Options are 9600, 19200, and 38400.

- Use the **`async modem-type`** command to configure the console port for the modem type you want to use. By default, the console port is set to work with MultiTech modems. Set this command to **null** to use any modem type other than MultiTech.
- Use the **`interface console`** command to enter the console interface configuration mode. Use the **no** form of this command to set the console parameters to their default values.
- Use the **`ip address`** command to assign an IP address and mask to the console port. This is the IP address to which a remote user can connect using telnet. For example, to assign the IP address 192.168.22.33 with mask 255.255.255.0 to the console port, use the following command:
  `G350-001(if:Console)# ip address 192.168.22.33 255.255.255.0`
  The default IP address of the console port is 10.3.0.1 with the mask 255.255.255.0.
- Use the **`ppp authentication`** command to decide the authentication method used when starting a client session on the PPP server. Use this command with one 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.
  - ***none*** — no password is sent.

  Note:

  This command changes the PPP authentication parameters of the USB port as well as the CONSOLE port, even if you use the command in console interface context.
- Use the **`shutdown`** command to disconnect a session.
- Use the **`timeout absolute`** command to set the number of minutes until the system automatically disconnects an idle PPP incoming session. By default, there is no timeout.

When you use a console device to access the CLI through the console port, you must configure the serial connection on the console device to match the configuration of the console port. The console port uses the following settings:

- **baud** — 9600
- **data bits** — 8
- **parity** — none
- **stop bits** — 1
- **flow control** — hardware

Chapter 9: Configuring a WAN Interface

This chapter provides information about configuring WAN features on the Avaya G350 Media Gateway and contains the following sections:

- WAN overview — a description of the WAN features supported on the G350
- Serial interface overview — an overview of serial interfaces
- Initial WAN configuration — instructions on how to configure a WAN line on the G350
- Backup interfaces — a description of backup interfaces and how they work on the G350
- Extended keepalive — a description of the keepalive feature for sending ping packets through an interface at defined intervals to determine if the interface is up or down
- Dynamic CAC — a description of dynamic CAC and how to configure dynamic CAC on a WAN interface
- Frame relay encapsulation — a description of the frame relay encapsulation features supported on the G350
- Priority DLCI — a description of class-based traffic assignment (priority DLCI) and how to configure priority DLCI on a WAN interface
- WAN configuration example — an example of a WAN configuration on the G350

WAN overview

You can use an MM340 E1/T1 media module or an MM342 USP media module as an endpoint for a WAN line. You can also use the Fast Ethernet port on the G350 chassis as the endpoint for a WAN line by configuring the Fast Ethernet interface for PPP over Ethernet (PPPoE). The G350 serves as a router, as well as the endpoint, for the WAN line. For more information about routing, see Configuring the router on page 159.

The G350 supports the following WAN features:

- PPP over channeled and fractional E1/T1 — the G350 has the ability to map several PPP sessions to a single E1/T1 interface
- PPP over USP
- PPPoE
- Unframed E1 for enabling full 2.048 Mbps bandwidth usage
- Point-to-Point frame relay encapsulation over channelized, fractional, or unframed E1/T1 ports or over a USP interface

- Frame relay — the G350 supports the following LMI types:
  - ANSI (Annex D)
  - ITU-T:Q-933 (Annex A0)
  - LMI-Rev1
  - No LMI
- Backup functionality supported between any type of Serial Layer 2 interface. For more information, see Backup interfaces on page 97.
- Dynamic CAC for Fast Ethernet, Serial, and GRE tunnel interfaces. For more information, see Dynamic CAC on page 101.
- Quality of Service (QoS) — the G350 uses Weighted Fair VoIP Queuing (WFVQ) as the default queuing mode for WAN interfaces. 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. The G350 also supports the VoIP Queue and Priority Queue legacy queuing methods. For more information, see Configuring Weighted Fair VoIP Queuing (WFVQ) on page 76.
- Policy — each interface on the G350 can have four active policy lists:
  - Ingress Access Control List
  - Ingress QoS List
  - Egress Access Control List
  - Egress QoS List

  Access control lists define which packets should be forwarded or denied access to the network. QoS lists change the DSCP and 802.1p priority of routed packets according to the packet characteristics. For more information, see Configuring policy on page 253.

  Each interface on the G350 can also have an active policy-based routing list. For more information, see Chapter 19: Configuring policy-based routing on page 273.
- RTP Header Compression — use of RTP compression can save up to 60% of the interface's bandwidth. RTP compression also enhances the efficiency of voice transmission over the network by compressing the headers of Real Time Protocol (RTP) packets, thereby minimizing the overhead and delays involved in RTP implementation. For more information, see Configuring RTP header compression on page 72.

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.

Figure 1: Layer 1 T1 Port on page 83 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.

Figure 1: Layer 1 T1 Port

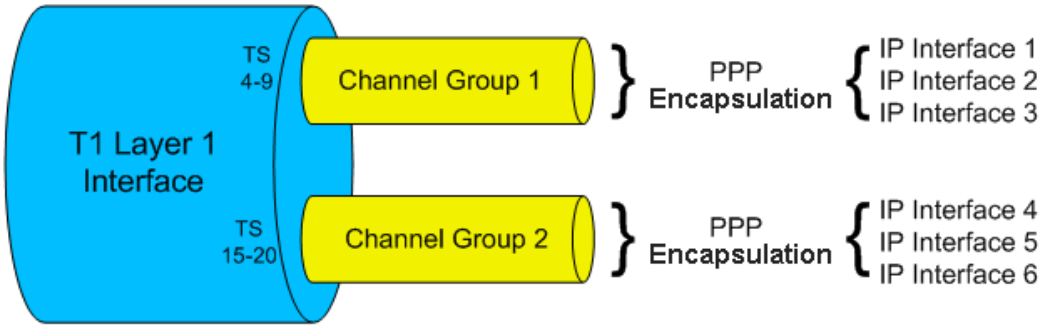


Figure 2: E1/T1 Port Channel Group on page 83 illustrates an E1/T1 port Channel Group. All data from the Channel Group is encapsulated using frame relay protocol. The data is sent via a frame relay serial interface and Sub-interfaces over the multiple IP interfaces defined using Data Link Connection Identifier (DLCI).

Figure 2: E1/T1 Port Channel Group

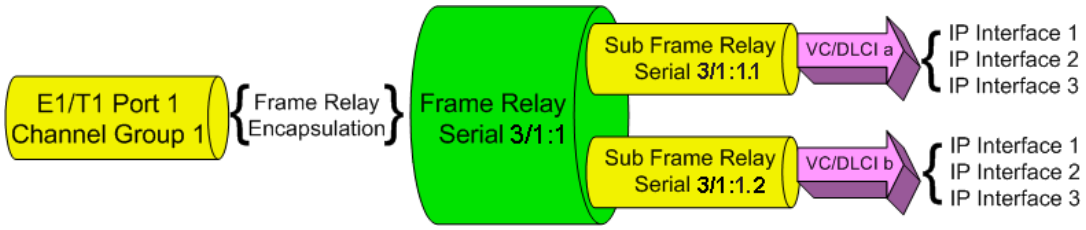


Figure 3: USP Port - PPP Protocol on page 84 illustrates a USP port. All data from the USP port is encapsulated using the PPP protocol, and is sent via a serial interface over the multiple IP interfaces defined for the Serial interface.

Figure 3: USP Port - PPP Protocol

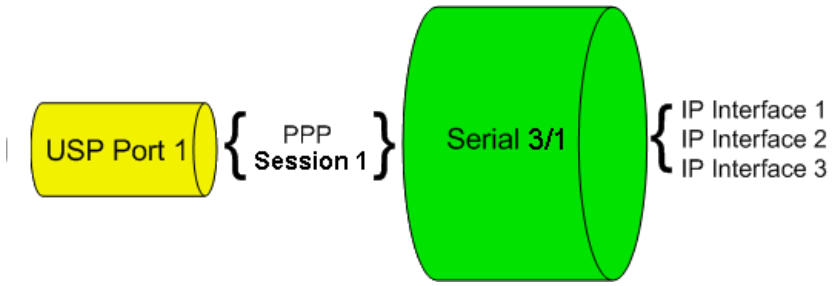
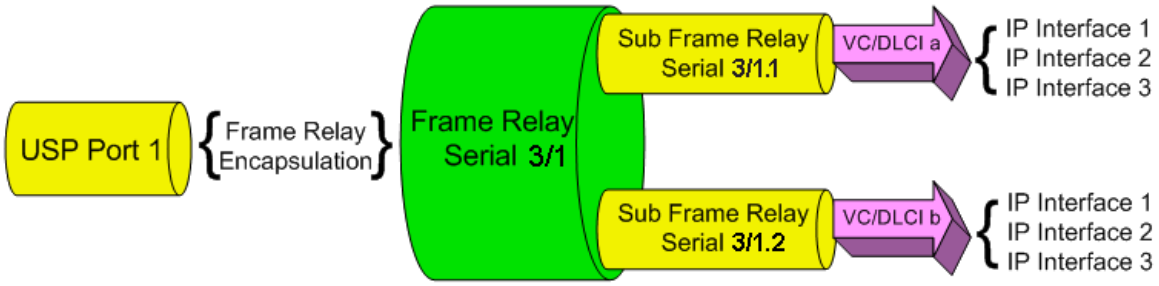


Figure 4: USP Port - Frame Relay Protocol on page 84 illustrates a USP port. All data from the USP port is encapsulated using the frame relay protocol, and is sent via a frame relay serial interface and sub-interfaces over the single IP interfaces defined using DLCI.

Figure 4: USP Port - Frame Relay Protocol



Frame Relay multipoint topology support

The Avaya G350 Media Gateway supports point-to-point frame relay connections. To enable you to use the G350 as an endpoint in a Point to Multi-Point (PTMP) topology, the G350 supports inverse ARP replies. The G350 responds to inverse ARP queries received on frame relay sub-interfaces with the proper inverse ARP replies.

When you connect the G350 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 Interface Serial 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

For more information on OSPF, see Configuring OSPF on page 194.

Initial WAN configuration

To configure the Avaya G350 Media Gateway to support a WAN:

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 G350 chassis as the endpoint for a WAN line by configuring this interface for PPPoE. See Configuring PPPoE on page 91.
2. Connect the WAN line to the media module. For more information, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.
3. Configure the WAN interface on the WAN media module:
   - For the MM340, see Configuring the Avaya MM340 E1/T1 WAN media module on page 85.
   - For the MM342, see Configuring the Avaya MM342 USP WAN media module on page 88.
4. By default, a G350 WAN interface uses Point-to-Point Protocol (PPP). For instructions on changing the default PPP parameters, see Configuring PPP on page 90.
5. If you want frame relay encapsulation on the WAN, configure frame relay. See Configuring frame relay on page 95.
6. Test the WAN configuration. See Verifying the WAN configuration and testing connectivity on page 96.
7. Use the **`copy running-config startup-config`** command to save the configuration.

Configuring the Avaya MM340 E1/T1 WAN media module

For a list of G350 default settings, see E1/T1 default settings on page 88. To display the current settings, use the **`show controllers`** command.

To configure an E1 or T1 port:

1. Use the **`show-ds`** command to check if the G350 is configured for E1 or T1 operation.
2. Use the **`ds-mode`** command to set the mode of the G350 to E1 or T1. Changing the line type requires resetting the module. The default value is T1.

3. Use the **controller <ds-mode> <slot/port>** command to enter controller context for the port to be configured. The prompt changes to:

   `G350-001(super-if:Serial s/p)#`

   where *s* is the slot number of the media module, and *p* is the port number.

4. 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 gain26, 0db). If the cable is 655 feet or less, use the command **cablelength short {133ft | 266ft | 399ft | 533ft | 655ft}** (default 133ft). When using the **cablelength short** form of the command, the transmit attenuation is configured using the loop length.

   - For E1 mode:

     clock source {line|internal} (default is line)

     framing {crc4|no-crc4|unframed} (default is crc4)

     linecode {ami|hdb3} (default is hdb3)

5. Use the **channel-group** command to specify the channel group and time slots to be mapped, as well as the DS0 speed. For 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.

6. Type **exit** to return to general context. The prompt returns to:

   `G350-001(super)#`

7. Use the **`interface Serial`** command to enter the context of the interface. 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 G350 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 4/1:1`** enters a serial interface on the media module in slot number 4, on port number 1, with channel group number 1.
   - **`interface Serial 5/1:2.3`** enters a serial interface on the media module in slot number 5, 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 3 for an E1 port, a channel group is automatically created on the entire E1 bandwidth. The channel group has the number 0. In Step 6, use the command **`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.

8. Configure the interface encapsulation:
   - By default, the serial interface uses PPP encapsulation. For information on setting PPP parameters, or instructions on returning the interface to the default PPP encapsulation after it has been configured for a different encapsulation, see Configuring PPP on page 90.
   - For frame relay encapsulation, see Configuring frame relay on page 95.
9. Use the **`ip address`** command to configure the IP address and subnet mask of the interface.
10. Type **`exit`** to return to general context. The prompt returns to:

    `G350-001(super)#`

11. If needed, repeat Step 7 through Step 9 to configure additional IP interfaces on the same channel group.
12. If needed, repeat Step 5 through Step 9 to configure additional channel groups on the same E1 or T1 port.
13. Test the WAN configuration. See Verifying the WAN configuration and testing connectivity on page 96.
14. Use the **`copy running-config startup-config`** command to save the configuration.

E1/T1 default settings

Table 6: E1/T1 default settings on page 88 shows the default settings for E1/T1 WAN lines on the G350:

Table 6: E1/T1 default settings

Function	Default setting
DS mode	T1
E1 framing	CRC4
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

Configuring the Avaya MM342 USP WAN media module

For a list of the USP default settings, see USP default settings on page 90.

To configure USP ports:

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 G350 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 4/1`** enters a serial interface on the media module in slot number 4, on port number 1.
   - **`interface Serial 5/1.2`** enters a serial interface on the media module in slot number 5, on port number 1, with IP interface number 2.

   The prompt changes to:

   ```
   G350-001(super-if:Serial s/p)#
   ```

   For example:

   ```
   G350-001(super-if:Serial 4/1)#
   ```

2. Use the following commands to change the idle characters, transmitter delay, encoding type, bandwidth parameters, line monitoring, and from their default settings:
   - **`idle characters {flags|marks}`** sets 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}`** sets 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 G350, or the router on the WAN have a receive buffer that is not large enough to hold the traffic sent by the G350. 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 G350.

   - **`nrzi-encoding`** enables 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}`** sets 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`** specifies 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`** inverts 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:
   - For PPP encapsulation, see Configuring PPP on page 90.
   - For frame relay encapsulation, see Configuring frame relay on page 95.
4. Type **`exit`** to return to general context. The prompt returns to:

   `G350-001(super)#`
5. Repeat Step 1 to configure additional serial interfaces on the USP port.
6. Test the WAN configuration. See Verifying the WAN configuration and testing connectivity on page 96.
7. Use the **`copy running-config startup-config`** command to save the configuration.

USP default settings

Table 7 shows the default settings for USP WAN lines on the G350:

Table 7: USP default settings

Function	Default setting
Encoding	NRZ
Bandwidth	2048 kbps
Line-up indicator signal	DCD

Configuring PPP

By default, 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:

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, use the **`encapsulation ppp`** command to change the encapsulation to PPP.
3. If you want to change the queuing mode of the interface, see Configuring Weighted Fair VoIP Queuing (WFVQ) on page 76 for instructions.
4. Use the following commands to change the interface parameters:
   - Use the **`ip address`** command to configure the IP address and subnet mask of the interface.
   - Use the **`ppp timeout ncp`** command to set the maximum time to wait for the network layer to negotiate. If this time is exceeded, the G350 restarts the PPP session.
   - Use the **`ppp timeout retry`** command to set the maximum time to wait for a response during PPP negotiation.
   - Use the **`keepalive`** command to 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. Type **exit** to return to general context. The prompt returns to:

   `G350-001(super)#`

6. Test the WAN configuration. See Verifying the WAN configuration and testing connectivity on page 96.
7. Use the **`copy running-config startup-config`** command to save the configuration.

Configuring PPPoE

You can configure the ETH WAN Fast Ethernet port as a WAN port using PPPoE (PPP over Ethernet). PPPoE offers dialup style authentication and accounting and allows subscribers to dynamically select their ISP.

Note:

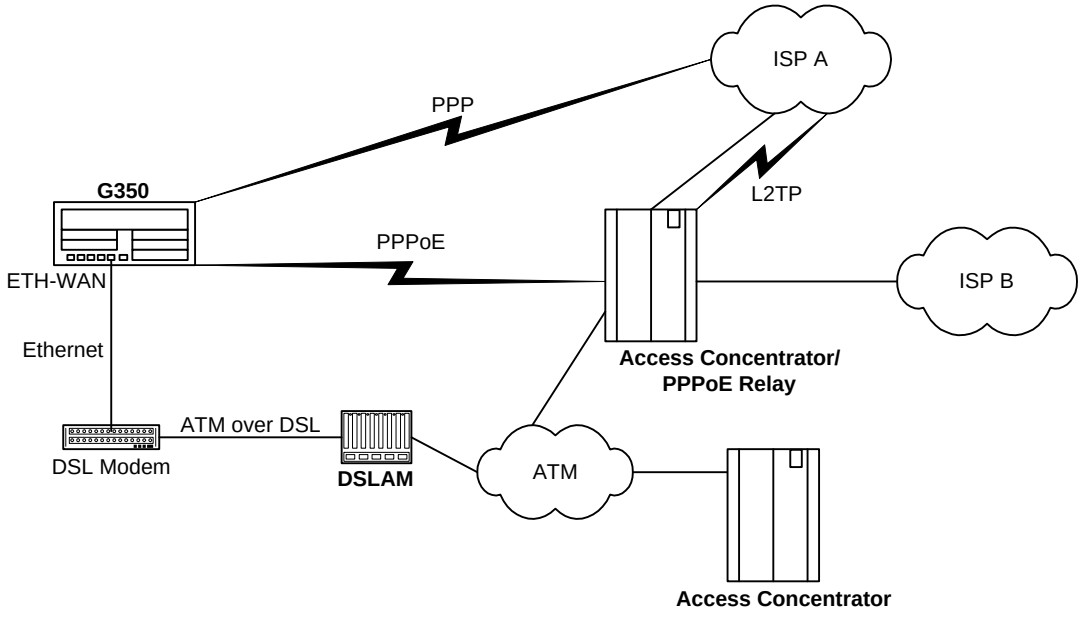
Version 2.2 does not support dynamic PPP address assignment from the remote peer.

PPPoE overview

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 G350) and an access concentrator. This enables the use of PPP authentication protocols (CHAP and PAP). Unlike other tunneling protocols such as L2TP and PPTP, PPPoE works directly over Ethernet rather than IP.

A typical broadband access network is based on aDSL modems configured as transparent Ethernet bridges. aDSL modems use ATM protocol, and the transparent bridging is done to a well known ATM VC. On the other side of the telephone line is a device called a DSLAM. The DSLAM terminates the aDSL physical layer, collects the ATM cells from the various aDSL subscribers, and places them on the SP ATM infrastructure. The Ethernet frames from the customer's host device can reach one or more access concentrators, which are the remote access servers.

Figure 5: Typical PPPoE Network Topology



PPPoE configuration

To configure PPPoE on the Fast Ethernet port:

1. Enter the context of the Fast Ethernet interface, using the command **`interface FastEthernet 10/2`**.
2. Use the **`encapsulation pppoe`** command 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 is configured on the interface
   - Dynamic CAC is enabled on the Fast Ethernet interface. See Dynamic CAC on page 101.
   - The interface is part of a primary-backup interface pair. See Backup interfaces on page 97.
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.

4. Configure an authentication method and parameters:
   - For PAP authenticating, type the **ppp pap-sent** command, followed by a username and password. For example:

```
G350-001(super-if:FastEthernet 10/2)# ppp pap-sent username avaya32 password 123456
Done!
```

   - For CHAP authentication, use the **ppp chap hostname** command, followed by a hostname, and the **ppp chap password** command, followed by a password. For example:

```
G350-001(super-if:FastEthernet 10/2)# ppp chap hostname avaya32
Done!
G350-001(super-if:FastEthernet 10/2)# ppp chap password 123456
Done!
```

Note:

Authentication parameters do not appear in the startup or running configuration files. You can use the **show ppp authentication** command to view authentication status. The **copy running-config startup-config** command stores authentication parameters in NVRAM.

5. You can use the following commands to change the interface parameters:
   - Use the **pppoe-client service name {name}**command to force the PPPoE client to connect only to access concentrators that support a specific service name. Use the **no** form of this command to deactivate connection to a specific service name. When connection to a specific service name is deactivated, the PPPoe client attempts to automatically discover the service name by initiating PADI frames with a blank service name.
   - Use the **mtu** command to set the interface's MTU to 1492. Since the header size of PPPoE packets is 8 bytes, setting the MTU to 1492 ensures that the overall packet size for the PPPoE interface will not exceed 1500, which is the MTU for Ethernet.
   - Use the **pppoe-client wait-for-ipcp** command to 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.
   - Use the **pppoe-client persistent delay** command to set the interval between pppoe-client dial attempts.
   - Use the **pppoe-client persistent max-attempts** command to limit the number of consecutive connection establishment retries. When this number is reached, the PPPoE client stops trying to establish connections. To have the PPPoE client resume

trying to establish connections, use the **shutdown** command to shut down the interface, followed by the **no shutdown** command to reopen the interface.

```
G350-001(super)# interface FastEthernet 10/2
G350-001(super-if:FastEthernet 10/2)#
G350-001(super-if:FastEthernet 10/2)# shutdown

Interface FastEthernet 10/2, changed state to administratively down
Line protocol on FastEthernet 10/2, changed state to down
Done!

G350-001(super-if:FastEthernet 10/2)# no shutdown
```

- In PPP, the remote peer requests the device to authenticate using a specific authentication method (CHAP or PAP). Use the **ppp chap refuse** command to not agree to authenticate with CHAP. Use the **ppp pap refuse** command to not agree to authenticate with PAP. These commands prevent the device from authenticating with a specific method.
- Use the **show ppp authentication** command to display the interface's PPP authentication status. This command displays the following:

  ```
  [PAP refuse]
  PAP sent-username: [not] configured
  [CHAP refuse]
  CHAP hostname: <used CHAP hostname>
  For example:
  ```

  ```
  G350-001(super-if:FastEthernet 10/2)# show ppp authentication
  PAP sent-username: configured
  CHAP refuse
  CHAP hostname: G350
  ```

- Use the **keepalive** command to 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. If five consecutive keepalive requests are not answered, the PPP session is terminated. To deactivate keepalive, use the **no** form of the command or set the health check interval to 0.

6. Type **exit** to return to general context. The prompt returns to:

   ```
   G350-001(super)#
   ```

7. Test the configuration. See Verifying the WAN configuration and testing connectivity on page 96.
8. Use the **copy running-config startup-config** command to save the configuration.

To shut down the port, and the PPPoE client (if configured), use the **shutdown** command in the interface context.

Configuring frame relay

To configure frame relay encapsulation on a WAN port:

1. Ensure that the port is configured on the media module:
   - For an E1/T1 port, see Configuring the Avaya MM340 E1/T1 WAN media module on page 85.
   - For a USP port, see Configuring the Avaya MM342 USP WAN media module on page 88.
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.
4. If needed, use the **`frame-relay lmi`** commands to change the Local Management Interface (LMI) parameters from their default values, or use the **`frame-relay traffic-shaping`** command to activate traffic shaping on the frame relay interface. For more information on traffic shaping, see Traffic Shaping and Marking on page 104.
5. If you want to change the queuing mode of the interface, see Configuring Weighted Fair VoIP Queuing (WFVQ) on page 76 for instructions.
6. Type **`exit`** to return to general context. The prompt returns to:

   `G350-001(super)#`
7. Use the **`interface Serial`** ***`if.fr-sub-if`*** **`point-to-point`** command to create a frame relay sub-interface and enter the context of the interface. For example:
   - **`interface Serial 4/1:2.1 point-to-point`**
     creates frame relay sub-interface number 1 on the E1/T1 media module in slot number 4, on port number 1, with channel group number 2
   - **`interface Serial 5/1:2.3.2 point-to-point`**
     creates frame relay sub-interface number 3 on the E1/T1 media module in slot number 5, on port number 1, with channel group number 2, and with IP interface number 2
   - **`interface Serial 4/1.2 point-to-point`**
     creates frame relay sub-interface number 2 on the USP media module in slot number 4, on port number 1
   - **`interface Serial 5/1.2.1 point-to-point`**
     creates frame relay sub-interface number 2 on the USP media module in slot number 5, on port number 1, with IP interface number 1

   Note:

   Currently only point-to-point frame relay sub-interfaces are supported.

8. Use the **`frame-relay interface-dlci DLCI-number`** command to configure a Data Link Connection Identifier (DLCI) for the frame relay sub-interface.
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. For more information, refer to Traffic Shaping and Marking on page 104.
10. Use the **`ip address`** command to configure an IP address and subnet mask for the frame relay sub-interface.
11. Type **`exit`** to return to general context. The prompt returns to:

    `G350-001(super)#`
12. If needed, repeat Step 6 through Step 10 to configure additional frame relay sub-interfaces on the same serial interface.
13. If needed, repeat Step 2 through Step 11 to configure frame relay encapsulation for other serial interfaces on the same WAN port.
14. Test the WAN configuration. See Verifying the WAN configuration and testing connectivity on page 96.
15. Use the **`copy running-config startup-config`** command to save the configuration.

Verifying the 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. Make sure the controller is up, and that all error counters do not increase.
- For all serial interfaces (E1/T1 and USB), use the **`show interfaces Serial`** command to verify that the interface and line protocol are both up:

  `Serial x/y:z is up, line protocol is up`
- For USB interfaces only, use the **`show interfaces Serial`** command to verify that all line signals are up:

  `DCD = up DSR = up DTR = up RTS = up CTS - up`

- Use the **`show frame-relay pvc`** command to view basic information about frame relay configuration. For more information about frame relay configuration, use the following commands:
  - **`show frame-relay fragment`** to display frame relay fragmentation statistics and configuration on all PVCs associated with the interface.
  - **`show frame-relay lmi`** to display LMI statistics for the interface.
  - **`show frame-relay map`** to display a summary table of frame relay sub-interfaces and DLCIs associated with the sub-interfaces.
  - **`show frame-relay traffic`** to display frame relay protocol statistics, including ARP requests and replies sent and received over the interface.
  - **`show map-class frame-relay`** to display the map-class Frame Relay table.
- 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.
- Use the **`show running-config`** command to display the configuration running on the device.
- Use the **`show startup-config`** command to display the configuration loaded at startup.
- Use the **`ping`** command to send ICMP echo request packets from the G350 to the interface serial peer IP address and verify that it responds.
- Use the **`ping`** command to send ICMP echo request packets to another node on the network. Each node is periodically pinged and checked if an answer was received. This checks host reachability and network connectivity.

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, or Fast Ethernet 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.

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 using the **`backup delay`** command:

- *`Failure delay`* — The time in seconds between the primary interface going down and the backup interface activation. Default = 0 seconds, maximum = 3600 seconds.
- *`Secondary Disable delay`* — The time in seconds between the primary interface restoration and the backup interface deactivation. Default = 0 seconds, maximum = 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.

For 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:

```
GG350-001(super)# interface FastEthernet 10/2
G350-001(super-if:FastEthernet 10/2)# backup delay 0 60
Done!
G350-001(super-if:FastEthernet 10/2)#
```

The following rules govern the interface backup relations:

- 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 switch over 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.

Backup commands

Use the following commands to configure a backup interface:

- Use the **`backup interface`** command, followed by the interface type and number, to set a backup interface. You must use this command from the context of the interface for which you are setting a backup interface.
- Use the **`backup delay`** command to 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. For example, the following command causes the G350 to switch immediately to the backup interface in the event of primary interface failure, and to delay 60 seconds before reverting back to the primary interface once the primary interface is restored to service:

  ```
  G350-001(super-if:FastEthernet 10/2)# backup delay 0 60
  ```

Extended keepalive

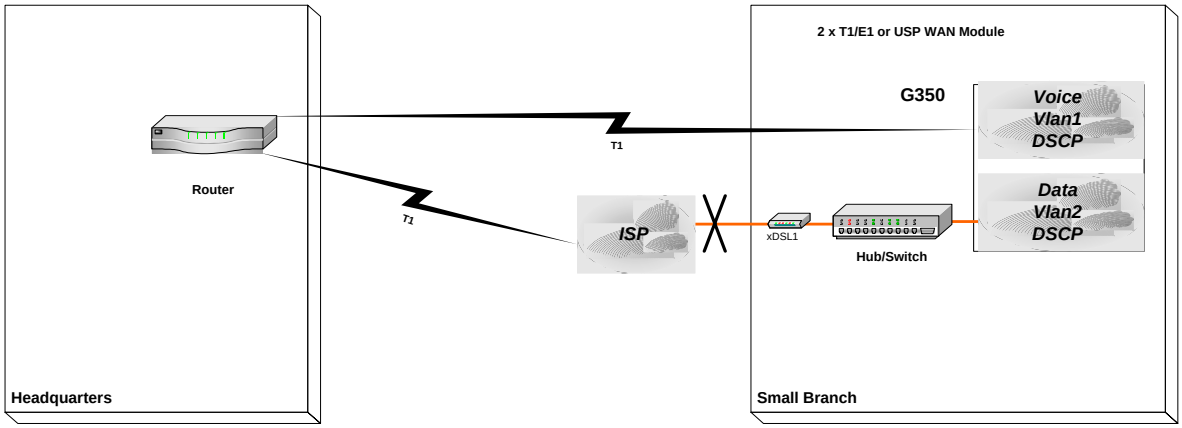
The extended keepalive feature is available for WAN Fast Ethernet interfaces. Extended keepalive is a mechanism for determining if a certain IP address is reachable. The source interface sends test packets (ping) and waits for a response. If no response is received after a certain number of tries, the 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 Configuring policy-based routing on page 273.

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.

Extended Keepalive is a mechanism that reports on the status of an IP address *and its next hop*. The destination interface is only declared to be alive if the next hop is also reachable. This feature is critical for mechanisms such as policy-based routing that must guarantee service on a particular path.

Figure 6: G350 with T1 and xDSL lines



For example, your branch office may have a G350 that connects to the 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. Normal keepalive cannot report on the status of the entire WAN path. If the FastEthernet line protocol is up but the xDSL connected to it is down, normal keepalive reports that the FastEthernet interface is up. Only Extended 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 Extended Keepalive to know the status of the interfaces on its next hop list.

Note:

Extended Keepalive is not used with a GRE tunnel interface. The GRE tunnel has its own keepalive mechanism. For details, refer to *Administration of the Avaya G350 Media Gateway*, 555-245-501.

Use the **`extended-keepalive`** command in the context of the interface to enable the extended keepalive feature. Use the **no** form of this command to deactivate the feature.

The **`extended-keepalive`** command 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 port.

Use the following commands to define the extended keepalive parameters. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`extended-keepalive timeout`** command to set the timeout (in seconds) for receiving the keepalive response. The default value is 1.
- Use the **`extended-keepalive success-retries`** command to set the number of consecutive successful keepalive packets necessary to set the interface's keepalive status as up. The default value is 1.

- Use the **extended-keepalive failure-retries** command to set the number of consecutive failed keepalive packets necessary to set the interface's keepalive status as down. The default value is 4.
- Use the **extended-keepalive interval** command to set the interval (in seconds) between keepalive packets. The default value is 5.
- Use the **extended-keepalive source-address** command to set the source IP address of the keepalive packets. The default value is the interface's primary IP address.
- Use the **show extended-keepalive** command to display the interface's extended keepalive status and parameters.

The following example configures extended keepalive on interface FastEthernet 10/2 to send keepalive packets to IP address 135.64.2.12 using MAC 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.

```
G350-001# interface FastEthernet 10/2
G350-001(super-if:FastEthernet 10/2)# extended-keepalive 135.64.2.12
11.22.33.44.55.66
G350-001(super-if:FastEthernet 10/2)# extended-keepalive interval 5
G350-001(super-if:FastEthernet 10/2)# extended-keepalive timeout 1
G350-001(super-if:FastEthernet 10/2)# extended-keepalive
failure-retries 3
G350-001(super-if:FastEthernet 10/2)# extended-keepalive
success-retries 2
Done!
```

A special version of the keepalive feature is available for GRE tunnels. See keepalive on page 171.

Dynamic CAC

Dynamic Call Admission Control (CAC) provides enhanced control over WAN bandwidth. When Dynamic CAC is enabled on an interface, the G350 informs the MGC of the actual bandwidth of the interface and tells 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 Communication Manager Call Admission Control: Bandwidth Limitation (CAC-BL) feature. For more information, refer to *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

You can enable dynamic CAC on the following interface types:

- **Fast Ethernet**
- **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.

Use the **`dynamic-cac bbl`** command in interface context to 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 G350 reports the bearer bandwidth limit of the interface with the highest activation priority. You can set the activation priority to any number between 1 and 255. The default activation priority is 50.

The following example sets dynamic CAC on Fast Ethernet interface 10/2, with a bearer bandwidth limit of 128 and an activation priority of 100:

```
G350-001# interface FastEthernet 10/2
G350-001(super-if:FastEthernet 10/2)# dynamic-cac 128 100
```

Use the **`show dynamic-cac`** command to display bandwidth information about the interface. The **`show dynamic-cac`** command displays the following information:

- **Current RBBL** — The current actual bandwidth available on the interface.
- **Last event** — The amount of time since the most recent update by the CAC process.
- **Last event BBL** — The interface's bandwidth at the time of the most recent update by the CAC process.

Note:

Dynamic CAC also requires configuration of the MGC. For details, refer to *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Frame relay encapsulation

The Avaya G350 Media Gateway supports the following frame relay encapsulation features:

- Priority DLCI
- Traffic shaping and marking per Virtual Channel (VC)
- Priority queuing

Note:

The term Virtual Channel (VC) refers to the unidirectional flow of ATM cells between connecting (switching or end-user) points that share a common identifier number.

To improve voice quality using RTP, see Configuring RTP header compression on page 72.

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 G350 supports class-based traffic assignment (priority DLCI). Priority DLCI is essentially a means for implementing QoS. The G350 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. For more information, see Configuring policy on page 253.

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. When using Priority DLCI, it is therefore recommended to verify that the primary DLCI is set as the High Priority DLCI in the Priority DLCI group.

On the Avaya G350 Media 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.

Traffic Shaping and Marking

Traffic shaping monitors outgoing traffic and takes appropriate action if traffic exceeds agreed parameters. The action could be to drop the packets or mark them as being high-drop priority.

The Avaya G350 Media Gateway supports the following traffic shaping parameters per PVC:

- **Committed Information Rate (CIR)** — the amount of committed bandwidth to which the customer is entitled
- **Discard Eligible (DE) pre-mark** — sets the threshold for pre-marking DE of non-high priority traffic, in percentage of CIR.
- **Link Fragmentation and Interleaving (LFI)** — enables fragmentation of large frame relay frames per PVC

You can configure the traffic shaping parameters within map classes. A map class is comprised of the following parameters:

- ***CIR*** — Default 56,000 bps
- ***Committed Burst (BC) size*** — default 7,000 bps
- ***Excess Burst (BE) size*** — default 0 bps
- ***DE pre-mark*** — Specifies the amount of non-high priority (0 to 5) packets over the BC and under the BE to label as DE. This amount is measured in percentage of CIR. The default is 100%, unconditionally dropping all packets above the BE.
- ***Fragmentation*** — Fragment size, in bytes. The default is 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 either the Primary VC or to the Priority DLCI group VCs.

Note:

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 using the **`frame-relay traffic-shaping`** command. After you enable traffic shaping, a default map class is applied to all currently configured PVCs. In this default map class, the BE is zero. All traffic above the BC is dropped.

Priority queuing

Priority queuing is designed to give all mission-critical programs higher priority than less critical traffic. Traffic is queued as high, normal, medium, or low. Using priority queuing, all high-priority traffic is serviced first, then normal, etc.

The frame relay ingress queuing mechanism functions the same as on PPP interfaces. The frame relay egress queuing mechanism also functions the same as on PPP interfaces, serving all PVCs configured on the interface, with an additional user-configurable DE buffer. The DE buffer contains all traffic marked as Discard Eligible, and has the lowest priority.

When using VoIP, the G350 enables a distinction within the high-priority queue between priorities 6 and 7. The G350 uses priority 6 for the voice-bearer traffic, and priority 7 for the voice-controller traffic. These two priorities are served on a round-robin basis. Within the high-priority queue, the priority 6 capacity is a maximum of 25% the size of the priority 7 capacity to reduce the delay of voice flow. The priority 6-7 distinction exists in data mode as well, where the queue is divided equally between both capacities.

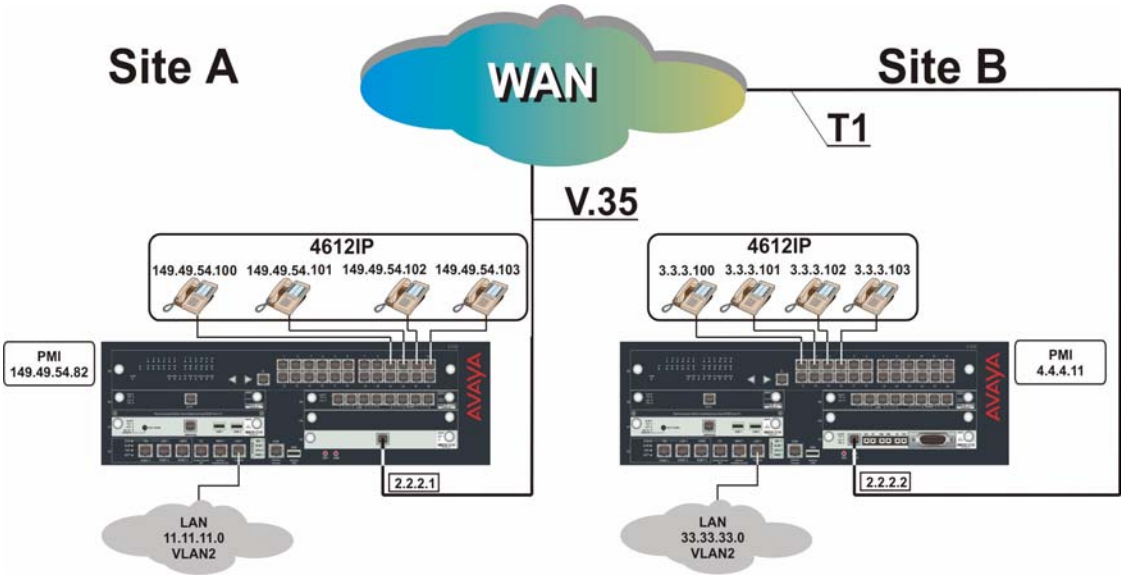
WAN configuration example

This section contains an example that illustrates a common PPP VoIP configuration between two sites connected over a WAN.

PPP VoIP configuration

The following figure illustrates a common PPP VoIP configuration between two sites connected over a WAN:

Figure 7: PPP VoIP configuration over WAN



Site A contains four IP phones and a G350 with S8300 and one MM342 media module. The MM342 media module connects the G350 to the WAN via a USP 128Kbps 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 Media Gateway, Media Server, 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.

- 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
  - G350 PMI - 149.49.54.82

Site B contains four IP phones and a G350 with S8300 and one MM340 media module. The MM340 media module connects the G350 to the WAN via a two-timeslot (128Kbps) T1 interface. The following are the connection details for Site B:

- IP phone 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
  - G350 PMI - 4.4.4.11

Configuration Example for Site A

The following is the procedure for configuring PPP VoIP on the G350 at Site A. Commands with footnotes are described at the end of the configuration procedure.

- Loopback and PMI interfaces configuration:

```
G350-001# interface Loopback 1
G350-001(if:Loopback 1)# ip address 149.49.54.82 24
Done!
G350-001(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.
G350-001(if:Loopback 1)# exit
G350-001# copy running-config startup-config
G350-001# reset
```

- VLAN interface configuration:

```
G350-001# interface Vlan 1
G350-001(if:Vlan 1)# ip address 149.49.54.24
Done!
G350-001(if:Vlan 1)# exit
G350-001# interface Vlan 2
G350-001(if:Vlan 2)# ip address 11.11.11.1 24
Done!
G350-001(if:Vlan 2)# exit
```

- Serial interface configuration:

```
G350-001# interface Serial 5/1
G350-001(if:Serial 5/1)# ip address 2.2.2.1 24
G350-001(if:Serial 5/1)# 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.

```
G350-001(if:Serial 5/1)# bandwidth 128
```

- VoIP configuration:

```
G350-001(if:Serial 5/1)# ip rtp header-compression
G350-001(if:Serial 5/1)# ip rtp compression-connections 20 (4)
G350-001(if:Serial 5/1)# ip rtp port-range 2048 3028       (5)
G350-001(if:Serial 5/1)# exit
```

- Static routes configuration:

```
G350-001# ip default-gateway 5/1
```

```
* 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 G350.

(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

The following is the procedure for configuring PPP VoIP on the G350 at Site B.

- Loopback and PMI interfaces configuration:

```
G350-001# interface Loopback 1
G350-001(if:Loopback1)# ip address 4.4.4.11 32
Done!
```

```
G350-001(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.
G350-001(if:Loopback1)# exit
G350-001# copy running-config startup-config
G350-001# reset
```

- VLAN interface configuration:

```
G350-001# interface Vlan 1
G350-001(if:Vlan 1)# ip address 3.3.3.1 24
G350-001(if:Vlan 1)# exit
G350-001# interface Vlan 2
G350-001(if:Vlan 1:2)# ip address 33.33.33.1 24
G350-001(if:Vlan 1:2)# exit
```

- Serial interface configuration:

```
G350-001# controller t1 5/1
G350-001(controller:5/1)# channel-group 1 timeslots 1-2 speed 64
G350-001(controller:5/1)# exit
G350-001# interface Serial 5/1:1
G350-001(if:Serial 5/1:1)# ip address 2.2.2.2 24
G350-001(if:Serial 5/1:1)# 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:

```
G350-001(if:Serial 5/1:1)# ip rtp header-compression
G350-001(if:Serial 5/1:1)# ip rtp compression-connections 20
G350-001(if:Serial 5/1:1)# ip rtp port-range 2048 3028
G350-001(if:Serial 5/1:1)# exit
```

- Static routes configuration:

```
G350-001# ip route 1.1.1.0 24 serial 5/1:1
G350-001# ip route 11.11.11.0 24 serial 5/1:1
```

Chapter 10: Configuring PoE

This chapter provides information about Power over Ethernet (PoE) using the MM314 PoE media module, and contains the following sections:

- PoE overview — an overview of PoE on the MM314 media module
- PoE configuration CLI commands — a list and descriptions of CLI commands for PoE configuration
- PoE configuration examples — examples of PoE configurations

PoE overview

This section provides an overview of Power over Ethernet (PoE) on the MM314 PoE media module, and includes the following topics:

- Introduction
- Load detection
- Powering devices

Introduction

The Avaya G350 MM314 PoE media module provides Inline DC power over the signal pairs, in addition to switched Ethernet, on the existing LAN infrastructure for devices such as IP telephones and Wireless LAN access points. This allows you to deploy devices in the network that require power without installing standard power cables. The G350 MM314 enables you to configure a power consumption usage threshold, as well as to generate traps when this threshold is crossed.

The MM314 PoE media module provides power over standard Category 3 and Category 5 cables. The MM314 PoE media module is designed to comply to the IEEE 802.3af standard.

Note:

When you connect a non-powered device to a PoE port, the PoE port status alternates between Searching and Fault. Ignore the Fault status.

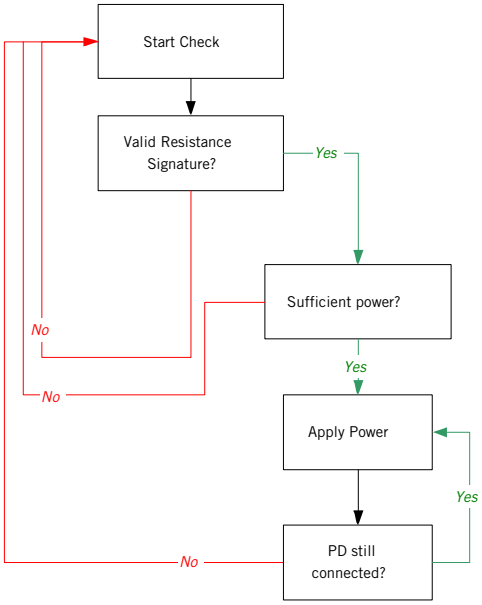
Load detection

The MM314 PoE media module periodically checks all ports, powered and non-powered, to check their status and the power status of connected devices. The module supplies power to a port only after it has detected that a suitable Powered Device (PD) is connected to the port. The MM314 PoE media module looks for an IEEE 802.3af-compliant signature from the device that indicates that the device requires power.

How the G350 detects a powered device

The following figure shows the process of applying PoE power to a PD.

Figure 8: Powered Device Detection



The MM314 PoE media module applies a low voltage to the power feed pairs and measures the current. A resistance of 19kΩ to 26.5kΩ is considered valid. If a valid signature is detected, and the MM314 has not exceeded its PoE allocated power, then power is supplied to the port.

Once power is provided to a port, it is checked periodically to see if a PD is still connected. If a PD is disconnected from a powered port, then power is denied to the port.

Plug and Play Operation

You can add and remove powered devices without manually reconfiguring the switch, since it performs a periodic automatic load detection scan on non-powered ports.

- If a powered device that fits the above criteria is detected on a non-powered port, then power is applied to the port.
- If a powered device is removed from a port, then power is denied to that port. The disconnected port is then scanned as well.

In addition, if the PoE module is removed and replaced with module of the same type, the port power configuration of the module is retained.

Powering devices

The Avaya G350 MM314 PoE media module has its own power supply. Therefore, a full 210 W of power is available for PDs. Each port can supply up to 19.5 W by default. If a powered device tries to draw more than the maximum allowed power per port, power is denied.

Since 210 W may not be enough for driving powered devices on all the ports simultaneously, a priority mechanism exists.

The priority mechanism determines the order in which ports are powered after the switch is booted.

There are three user-configurable PoE priority levels:

- Low
- High
- Critical

The default value for all ports is Low.

Power is automatically applied to PDs according to their priority when the power budget increases. If the power budget is exceeded, power is not provided to a new PD when you attach it, even if you define its priority as High or Critical.

Note:

The order in which ports are powered within the same priority group is not sequential.

PoE configuration CLI commands

Use the following commands to configure PoE on an Avaya G350 MM314 PoE media module:

- Use the **`set port powerinline`** command to enable or disable load detection on a port.
- Use the **`set port powerinline type`** command to configure the connected PD type.
- Use the **`set port powerinline priority`** to configure the PoE priority level over a port.
- Use the **`set powerinline trap enable`** to configure PoE traps and the consumption usage threshold value.
- Use the **`show powerinline`** command to display Power over Ethernet (PoE) information.

Note:

If another PoE-enabled device (such as a P333T-PWR switch) is connected to a port, the **`show powerinline`** command may incorrectly show the port power status as Delivering Power. To disable inline power for a port connected to a P333T-PWR, use the command **`set port powerinline disable`**.

PoE configuration examples

This section provides PoE configuration examples.

The following example enables PoE on a port:

```
G350-003(super)# set port powerinline 6/12 enable
Load detection process on port 6/12 is enabled.
```

The following example disables PoE on a port:

```
G350-003(super)# set port powerinline 6/12 disable
Load detection process on port 6/12 is disabled.
```

The following example configures PoE priority on a port:

```
G350-003(super)# set port powerinline priority 6/14 high
Powering priority on port 6/14 was set to High.
```

The following example displays PoE information:

```
G350-003(super)# show powerinline

Actual powerinline power consumption is 4 W.

Powerinline power consumption trap threshold is 207(99%) Watts.
```

```
Powerline traps are enabled

Port      Inline                  Powering     PD
          Operational             Priority     Type
          Status
------    ------------------      ---------    --------
6/1       Searching               Low          telephone
6/2       Searching               Low          telephone
6/3       Searching               Low          telephone
6/4       Searching               Low          telephone
6/5       Searching               Low          telephone
6/6       Searching               Low          telephone
6/7       Searching               Low          telephone
6/8       Searching               Low          telephone
6/9       Searching               Low          telephone
6/10      Searching               Low          telephone
6/11      Searching               Low          telephone
6/12      Disabled                Low          telephone
6/13      Searching               Low          telephone
6/14      Searching               High         telephone
6/15      Searching               Low          telephone
6/16      Searching               Low          telephone
6/17      Fault                   Low          telephone
6/18      Fault                   Low          telephone
6/19      Searching               Low          telephone
6/20      Searching               Low          telephone
6/21      Searching               Low          telephone
6/22      Fault                   Low          telephone
6/23      Delivering Power        Low          telephone
```

Chapter 11: Configuring Emergency Transfer Relay (ETR)

This chapter provides information about configuring the G350's Emergency Transfer Relay (ETR) feature and contains the following sections:

- ETR overview — an overview of the G350's ETR feature
- Setting ETR state — instructions on how to set the ETR state
- Viewing ETR state — instructions on how to display the ETR state

ETR overview

The ETR feature provides basic telephone services in the event of system failure, such as a power outage or a failed connection to Avaya Communication Manager. ETR is activated automatically. When ETR is activated, the Avaya G350 Media Gateway connects the fixed analog trunk port (7/1) to the fixed analog line port (7/2). An outside telephone exchange can be connected to the trunk port and an analog telephone can be connected to the line port. All calls are then directed by the analog relay between the outside line and the analog telephone. A current-loop detection circuit prevents ongoing calls from being disconnected when normal functioning resumes. If a call is in progress on LINE 1 when the problem ends, the call continues. The fixed trunk port (7/1) and analog line ports (7/2 and 7/3) do not start to operate until the active call ends.

When ETR is active and the G350 has power, the ETR front panel LED is lit.

Setting ETR state

By default, ETR is set to go into effect automatically in the event of power outage or failed connection to Avaya Communication Manager. You can activate and deactivate ETR manually via the CLI.

To activate ETR manually, use the following command:

```
set etr 7 manual-on
```

Generally, you should only use this command for testing. The manual-on option activates the connection between the analog trunk port (7/1) and the first analog line port (7/2). The other analog line port (7/3) will also be disabled.

To deactivate ETR manually, use the following command:

`set etr 7 manual-off`

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

To restore ETR to automatic activation, use the following command:

`set etr 7 auto`

If the system fails, the trunk and port are automatically latched.

Note:

A call in progress will be terminated when ETR is activated wither automatically or manually. The relay call will be terminated only when ETR is deactivated manually.

Viewing ETR state

You can use the **`show etr`** command to display ETR information. This information includes the following:

- ETR setting (auto, manual-off, or manual-on)
- Module status (in service, out of service, or out of service waiting for off-hook)
- Trunk number of the trunk connected to ETR
- Line number of the line connected to ETR
- Line status (**`off hook`** or **`on hook`**)

Chapter 12: Configuring SNMP

This chapter provides information about configuring SNMP on the G350 and contains the following sections:

- SNMP configuration overview — an overview of SNMP configuration on G350 devices
- SNMP versions — a description of the SNMP versions supported by the G350
- Configuring SNMP traps — instructions on how to configure SNMP traps on G350 devices
- Configuring SNMP access — instructions on how to configure SNMP access on G350 devices
- Configuring dynamic trap manager — instructions on how to configure dynamic trap manager, a feature that ensures that traps are always sent to the G350's active MGC
- SNMP configuration examples — examples of SNMP configuration

SNMP configuration overview

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:

- 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 G350.

There are several ways that the SNMP manager and the agent communicate. The manager can:

- Retrieve a value – a *get* action.
  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 — a *get-next* action.
  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 — a *get-bulk* action.
  The get-bulk operation retrieves the specified number of instances of the requested MIB variable. This minimizes the number of protocol exchanges required to retrieve a large amount of data.

  Note:

  Get-bulk is not supported in SNMPv1.
- Change a configuration on the agent — a *set* action.
  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.
- An agent can send an unsolicited message to the manager at any time if a significant, predetermined event takes place on the agent. This message is called a *notification*. 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 Traps and MIBs on page 323.

SNMP versions

There are currently three versions of SNMP:

- SNMPv1
- SNMPv2c
- SNMPv3

The Avaya G350 Media Gateway supports all three of these versions. The implementation of SNMPv3 on the G350 is backwards compatible. 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 user name 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 uses can access SNMPv3 at the same time.

SNMP supports three security levels:

- **NoAuthNoPriv** — This is the lowest level of SNMPv3 security. No Message Authentication Code (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.

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:

- ***`Username`*** — A string of up to 32 characters representing the name of the user.
- ***`Groupname`*** — A string of up to 32 characters representing the name of the group with which the user is associated.
- ***`SecurityModel`*** — The SNMP version functionality that the user is authorized to use. Possible values are: v1 (SNMPv1), v2c (SNMPv2c), and v3 (SNMPv3).
- ***`Authentication Protocol`*** — The authentication protocol to use. Possible values are: noAuth (no authentication), md5 (HMAC MD5), and sha (HMAC SHA-1).
- ***`Authentication Password`*** — A string of between 8 and 64 characters specifying the user's authentication password. The authentication password is transformed using the authentication protocol and the SNMP engine ID to create an authentication key.
- ***`Privacy Protocol`*** — The privacy protocol to use. Possible values are: No privacy, DES privacy.
- ***`Privacy Password`*** — A string of between 8 and 64 characters specifying the user's privacy password.

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 mode and level with which the user is communicating with the G350. Within a group, the following combinations of security mode and level can be mapped to views:

- **SNMPv1** — Anyone with a valid SNMPv1 community name.
- **SNMPv2c** — Anyone with a valid SNMPv2c community name.
- **NoAuthNoPriv** — An SNMPv3 user using the NoAuthNoPriv security level.
- **AuthNoPriv** — An SNMPv3 user using the AuthNoPriv security level.
- **AuthPriv** — An SNMPv3 user using the AuthPriv security level.

If views are not defined for all security modes 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.

To create an SNMPv3 group, the following information must be provided:

- **GroupName** — A 32-character string representing the name of the group.
- **SNMPv1** — The name of the view for anyone communicating with the device via SNMPv1.
- **SNMPv2c** — The name of the view for anyone communicating with the device via SNMPv2c.
- **NoAuthNoPriv** — The name of the view for SNMPv3 NoAuthNoPriv users.
- **AuthNoPriv** — The name of the view for SNMPv3 AuthNoPriv users.
- **AuthPriv** — The name of the view for SNMPv3 AuthPriv users.

The G350 includes the following pre-configured groups:

Group Name	Security Model	Security Level	Read View Name	Write View Name	Trap View Name
ReadCommG	v1	1 (noAuthNoPriv)	snmpv1View		snmpv1View
ReadCommG	v2	1 (noAuthNoPriv)	snmpv1View		snmpv1View
WriteCommG	v1	2 (noAuth)	snmpv1 WriteView	snmpv1 WriteView	snmpv1 WriteView

1 of 2

Group Name	Security Model	Security Level	Read View Name	Write View Name	Trap View Name
WriteCommG	v2c	2 (noAuth)	snmpv1 WriteView	snmpv1 WriteView	snmpv1 WriteView
v3ReadWriteG	v3 (USM)	2 (noAuth)	v3configview	v3configview	v3configview
v3ReadOnlyG	v3 (USM)	2 (noAuth)	v3configview		v3configview
initial	v3 (USM)	1 (noAuthNoPriv)	restricted	restricted	restricted
v3AdminViewG	v3 (USM)	3 (AuthPriv)	iso	iso	iso
					2 of 2

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 G350's MIB tree. You can use wildcards to include or exclude an entire branch of OIDs in the MIB tree, using an asterisk instead of the specific node. For a list of MIBs and their OIDs, see G350 MIBs on page 331.

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.

Configuring SNMP traps

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 G350 interfaces. Use the following commands to configure the trap receivers table:

Note:

You need an Admin privilege level to use the SNMP commands.

- Use the **`snmp-server enable notifications`** command to enable SNMP traps and notifications. Use the **no** form of this command to disable SNMP traps and notifications.
- Use the **`set port trap`** command to enable and disable link-up and link-down notifications and traps.
- Use the **`set snmp trap enable/disable auth`** command to enable and disable authentication failure traps for all managers.
- Use the **`set snmp trap enable frame-relay`** command to enable frame relay traps for all managers.
- Use the **`show snmp`** command to display SNMP information.
- Use the **`snmp-server informs`** command to configure the SNMPv3 timeout and retries for notifications.
- Use the **`snmp-server host`** command to define an SNMPv3 notification host. Use the **no** form of this command to remove an SNMPv3 notification host and to remove notification filter groups from a specific host. You can define the following parameters with this command:
  - ***`type`*** — Determines whether to send traps or informs to the recipient. The default is traps.
  - ***`version`*** — Determines the SNMP security model (v1, v2c, v3). If the security model is v1, you must add the v1 community string to use in notifications. If you select v3, you must also specify the authentication method. Options are:
    - ***`auth`*** — authentication without encryption
    - ***`noauth`*** — no authentication
    - ***`priv`*** — authentication with encryption
  - ***`community string`*** — The v1 community string to use in notifications
  - ***`user name`*** — The v3 user name to use in notifications
  - ***`udp port`*** — Optional. A keyword and variable that specify which UDP port of the target host to use as the destination UDP port when sending a notification to this manager. The default is 162.

- ***notification type*** — The type of traps to be sent. You can choose from the following:
  - ***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*** — media 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

Note:

There is no default value for the ***notification type*** parameter. Thus, you must enter a value in order to send traps.

- Use the **snmp trap link-status** command to enable Link Up and Link Down traps on an interface. You must use this command from an interface context.
- Use the **no snmp trap link-status** command to disable Link Up and Link Down traps on an interface. You must use this command from an interface context.

Configuring SNMP access

Use the following commands to configure SNMP access:

Note:

You need an Admin privilege level to use the SNMP commands.

- Use the **`ip snmp enable`** command to enable SNMP access to the G350. Use the **no** form of this command to disable SNMP access to the G350.
- Use the **`snmp-server community`** command to enable SNMPv1 access to the G350. Use the **no** form of this command to disable SNMPv1 access to the G350.
- Use the **`snmp-server user`** command to create an SNMPv3 user. Use the **no** form of this command to remove an SNMPv3 user.
- Use the **`snmp-server group`** command to create an SNMPv3 group. Use the **no** form of this command to remove an SNMPv3 group.
- Use the **`snmp-server remote-user`** command to create an SNMPv3 remote user for SNMP notifications. Use the **no** form of this command to remove an SNMPv3 remote user for SNMP notifications.
- Use the **`set snmp community`** command to create or modify an SNMPv1 community.
- Use the **`snmp-server engineID`** command to configure the SNMPv3 engine ID. Use the **no** form of this command to configure the engine ID to its default value. The SNMP engine ID is set automatically by a calculation based on the MAC address of the host device, but you can change the engine ID using this command. If the SNMP engine ID changes, all users other than the default user are invalid and must be redefined.
- Use the **`snmp-server view`** command to add or exclude OIDs from a view. Use the **no** form of this command to delete an SNMPv3 view.
- Use the **`show snmp view`** command to display a list of SNMPv3 views.
- Use the **`show snmp userToGroup`** command to display a table of SNMPv3 users and the groups to which they are mapped.
- Use the **`show snmp engineID`** command to display the SNMPv3 engine ID.
- Use the **`show snmp group`** command to display a list of SNMPv3 groups.
- Use the **`show snmp user`** command to display a list of SNMPv3 users.
- Use the **`show snmp`** command to display a list of SNMP notification receivers.

Configuring dynamic trap manager

Dynamic trap manager is a special feature that ensures that the G350 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 can not be removed.

Use the **`snmp server dynamic-trap-manager`** command to specify the parameters of the dynamic trap manager feature. You can configure the following parameters:

- ***`type`*** — Determines whether to send traps or informs to the recipient. The default is traps.
- ***`version`*** — Determines the SNMP security model (v1, v2c). If the security model is v1, you must add the v1 community string to use in notifications.
- ***`udp port`*** — Optional. A keyword and variable that specify which UDP port of the target host to use.
- ***`notification type`*** — The type of traps to be sent. To send all types of traps, set this parameter to *all*. For a list of possible notification types, see Configuring SNMP traps on page 125.

Note:

There is no default value for the ***`notification type`*** parameter. Thus, you must enter a value in order for the dynamic trap manager to send traps.

The following example configures dynamic trap manager to send all traps:

```
G350-001(super)# snmp-server dynamic-trap-manager traps v1 public
udp-port 162 all
```

SNMP configuration examples

This section provides SNMP configuration examples:

The following example enables link up/down traps on an Ethernet interface:

```
G350-001(super)# interface FastEthernet 10/2
G350-001(super-if:FastEthernet 10/2)# snmp trap link-status
Done!
```

The following example adds an SNMPv1 trap receiver:

```
G350-001(super)# set snmp trap 192.36.44.18
SNMP trap receiver added.
```

The following example disables all traps for an SNMPv1 trap receiver:

```
G350-001(super)# set snmp trap 192.36.44.18 disable all
SNMP all traps disabled.
```

The following example enables config traps for an SNMPv1 trap receiver:

```
G350-001(super)# set snmp trap 192.36.44.18 enable config
SNMP config trap enabled.
```

The following example displays SNMP information:

```
G350-001(super)# show snmp
Authentication trap enabled

Community-Access     Community-String
----------------     ----------------
read-only            public
read-write           public
trap                 public
Trap-Rec-Address     Traps Enabled
----------------     ----------------
192.36.44.18         config
```

The following example deletes an SNMPv1 trap receiver:

```
G350-001(super)# clear snmp trap 192.36.44.18
SNMP trap receiver deleted.
```

The following example disables link up/down traps on an Ethernet interface:

```
G350-001(super-if:FastEthernet 10/2)# no snmp trap link-status
Done!
```

The following example creates a read-only user:

```
G350-001# snmp-server user <username> v3 ReadOnlyG v3 auth {md5|sha}
<authPassword> priv des56 <privPassword>
```

The following example creates a read-write user:

G350-001# snmp-server user <username> v3 ReadWriteG v3 auth {md5|sha} <authPassword> priv des56 <privPassword>

The following example creates an admin user:

G350-001# snmp-server user <username> v3 v3AdminG v3 auth {md5|sha} <authPassword> priv des56 <privPassword>

The following example sets the SNMPv1 read-only community:

```
G350-001(super)# set snmp community read-only read
SNMP read-only community string set.
```

The following example sets the SNMPv1 read-write community:

```
G350-001(super)# set snmp community read-write write
SNMP read-write community string set.
```

The following example sets the SNMPv1 trap community:

```
G350-001(super)# set snmp community trap trap
SNMP trap community string set
```

The following example enables link up/down trap on a LAN port (6/1):

```
.G350-001(super)# set port trap 6/1 enable
Port 6/1 up/down trap enabled
```

The following example disables link up/down trap on a LAN port:

```
G350-001(super)# set port trap 6/1 disable
Port 6/1 up/down trap disabled
```

Chapter 13: Configuring advanced switching

This chapter provides information about configuring advanced switching on the switch ports of the Avaya MM314 media module and contains the following sections:

- Configuring VLANs — instructions on how to configure VLANs
- Configuring port redundancy — instructions on how to configure port redundancy
- Configuring port mirroring — instructions on how to configure port mirroring
- Configuring spanning tree — instructions on how to configure spanning tree
- Port classification — instructions on how to configure port classification

Configuring VLANs

This section contains information about VLAN configuration on the G350's switch ports and includes the following topics:

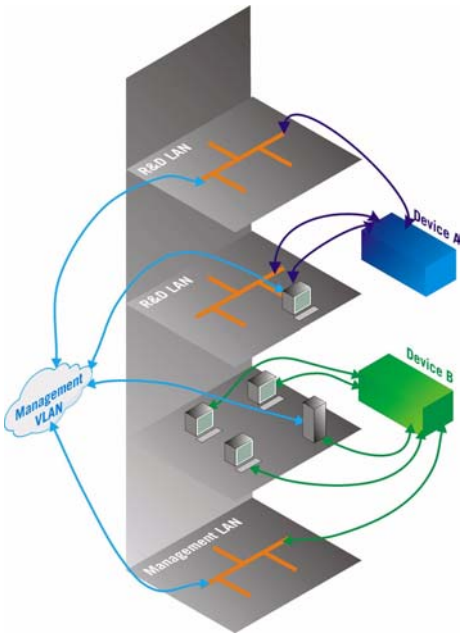
- VLAN overview — an overview of VLANs and how they can be used in a network
- VLAN tagging — an explanation of VLAN tagging
- Multi VLAN binding — an explanation of Multi VLAN binding, also known as Multiple VLANs per port
- G350 VLAN table — an explanation of the G350's VLAN table
- Ingress VLAN security — an explanation of the G350's ingress security mechanism
- ICC-VLAN — instructions on how to configure the ICC-VLAN
- VLAN CLI commands — a list and explanation of the CLI commands used to configure VLANs in the G350
- VLAN configuration examples — examples of how to use CLI commands to configure VLANs in the G350

VLAN overview

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.

The following figure illustrates how a simple VLAN can connect several endpoints in different locations and attached to different hubs. In this example, the Management VLAN consists of stations on numerous floors of the building which are connected to both Device A and Device B.

Figure 9: VLAN Overview



In virtual topological networks, the network devices can be located in diverse places around the LAN. These devices can be in different departments, on different floors, or in different buildings. Connection is achieved through software. Each network device is connected to a switch, and the network manager uses management software to assign each device to a virtual topological network. Elements can be combined into a VLAN even if they are connected to different devices.

You can use VLANs whenever there are one or more groups of network users that you want to separate from the rest of the network.

In the following figure, the switch has three separate VLANs: Sales, Engineering, and Marketing. Each VLAN has several physical ports assigned to it with PCs connected to those ports. When traffic flows from a PC on the Sales VLAN, for example, that traffic is *only* forwarded out the other ports assigned to that VLAN. Thus, the Engineering and Marketing VLANs are not burdened with processing that traffic.

Figure 10: VLAN Example.

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 following parameters:

- Port VLAN ID
- Tagging Mode

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 (e.g., type **`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 they entered through.

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 his or her own VLAN for privacy. The whole building has a shared high-speed connection to the ISP.

In order to accomplish this, the G350 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 it

The following figure shows these binding modes.

Figure 11: Multi VLAN Binding

Static Binding

- The user manually specifies the list of VLAN IDs to be bound to the port, up to eight VLANs
- Default mode for all ports
- Only VLAN 9, and any other VLANs statically configured on the port will be allowed to access this port

Bind to Configured

- The VLAN table of the port will support 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

G350 VLAN table

The G350 VLAN table lists all VLANs configured on the G350. You can configure up to eight VLANs. To display a list of VLANs, use the **`show vlan`** command.

When the VLAN table reaches its maximum capacity, you can not 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 the through that port. Unassigned packets receive the PVID of the port and are therefore allowed to enter.

ICC-VLAN

When the G350 includes an ICC, the ICC connects to the G350 via 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 type the **icc-vlan** command.

To show the current ICC-VLAN, type the **show icc-vlan** command from the general context.

The following example sets Vlan 2 as the ICC-VLAN:

```
G350-001(super)# interface vlan 2
G350-001(super-if:Vlan 2)# icc-vlan
Done!
G350-001(super-if:Vlan 2)# exit
G350-001(super)# show icc-vlan
VLAN 2
G350-001(super)#
```

VLAN CLI commands

The following commands are used to configure VLANs. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **clear port static-vlan** command to delete VLANs statically configured on a port.
- Use the **clear vlan** command to 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. When you clear a VLAN, all ports assigned to that VLAN are assigned to the default VLAN #1.
- Use the **interface vlan** command to create a VLAN interface, enter it into the VLAN table, and enter the Interface VLAN configuration mode.
- Use the **no interface vlan** command to delete a VLAN interface and remove the entry from the VLAN table.

- Use the **`set port static-vlan`** command to assign static VLANs to ports.
- Use the **`set port vlan`** command to set the port VLAN ID (PVID).
- Use the **`set port vlan-binding-mode`** command to define the binding method used by ports.
- Use the **`set trunk`** command to configure the VLAN tagging mode of a port.
- Use the **`set vlan`** command to configure VLANs.
- Use the **`show cam vlan`** command to display all mac entries in the CAM table for a specific vlan.
- Use the **`show interfaces vlan`** command to display interface configuration and statistics for a particular VLAN or all VLANs.
- Use the **`show port-vlan-binding`** command to display port VLAN binding mode information. If no module number is specified then information for all ports on all modules is displayed. If no port number is specified, information for all ports on the specified module is displayed.
- Use the **`show trunk`** command to display VLAN tagging information for the switch.
- Use the **`show vlan`** command to display the VLANs configured in the switch.

VLAN configuration examples

This section provides VLAN configuration examples.

The following example deletes a statically bound VLAN from a port:

```
G350-001(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:

```
G350-001(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:

```
G350-001(super)# interface Vlan 66
G350-001(super-if:Vlan 66)# icc-vlan
Done!
```

The following example enters configuration mode for a VLAN interface:

```
G350-001(super)# interface Vlan 66
G350-001(super-if:Vlan 66)#
```

The following example deletes a VLAN interface:

```
G350-001(super)# no interface vlan 66
Done!
```

The following example statically binds a VLAN to a port:

```
G350-001(super)# set port static-vlan 10/3 54
VLAN 54 is bound to port 10/3
```

The following example sets a port's VLAN ID:

```
G350-001(super)# set port vlan 54 10/3

VLAN 54 modified
VLAN     Mod/Ports

----     ---------------------------

 54      10/3
```

The following example sets a port's VLAN binding mode:

```
G350-001(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:

```
G350-001(super)# set trunk 10/3 dot1q
Dot1Q VLAN tagging set on port 10/3.
```

The following example creates a VLAN:

```
G350-001(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:

```
G350-001(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      10/2
00:02:4b:5b:28:40      54       6/13
```

The following example displays the ICC-VLAN:

```
G350-001(super)# show icc-vlan
VLAN 1
```

The following example displays interface configuration and statistics for a VLAN:

```
G350-001(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:

```
G350-001(super)# show port vlan-binding-mode 10
port 10/3 is bind to all configured VLANs
```

The following example displays VLAN tagging information:

```
G350-001(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:

```
G50-001(super)# show vlan

VLAN ID VLAN-name
------- --------------------------------
1       V1
54      Marketing
66      V66
2121    Training
Total number of VLANs: 4
```

Configuring port redundancy

This section contains information about port redundancy configuration on G350 switch ports and includes the following topics:

- Port redundancy overview — an overview of port redundancy on the G350
- Secondary port activation — a description of how the secondary port is activated
- Switchback — a description of how switchback occurs
- Port redundancy CLI commands — a list and description of the CLI commands used to configure port redundancy
- Port redundancy configuration examples — examples of port redundancy configurations

Port redundancy overview

Redundancy involves the duplication of devices, services, or connections, so, in the event of a failure, the redundant duplicate can take over for the one that failed.

Since computer networks are critical for business operations, it is vital to ensure that the network continues to function even if a piece of equipment fails. Even the most reliable equipment might fail on occasion, but a redundant component can ensure that the network continues to operate despite such failure.

To achieve port redundancy, you can define a redundancy relationship between any two ports in a switch. One port is defined as the primary port and the other as the secondary port. If the primary port fails, the secondary port takes over.

You can configure up to 25 pairs of ports per chassis. Each pair contains a primary and secondary port. You can configure any type of Ethernet port to be redundant to any other. You can configure redundant ports from among the Ethernet LAN port on the G350 front panel and the Ethernet ports (1-24) and the Gigabit Ethernet port (51) on the MM314 Media Module.

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 CLI commands

The following commands are used to configure port redundancy. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`set port redundancy enable/disable`** command to globally enable or disable the redundancy pairs you have defined. Using this command will not delete existing redundancy entries.
- Use the **`set port redundancy on/off`** command to define or remove redundancy pairs. Use the **`show port redundancy`** command to ensure that there is no redundancy scheme already defined on any of the links.
- Use the **`set port redundancy-intervals`** command to configure the two time constants that determine redundancy switchover parameters.
- Use the **`show port redundancy`** command to display information about software port redundancy schemes defined for the switch.

Note:

If you configure the Ethernet LAN port on the G350 front panel to be redundant with the Gigabit Ethernet port on the MM314 Media Module, the Ethernet LAN port becomes the primary port after resetting the G350 even if you configured the Gigabit Ethernet port to be primary. To prevent this, use the **`set port redundancy-intervals`** command with the switchback interval parameter set to 0.

Port redundancy configuration examples

This section provides port redundancy configuration examples.

The following example creates a port redundancy pair:

```
G350-003(super)# set port redundancy 6/3 6/5 on 1
Monitor: Port 6/5 is redundant to port 6/3.
Port redundancy is active - entry is effective immediately
```

The following example deletes a port redundancy pair:

```
G350-003(super)# set port redundancy 6/3 6/5 off
Entry Monitor removed: Port 6/5 is not redundant to port 6/3.
```

The following example enables all configured port redundancies:

```
G350-003(super)# set port redundancy enable
All redundancy schemes are now enabled
```

The following example disables all configured port redundancies:

```
G350-003(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:

```
G350-003(super)# set port redundancy-intervals 60 30
Done!
```

The following example displays port redundancy information:

```
G350-003(super)# show port redundancy

Redundancy Name     Primary Port        Secondary Port      Status
-----------------   --------------      ----------------    --------
Monitor               6/3                     6/5             primary
Minimum Time between Switchovers: 60
Switchback interval: 30
```

Configuring port mirroring

This section provides information about configuring port mirroring on G350 devices and includes the following topics:

- Port mirroring overview — an overview of port mirroring on the G350
- Port mirroring CLI commands — a list and description of the CLI commands used to configure port mirroring on the G350
- Port mirroring configuration examples — examples of port mirroring configurations

Port mirroring overview

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 port.

You can define one source port and one destination port on each G350 chassis for received (Rx), transmitted (Tx), or transmitted and received (both) traffic.

Port mirroring constraints

You cannot use the LAN port or the WAN Fast Ethernet port in port mirroring.

Port mirroring CLI commands

The following commands are used to configure port mirroring on the G350. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`set port mirror`** command to define a port mirroring pair in the switch.
- Use the **`show port mirror`** command to display mirroring information for the switch.
- Use the **`clear port mirror`** command to cancel port mirroring.

Port mirroring configuration examples

This section provides port mirroring configuration examples.

The following example creates a port mirroring pair:

```
G350-003(super)# set port mirror source-port 6/2 mirror-port 6/10
sampling always direction rx
Mirroring rx packets from port 6/2 to port 6/10 is enabled
```

The following example displays port mirroring information:

```
G350-003(super)# show port mirror
port mirroring
Mirroring both Rx and Tx packets from port 6/2 to port 6/10 is enabled
```

The following example disables port mirroring:

```
G350-003(super)# clear port mirror
```

Configuring spanning tree

This section provides information about configuring spanning tree on the G350 and contains the following topics:

- Spanning tree overview — an overview of spanning tree protocol
- Spanning tree CLI commands — a list and description of CLI commands used to configure spanning tree protocol on the G350
- Spanning tree configuration examples — examples of spanning tree protocol configurations

Spanning tree overview

G350 devices 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 a minute or so. 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.
- 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 G350 on a per-port basis to minimize this effect.

Rapid Spanning Tree Protocol (RSTP)

About the 802.1w (RSTP) standard

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 — port closest to the root bridge
- Designated port — 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 provides a means of fast network convergence after a topology change. It does this by assigning different treatments to different port types. The port types and the treatment they receive follow:

- 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, it's 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.

  Use the **`set port edge admin state`** command, 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. For example, the following command specifies that ports 5 to 13 on module 4 are edge ports:

  ```
  G350-001(super)# set port edge admin state 4/5-13 edge-port
  ```

  The following command specifies that port 6 on module 6 is not an edge port:

  ```
  G350-001(super)# set port edge admin state 6/6 non-edge-port
  ```

  Use the **`show port edge state`** command, 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.

- 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.

  Use the **`set port point-to-point admin status`** command, 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 parameters 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`* — tries to automatically detect the port's connection type

  For example, the following command specifies that ports 3 to 5 on module 5 are treated is if they were connected point-to-point:

  ```
  G350-001(super)# set port point-to-point admin status 5/3-5
  force-true
  ```

  Use the **`show port point-to-point status`** command, 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 CLI commands

Use the following commands to configure spanning tree. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`set port spantree`** command to enable or disable the spanning tree mode for specific switch ports.
- Use the **`set spantree default-path-cost`** command to set the version of the spanning tree default path cost used by this bridge.
- Use the **`set spantree enable/disable`** command to enable or disable the spanning tree algorithm.
- Use the **`set spantree forward-delay`** command to specify the time used when transferring the state of a port to the forwarding state.
- Use the **`set spantree hello-time`** command to specify the time interval between the generation of configuration BPDUs by the root.
- Use the **`set spantree max-age`** command to specify the time to keep an information message before it is discarded.
- Use the **`set spantree priority`** command to set the bridge priority for STP.

- Use the **`set spantree tx-hold-count`** command to 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.
- Use the **`set spantree version`** command to set the version of the spanning tree protocol.
- Use the **`show spantree`** command to display spanning-tree information.

Spanning tree configuration examples

This section provides spanning tree configuration examples.

The following example enables spanning tree on a port:

```
G350-003(super)# set port spantree enable 6/8
port 6/8 was enabled on spantree
```

The following example disables spanning tree on a port:

```
G350-003(super)# set port spantree disable 6/8
port 6/8 was disabled on spantree
```

The following example configures the version of the spanning tree default path cost used by this bridge:

```
G350-003(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:

```
G350-003(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:

```
G350-003(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:

```
G350-003(super)# set spantree max-age 21
bridge max age is set to 21.
```

The following example configures the bridge priority for spanning tree:

```
G350-003(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:

```
G350-003(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:

```
G350-003(super)# set spantree version rapid-spanning-tree
Spanning tree version is set to rapid spanning tree.
```

The following example displays spanning tree information:

```
G350-003(super)# show spantree
```

```
Spanning tree state is enabled
Designated Root:  00-40-0d-92-22-81
Designated Root Priority: 32768
Designated Root Cost: 19
Designated Root Port: 6/24
Root Max Age: 20   Hello Time: 2
Root Forward Delay: 15
Bridge ID MAC ADDR: 00-04-0d-29-c4-ca
Bridge ID priority: 36864
Bridge Max Age: 21        Bridge Hello Time: 2
Bridge Forward Delay: 16  Tx Hold Count 4
Spanning Tree Version is rapid spanning tree
Spanning Tree Default Path Costs is according to common spanning tree
```

```
Port   State         Cost       Priority
------ ------------- ---------- ------------
6 /1   not-connected 100        128
6 /2   not-connected 100        128
6 /3   not-connected 100        128
6 /4   not-connected 100        128
6 /5   not-connected 100        128
6 /6   not-connected 100        128
6 /7   not-connected 100        128
6 /8   not-connected 100        128
6 /9   not-connected 100        128
6 /10  not-connected 100        128
6 /11  not-connected 100        128
6 /12  not-connected 100        128
6 /13  Forwarding    19         128
6 /14  not-connected 100        128
6 /15  not-connected 100        128
6 /16  not-connected 100        128
6 /17  Forwarding    19         128
6 /18  Forwarding    19         128
6 /19  not-connected 100        128
6 /20  not-connected 100        128
```

```
6 /21  not-connected 100        128
6 /22  Forwarding    19         128
6 /23  Forwarding    19         128
6 /24  Forwarding    19         128
6 /51  not-connected 4          128
```

Port classification

This section provides information on configuring port classification on the G350 and includes the following topics:

- Port classification overview — an overview of port classification on the G350
- Port classification CLI commands — a list and description of the CLI commands used to configure port classification on the G350
- Port classification configuration examples — examples of port classification configurations

Port classification overview

With the G350, 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 1GB port is classified as valuable by default.

Port classification CLI commands

Use the following commands to configure port classification. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`set port classification`** command to 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.
- Use the **`show port classification`** command to display a port's classification.

Port classification configuration examples

This section provides port classification configuration examples.

The following example classifies a port as a valuable port:

```
G350-003(super)# set port classification 6/4 valuable
Port 6/4 classification has been changed.
```

The following example displays the port classification of all ports on the device:

```
G350-003(super)# show port classification
Port      Port Classification
--------  -------------------------
6/1       regular
6/2       regular
6/3       regular
6/4       valuable
6/5       regular
6/6       regular
6/7       regular
6/8       regular
6/9       regular
6/10      regular
6/11      regular
6/12      regular
6/13      regular
6/14      regular
6/15      regular
6/16      regular
6/17      regular
6/18      regular
6/19      regular
6/20      regular
6/21      regular
6/22      regular
6/23      regular
6/24      regular
6/51      valuable
10/3      regular
```

Chapter 14: Configuring contact closure

This chapter provides information about configuring the G350's contact closure feature and contains the following sections:

- Contact closure overview — an overview of contact closure configuration on the G350
- Contact closure hardware configuration — instructions on how to configure the contact closure hardware
- Contact closure software configuration — instructions on how to configure the G350 to use contact closure
- Showing contact closure status — instructions on how to display the contact closure configuration

Contact closure overview

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 Avaya G350 Media Gateway to use a media server with Avaya Communication Manager software. For more information, see Configuring the Media Gateway Controller (MGC) on page 51.

It is recommended that you use an Avaya Partner Contact Closure Adjunct™ for contact closure. For more information, see *Overview of the Avaya G350 Media Gateway*, 555-245-201. 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 Avaya G350 Manager.

Note:

Configuration of the feature access code is performed through the Avaya Communication Manager. For more information, see *Administrator's Guide for Avaya Communication Manager*, 555-233-506.

Contact closure hardware configuration

To configure your hardware for contact closure:

1. Connect an Avaya Partner Contact Closure Adjunct to the Contact Closure port on the Avaya G350 Media Gateway front panel. The Contact Closure port is labeled CC. Use a telephone cable with standard RJ-11 connectors.
2. 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 of the Avaya G350 Media Gateway*, 555-245-201.

Contact closure software configuration

You can specify the following 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.

To configure the Avaya G350 Media Gateway to activate contact closure when the feature access code is dialed:

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 5 seconds after the call controller triggers contact closure in the relay.

   ```
   set contact-closure pulse-duration 10/1:2 5
   ```

To activate contact closure manually, 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
```

To deactivate contact closure manually, 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

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.

```
G350-101(super)# show contact-closure

MODULE   PORT   RELAY   ADMIN            PULSE DURATION (secs)   STATUS
-------  -----  ------  ----------------  ---------------------- ------
10       1      1       mgc               5 secs                  off
10       1      2       mgc               3 secs                  off
```

Chapter 15: Configuring RMON monitoring

This chapter provides information on monitoring the G350 and includes the following sections:

- RMON overview — an overview of the RMON network monitoring standard
- RMON CLI commands — a list and description of the CLI commands used to configure RMON monitoring on the G350
- RMON configuration examples — examples of RMON configurations

RMON overview

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 Avaya G350 Media Gateway. The G350 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 CLI commands

Use the following commands to configure RMON. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`rmon alarm`** command to create an RMON alarm entry.
- Use the **`rmon event`** command to create an RMON event entry.
- Use the **`rmon history`** command to create an RMON history entry.
- Use the **`show rmon alarm`** command to display all RMON alarm entries.
- Use the **`show rmon event`** command to display RMON event entries.
- Use the **`show rmon history`** command to display RMON alarm entries.
- Use the **`show rmon statistics`** command to display RMON statistics.

RMON configuration examples

This section provides RMON configuration examples.

The following example creates an RMON alarm entry:

```
G350-003(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:

```
G350-003(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 24 of the module in slot 6, recording activity over 60 intervals (buckets) of 20 seconds each.

```
G350-003(super)# rmon history 80 6/24 interval 20 buckets 60 owner root
history index 80 was created successfully
```

The following example displays information about an RMON alarm entry:

```
G350-003(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:

```
G350-003(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:

```
G350-003(super)# show rmon history 80

history

Entry 80 is active, owned by root
Monitors the port 6/24 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:

```
G350-003(super)# show rmon statistics 6/24

Statistics for port 6/24 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,
```

Chapter 16: Configuring the router

This chapter provides information about configuring the G350 router and contains the following sections:

- Overview of the G350 router — a list of features supported on the G350 router, along with instructions for enabling and disabling the router
- Configuring interfaces — instructions on how to configure Fast Ethernet, Loopback, Serial, and VLAN interfaces on the router
- Configuring the routing table — instructions on how to configure the routing table
- Configuring GRE tunneling — instructions on how to configure GRE tunnels on the router
- Configuring DHCP and BOOTP relay — instructions on how to configure DHCP and BOOTP relays for routing on the G350
- Configuring DHCP server — instructions on how to configure DHCP server on the G350
- Configuring broadcast relay — instructions on how to configure broadcast relay for routing on the G350
- Configuring the ARP table — instructions on how to configure the ARP table
- Enabling proxy ARP — instructions on how to enable proxy ARP on an interface
- Configuring ICMP errors — instructions on how to configure whether the router sends ICMP error messages
- Configuring RIP — instructions on how to configure RIP parameters for each interface on the router
- Configuring OSPF — instructions on how to configure OSPF parameters for each interface on the router
- Route redistribution — instructions on how to configure route redistribution among multiple routing protocols
- Configuring VRRP — instructions on how to configure the VRRP protocol so as to support redundancy of LAN routers and load balancing
- Configuring fragmentation — instructions on how to configure IP fragmentation and reassembly on the G350 router

Overview of the G350 router

The Avaya G350 Media Gateway has an internal router. You can configure the following routing features on the router:

- Interfaces
- Routing table
- GRE tunneling
- DHCP and BOOTP relay
- Broadcast relay
- ARP table
- ICMP errors
- RIP
- OSPF
- Route redistribution
- VRRP
- Fragmentation

Use the **`ip routing`** command to enable the router. Use the **`no`** form of this command to disable the router.

Configuring interfaces

This section provides information about configuring interfaces on the router and includes the following topics:

- Router interface concepts — a description of the types of interfaces that you can configure on the G350 router
- IP Interface configuration commands — a list and descriptions of the CLI commands used to configure interfaces on the G350 router
- Interface configuration examples — examples of router interface configurations

Router interface concepts

The router in the Avaya G350 Media Gateway includes the following interface categories:

- physical
- Layer 2 virtual
- Layer 3 routing

Physical router interfaces

The following are the physical interfaces of the G350 router:

- **WAN Interfaces** — When you add a WAN media module to the Avaya G350 Media 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.
- **Fast Ethernet Interface** — The 10/3 Fast Ethernet port on the front panel of the G350 provides a Fast Ethernet interface. This interface is an autosensing 10/100Mbps 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 91.
- **Switching Interface** — An internal 100Mbps connection to the G350 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 G350 without an external VPN or firewall, Vlan 1 is used to connect the internal G350 router to the internal G350 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 Configuring GRE tunneling on page 166.

Layer 2 logical interfaces

- **VLAN (on the Switching Interface)** — The G350 switch can have multiple VLANs defined within its switching fabric. The G350 router supports up to eight VLANs that can be configured over its internal switching interface connection.
- **Serial Interface** — A 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 Initial WAN configuration on page 85.

  Note:

  One or more IP interfaces can be defined over each serial, Fast Ethernet, switching, and Loopback interface.

IP Interface configuration commands

To configure an interface:

1. To create an interface, type the **`interface`** command, 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 2/1
   ```

2. Use the **`ip address`** command, 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.

Use the following commands to configure the interface parameters. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`ip admin-state`** command to set the administrative state of the IP interface. The default state is up.
- Use the **`ip broadcast-address`** command to update the interface broadcast address.

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:

```
G350-001# interface FastEthernet 10/2
G350-001(if:FastEthernet 10/2)# 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:

```
G350-001# interface Vlan 2
G350-001(if:Vlan 2)# ip address 10.30.50.70 255.255.0.0
Done!
```

Configuring the routing table

This section provides information about configuring the routing table and includes the following topics:

- Overview of the routing table — an overview of the routing table and the types of routes you can configure on the routing table
- Via-interface static route — instructions on how to configure a via interface static route
- Permanent static route — instructions on how to configure a permanent static route
- Discard route — instructions on how to configure a discard route
- Routing table commands — a list and descriptions of CLI commands used to configure the routing table

Overview of the routing table

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 165. When the underlying Layer 2 interface becomes active, the static route enters the routing table again.

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. See Via-interface static route on page 165.
- **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 Avaya G350 Media Gateway has an IP interface.

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.

Static routes can be advertised by routing protocols, such as RIP and OSPF. For more information, see Route redistribution on page 197. Static routes also support load-balancing similar to OSPF. 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 it's own **`ip route`** command.

Using the **`no ip route`** command deletes the route including all of its 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, perform one of the following:

- Use the single **`ip route 10.1.1.0 24 149.49.54.1 149.49.75.1`** command specifying all next-hops together,

Or

- Use the individual **`ip route 10.1.1.0 24 149.49.54.1`** and **`ip route 10.1.1.0 24 149.49.75.1`** commands.

Next-hops can only be added to an existing static route if they have the same preference and metric as the currently defined next-hops.

Note:

Metrics are used to choose between routes of the same protocol. Preferences are used to choose between routes of different protocols.

The Avaya G350 Media Gateway supports the following Static Route configurations:

- Via-interface static route
- Permanent static route
- Discard route

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 2/1:1`** creates a static route to the network 193.168.10.0 24 via the Serial 2/1:1 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-hops are required, each must be configured by separate **`ip route`** commands.

Permanent static route

The Avaya G350 Media 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 2/1:1 permanent`** creates a permanent static route to the network 193.168.10.0 24 via the Serial 2/1:1 interface.

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 97.

Discard route

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, and is configured using the **`ip route <network> <mask> null0`** command.

For example, the command **`ip route 134.66.0.0 16 Null0`** configures the network 134.66.0.0 16 as a discard route.

Routing table commands

Use the following commands to configure the routing table. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`clear ip route all`** command to delete all dynamic routing entries from the routing table.
- Use the **`ip default-gateway`** command to define a default gateway for the router. Use the **`no`** form of this command to remove the default gateway.
- Use the **`ip route`** command to establish a static route. Use the **`no`** form of this command to remove a static route.
- Use the **`show ip route`** command to display information about the IP routing table.
- Use the **`show ip route best-match`** command, followed by an IP address, to display a routing table for a destination address.
- Use the **`show ip route static`** command to display static routes.
- Use the **`show ip route summary`** command to display the number of routes known to the device.
- Use the **`traceroute`** command, followed by an IP address, to trace the route an IP packet would follow to the specified IP address. The G350 traces the route by launching UDP probe packets with a small time to live (TTL), then listening for an ICMP time exceeded reply from a gateway.

Configuring GRE tunneling

This section provides information about configuring GRE tunnels and contains the following topics:

- GRE tunneling overview — an overview of GRE tunneling
- Setting up a GRE tunnel — instructions on how to configure a GRE tunnel
- Routing packets to a GRE tunnel — instructions on how to route packets to a GRE tunnel
- Preventing nested tunneling in GRE tunnels — instructions on how to prevent GRE tunnels from causing loops
- Optional GRE tunnel features — a description of optional features you can configure on GRE tunnels
- Additional GRE tunnel parameters — a list and description of additional GRE tunnel parameters
- GRE tunnel application example — a sample application for GRE tunneling

GRE tunneling overview

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 the following: 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 97.

For an example of a GRE tunneling application, see GRE tunnel application example on page 175.

Routing packets 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 Configuring the routing table on page 163.
- 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 Configuring policy-based routing on page 273.

Preventing 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 G350 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 reconfigured to eliminate the nested tunneling.

In addition to checking for nested tunneling, the G350 prevents loops in connection with GRE tunnels by preventing the same packet from being encapsulated more than once in the G350.

Several things can lead to nested tunneling in a GRE tunnel:

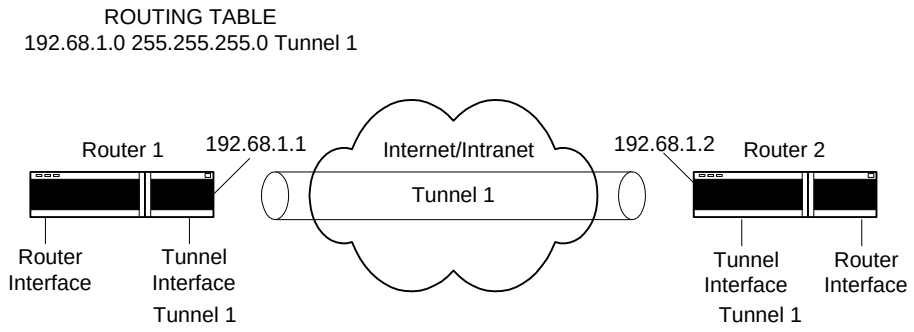
- A static route exists on the source tunnel endpoint that tells the tunnel to route packets addressed to the receiving tunnel endpoint via the tunnel itself.
- The local endpoint of the tunnel learns the tunnel as a route to the tunnel's remote endpoint via OSPF or RIP.

- A combination of static routes via parallel tunnels lead to a situation in which each tunnel is routing packets via another tunnel. For example:

```
G350-001(super)# interface tunnel 1
G350-001(super-if:Tunnel 1)# tunnel source x.x.x.x
G350-001(super-if:Tunnel 1)# tunnel destination 1.0.0.1
Done!
G350-001(super-if:Tunnel 1)# exit
G350-001(super)# interface tunnel 2
G350-001(super-if:Tunnel 2)# tunnel source x.x.x.x
G350-001(super-if:Tunnel 2)# tunnel destination 2.0.0.1
Done!
G350-001(super-if:Tunnel 2)# exit
G350-001(super)# interface tunnel 3
G350-001(super-if:Tunnel 3)# tunnel source x.x.x.x
G350-001(super-if:Tunnel 3)# tunnel destination 3.0.0.1
Done!
G350-001(super-if:Tunnel 3)# exit
G350-001(super)# ip route 1.0.0.1 tunnel 2
Done!
G350-001(super)# ip route 2.0.0.1 tunnel 3
Done!
G350-001(super)# ip route 3.0.0.1 tunnel 1
Done!
```

Using the network shown in Figure 12 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.

Figure 12: Nested Tunneling Example



The following are recommended ways to avoid nested tunneling:

- Announce policy.

  Configure a policy rule on the receiving tunnel endpoint (router 2) that will cause the receiving endpoint to block advertisements of the source network (192.68.1.0) in its routing updates. This will prevent 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 12 as an illustration, you would configure the following policy rule on router 2 and activate it on the router RIP with the matching interface:.

```
G350-001(super)# ip distribution access-list-name 1 "list #1"
Done!
G350-001(super)# ip distribution access-default-action 1 default-action-permit
Done!
G350-001(super)# ip distribution access-list 1 10 "deny" 192.68.1.0 0.0.0.255
Done!
G350-001(super)# router rip
G350-001(super router:rip)# distribution-list 1 out FastEthernet 10/2
Done!
G350-001(super router:rip)# exit
G350-001(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 Figure 12 as an illustration, you would configure the following policy rule on router 1 and activate it on the router RIP with the matching interface:

```
G350-001(super)# ip distribution access-list-name 1 "list #1"
Done!
G350-001(super)# ip distribution access-default-action 1 default-action-permit
Done!
G350-001(super)# ip distribution access-list 1 10 "deny" 192.68.1.0 0.0.0.255
Done!
G350-001(super)# router rip
G350-001(super router:rip)# distribution-list 1 in FastEthernet 10/2
Done!
G350-001(super router:rip)# exit
G350-001(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:

```
G350-001(super)# ip route 192.68.1.2 255.255.0.0 192.68.1.3 high permanent
Done!
G350-001(super)#
```

Optional GRE tunnel features

You can configure the following optional features in GRE tunnels:

- keepalive — enables periodic checking to determine if the tunnel is up or down.
- Dynamic MTU discovery — determines and updates the lowest MTU on the current route through the tunnel.

keepalive

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.

Use the **keepalive** command in the context of the GRE tunnel interface to enable the tunnel keepalive feature. Use the **no** form of this command to deactivate the feature.

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.

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.

```
G350-001# interface Tunnel 1
G350-001(if:Tunnel 1)# tunnel keepalive 20 3
Done!
```

Note:

You do not have to configure tunnel keepalive on both sides of the tunnel.

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 Overview of fragmentation on page 201.

Use the **`tunnel path-mtu-discovery`** command in the context of the GRE tunnel interface to enable dynamic MTU discovery by the tunnel. Use the **no** form of this command to deactivate the feature.

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.

Setting up a GRE tunnel

To set up a GRE tunnel:

1. Use the **`interface tunnel`** command, followed by a number identifying the tunnel, to create the new tunnel interface. If you are changing the parameters of an existing tunnel, use the **`interface tunnel`** command, followed by a number identifying the tunnel, to enter the context of the tunnel. For example:

```
G350-001(super)# interface tunnel 2
G350-001(super-if:Tunnel 2)#
```

2. In the interface context, use the **`tunnel source`** command, followed by the public IP address of the local tunnel endpoint, to set the source address of the tunnel. For example:

```
G350-001(super-if:Tunnel 2)# tunnel source 70.70.70.2
Done!
G350-001(super-if:Tunnel 2)#
```

3. In the interface context, use the **`tunnel destination`** command, followed by the IP address of the remote tunnel endpoint, to set the destination address of the tunnel. For example:

```
G350-001(super-if:Tunnel 2)# tunnel destination 20.0.1.1
Done!
G350-001(super-if:Tunnel 2)#
```

Note:

The Avaya G350 Media Gateway does not check whether the configured tunnel source IP address is an existing IP address registered with the G350 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 on page 171.

   To configure keepalive for a tunnel interface, type the keepalive command in the 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.

```
G350-001(super-if:Tunnel 2)# keepalive 20 3
Done!
G350-001(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 172.

   The following example configures dynamic MTU discovery, with an age timer of 15 minutes.

```
G350-001(super-if:Tunnel 2)# tunnel path-mtu-discovery age-timer 15
Done!
G350-001(super-if:Tunnel 2)#
```

6. Type the **`copy running-config startup-config`** command. This saves the new tunnel interface configuration in the startup configuration file.

For a list of optional GRE tunnel features, refer to Optional GRE tunnel features on page 171. For a list of additional GRE tunnel CLI commands, refer to Additional GRE tunnel parameters on page 174.

Additional GRE tunnel parameters

Use the following commands to configure additional GRE tunnel parameters. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`tunnel checksum`** command in the context of the GRE tunnel interface to 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. Use the **no** form of this command to disable checksums.
- Use the **`tunnel key`** command in the context of the GRE tunnel interface to 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. Use the **no** form of this command to disable key checking.
- Use the **`tunnel DSCP`** command in the context of the GRE tunnel interface to 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 between 0 and 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.
- Use the **`tunnel TTL`** command in the context of the GRE tunnel interface to 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 between 1 and 255. The default tunnel TTL value is 255.
- Use the **`show interface tunnel`** command to show interface configuration and statistics for a particular tunnel or all GRE tunnels.

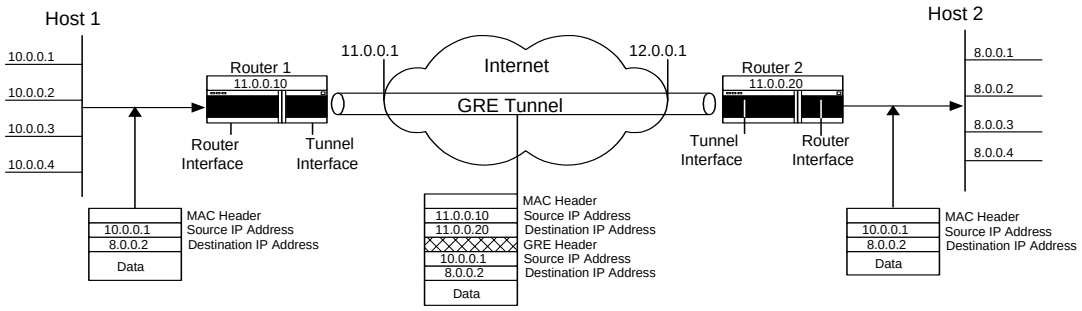
  Note:

  If the tunnel interface is down, the **`show interface tunnel`** command displays the MTU value as *not available*.

GRE tunnel application example

This section provides an example of a GRE tunnel application and its configuration.

Figure 13: Simple GRE tunneling application example



In the example shown in Figure 13, Host 1 and Host 2 are private networks using a GRE tunnel to connect them via the Internet. 11.0.0.10 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:

Router 1 Configuration

```
G350-001(super)# interface FastEthernet 10/2
G350-001(super-if:FastEthernet 10/2)# ip address 11.0.0.10 255.255.255.0
G350-001(super-if:FastEthernet 10/2)# exit
G350-001(super)# interface tunnel 1
G350-001(super-if:Tunnel 1)# keepalive 10 3
Done!
G350-001(super-if:Tunnel 1)# tunnel source 11.0.0.10
Done!
G350-001(super-if:Tunnel 1)# tunnel destination 12.0.0.20
Done!
G350-001(super-if:Tunnel 1)# ip address 1.1.1.1 255.255.255.0
Done!
G350-001(super-if:Tunnel 1)# exit
G350-001(super)# ip route 12.0.0.0 255.255.255.0 11.0.0.1 1 high
G350-001(super)# router ospf
G350-001(super router:ospf)# network 1.1.1.0 0.0.0.255 area 0.0.0.0
Done!
G350-001(super router:ospf)# exit
G350-001(super)#
```

Router 2 Configuration

```
G350-001(super)# interface vlan 1
G350-001(super-if:Vlan 1)# ip address 12.0.0.10 255.255.255.0
G350-001(super-if:Vlan 1)# exit
G350-001(super)# interface tunnel 1
G350-001(super-if:Tunnel 1)# tunnel source 12.0.0.20
Done!
G350-001(super-if:Tunnel 1)# tunnel destination 11.0.0.10
Done!
G350-001(super-if:Tunnel 1)# ip address 1.1.1.2 255.255.255.0
G350-001(super-if:Tunnel 1)# exit
G350-001(super)# ip route 11.0.0.0 255.255.255.0 12.0.0.1 1 high
G350-001(super)# router ospf
G350-001(super router:ospf)# network 1.1.1.0 0.0.0.255 area 0.0.0.0
Done!
G350-001(super router:ospf)# exit
G350-001(super)#
```

Configuring 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 G350 can alternatively function as a DHCP server, providing DHCP service to local devices. For information about configuring DHCP server on the G350, see Configuring DHCP server on page 179.

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 diskette drive. It is used when the user or station location changes frequently. The protocol is defined by RFC 951.

DHCP/BOOTP relay

The Avaya G350 Media 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 G350 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 G350 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 G350 with the relay address on that subnet so the DHCP/BOOTP server can accept the request.

DHCP/BOOTP Relay in G350 is configurable per VLAN and allows for two DHCP/BOOTP servers to be specified. In this case, the G350 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 G350.

DHCP/BOOTP relay commands

Use the following commands to configure DHCP relay and BOOTP relay:

- Use the **`ip bootp-dhcp network`** command to 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. Use the **no** form of this command to restore the default value. You must be in interface context to use this command.
- Use the **`ip bootp-dhcp relay`** command to enable relaying of BOOTP and DHCP requests to the BOOTP/DHCP server. Use the **no** form of this command to disable relaying of BOOTP and DHCP requests. You must be in general context to use this command.
- Use the **`ip bootp-dhcp server`** command to add a BOOTP/DHCP server to handle BOOTP/DHCP requests received by this interface. A maximum of two servers can be added to a single interface. Use the **no** form of this command to remove a server. You must be in interface context to use this command.

Configuring DHCP server

The G350 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 G350, local branch devices are not dependant on receiving configuration parameters over the WAN from a remote DHCP server and therefore can be assigned IP configuration parameters in case of WAN failure.

The G350 supports the following DHCP server features:

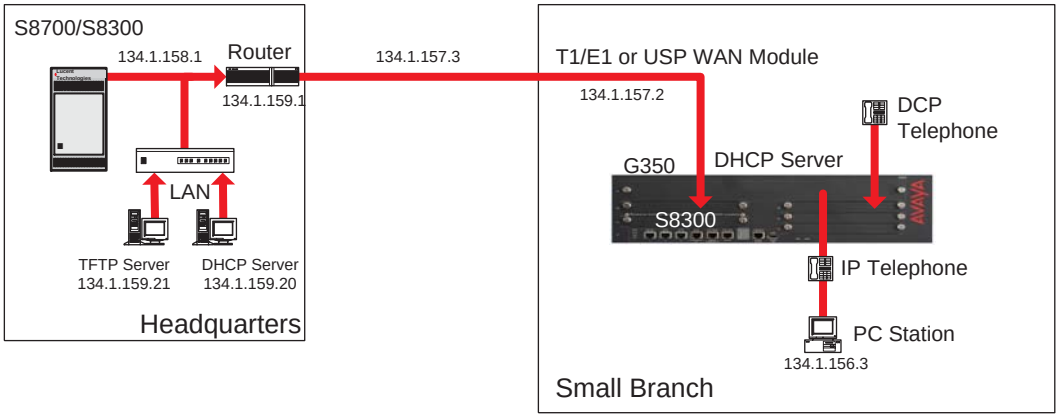
- Up to 32 DHCP pools
- Up to 120 users
- Up to 256 IP addresses for all DHCP pools together
- Automatic and reservation pools
- Standard DHCP options and IP phone and wireless special options
- Vendor specific information option
- DHCP relay packets
- Global statistics
- Syslog/traps for special events

The G350 Media Gateway can function as a DHCP server or 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 G350 to provide DHCP service to voice devices while DHCP requests by data devices are routed to a central remote DHCP server using DHCP relay.

Application — G350 as a DHCP server and router

In the typical application shown in Figure 14, the G350 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. In case of WAN failure, the local DHCP server can still allocate 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.

Figure 14: G350 as server and router



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 G350 also supports reservation pools, which map hardware addresses/client identifiers to specific IP addresses. Reservation pools may be required for security issues or VPN appliances.

Overlap between pools is not allowed. You cannot configure a reservation pool on an IP address that falls within the range of another pool.

DHCP server CLI configuration

To configure DHCP server on the G350:

1. Use the **`ip dhcp pool`** command, 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.
   - The start IP address and end IP address can be in the range of 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 182 and, for vendor specific options, Configuring vendor-specific options on page 183.
8. Repeat steps 1-7 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 **`ic dhcp activate pool`** command in general context, followed by the pool number.
10. Use the **`ip dhcp-server`** command 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 which is not part of the current network and beyond the allowed maximum of 256 IP addresses, you must first enter the **`no start ip address`** and **`no end ip address`** before configuring the new start and end IP addresses.

Configuring Options

DHCP options are various types of network configuration information that the DHCP client can receive from the DHCP server. The G350 supports all DHCP options. The most common options used for IP phones are listed in Table 8. Some options are configured with specific CLI commands, which are also listed in Table 8. Options 0, 50, 51, 52, 53, 54, 55, 56, and 255 are not configurable.

Table 8: Common user-configurable DHCP options

Option	Description	Specific command
1	Subnet Mask	**`subnet-mask`**
3	Router	**`default-router`**
6	Domain name server	**`dns_server`**
7	Log Server	
15	Domain Name	**`domain-name`**
43	vendor-specific information	**`vendor-specific-option`**
44	Wins/NBNS server	
46	Wins/NBT Node Type	
51	IP Address Lease Time	**`lease`**
66	TFTP server name	
69	SMTP server	
176	Avaya IP phone private	

To configure an option:

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 Table 8 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.

Configuring vendor-specific options

You can configure an option unique to an individual vendor class. This is called a vendor-specific option (option 43).

To configure a vendor-specific option:

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.

DHCP pool configuration examples

The following example defines a dynamic pool for voice devices

```
G350-001(super)# ip dhcp pool 1
G350-001(super-DHCP 1)# name "IP phone Pool"
Done!
G350-001(super-DHCP 1)# start-ip-addr 135.64.20.2
Done!
G350-001(super-DHCP 1)# end-ip-addr 135.64.20.30
Done!
G350-001(super-DHCP 1)# subnet-mask 255.255.255.0
Done!
G350-001(super-DHCP 1)# default-router 135.64.20.1
Done!
G350-001(super-DHCP 1)# option 176
G350-001(super-DHCP 1/option 176)# name "Avaya IP phone option"
Done!
G350-001(super-DHCP 1/option 176)# value ascii "MCIPADD=10.10.2.140,
MCPORT=1719, TFTPSRVR=10.10.5.188"
Done!
350-001(super-DHCP 1/option 176)# exit
G350-001(super-DHCP 1)# exit
G350-001(super)# ip dhcp activate pool 1
Done!
G350-001(super)# ip dhcp-server
Done!
G350-001(super)#
```

The following example defines a dynamic pool for data devices:

```
G350-001(super)# ip dhcp pool 2
G350-001(super-DHCP 2)# name "Data Pool"
Done!
G350-001(super-DHCP 2)# start-ip-addr 135.64.20.34
Done!
G350-001(super-DHCP 2)# end-ip-addr 135.64.20.60
Done!
G350-001(super-DHCP 2)# subnet-mask 255.255.255.0
Done!
G350-001(super-DHCP 2)# default-router 135.64.20.33
Done!
G350-001(super-DHCP 2)# dns-server 10.10.1.1
Done!
G350-001(super-DHCP 2)# domain-name my.domain.com
Done!
```

```
G350-001(super-DHCP 2)# option 176
G350-001(super-DHCP 2/option 176)# value ascii "MCIPADD=192.168.50.17,
192.168.50.15, MCPORT=1719, TFTPSRVR=192.168.50.1, TFTPDIR=/phonedir/"
Done!
G350-001(super-DHCP 2/option 176)# exit
G350-001(super-DHCP 2)# exit
G350-001(super)# ip dhcp activate pool 2
Done!
G350-001(super)# ip dhcp-server
Done!
G350-001(super)#
```

The following example configures a vendor-specific option for DHCP pool 5:

```
G350-001(super-DHCP 5)# vendor-specific-option 1
G350-001(super-DHCP 5/vendor specific 1)# class-identifier
"ccp.avaya.com"
Done!
G350-001(super-DHCP 5/vendor specific 1)# value raw ascii "gfdgfd"
Done!
G350-001(super-DHCP 5/vendor specific 1)# exit
G350-001(super-DHCP 5)#
```

The following example defines a reservation pool for data devices:

```
G350-001(super)# ip dhcp pool 3
G350-001(super-DHCP 3)# name "Data 1 Server"
Done!
G350-001(super-DHCP 3)# start-ip-addr 135.64.20.61
Done!
G350-001(super-DHCP 3)# end-ip-addr 135.64.20.61
Done!
G350-001(super-DHCP 3)# subnet-mask 27
Done!
G350-001(super-DHCP 3)# client-identifier 01:11:22:33:44:55:66
Done!
G350-001(super-DHCP 3)# default-router 135.64.20.33
Done!
G350-001(super-DHCP 3)# dns-server 10.10.1.1
Done!
G350-001(super-DHCP 3)# exit
G350-001(super)# ip dhcp activate pool 3
Done!
G350-001(super)#
```

Configuring broadcast relay

When you configure broadcast relay, the router forwards broadcast packets across interfaces. You can configure the following types of broadcast relay:

- Directed broadcast forwarding
- NetBIOS rebroadcast
- DHCP and BOOTP client broadcast

For more information about DHCP and BOOTP client broadcast, see Configuring DHCP and BOOTP relay on page 177.

Directed broadcast forwarding

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 Avaya G350 Media Gateway, you can configure whether the G350 forwards directed broadcast packets to the network address or subnet mask address of the interface.

Use the **`ip directed-broadcast`** command 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 Avaya G350 Media 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.

Use the **`ip netbios-rebroadcast both`** command to enable NetBIOS rebroadcasts on an interface. Use the **`ip netbios-rebroadcast disable`** command to disable NetBIOS rebroadcasts on an interface.

Configuring the ARP table

When you configure the 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

Note:

To change an entry in the ARP table, delete the entry and add it back with revised parameters.

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 (Address Resolution Protocol).

The ARP table

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.

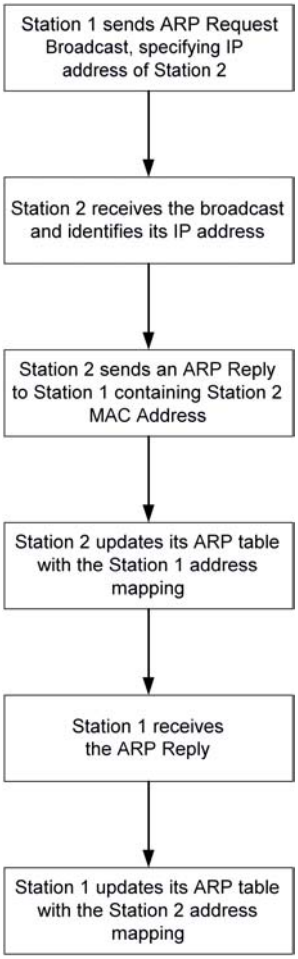
There are two types of entries in the ARP table:

- Static ARP table entries
- Dynamic ARP table entries

Static ARP table entries do not expire. You add static ARP table entries manually with 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:

```
G350-001# arp 192.168.7.8 00:40:0d:8c:2a:01
```

Dynamic ARP table entries are mappings between IP addresses and MAC addresses that the switch used recently. Dynamic ARP table entries expire after an amount of time that you can configure. The following figure shows how a switch adds dynamic ARP table entries:



You can 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:

```
G350-001# no arp 192.168.13.76
```

ARP table commands

Use the following commands to configure the ARP table. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`arp`** command to add a permanent entry to the Address Resolution Protocol (ARP) table. Use the **`no`** form of this command to remove either a static entry or a dynamically learned entry from the ARP table.
- Use the **`arp timeout`** command to configure the amount of time, in seconds, that an entry remains in the ARP table. Entering the **`arp timeout`** command without a time parameter will display the current timeout value. Use the **`no`** form of this command to restore the default value (four hours).
- Use the **`clear arp-cache`** command to delete all dynamic entries from the ARP table and the IP route cache.
- Use the **`ip max-arp-entries`** command to specify the maximum number of ARP table entries allowed in the ARP table. Use the **`no`** form of this command to restore the default value.
- Use the **`show ip arp`** command to display a list of the ARP resolved MAC to IP addresses in the ARP table.
- Use the **`show ip reverse-arp`** command to display the IP address of a host, based on a known MAC address.

Enabling proxy ARP

The G350 supports proxy ARP. Proxy ARP is a technique by which a router provides a false identity when answering ARP requests intended for another device. By falsifying its identify, the router accepts responsibility for routing packets to their true destination.

Proxy ARP can help devices on a subnet to reach remote subnets without the need to configure routing or a default gateway.

To enable proxy ARP on a G350 interface, use the **`ip proxy-arp`** command. Use the **`no`** form of this command to disable proxy ARP on an interface.

Configuring 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. Use the following commands to configure ICMP errors:

- Use the **`ip icmp-errors`** command to set ICMP error messages to ON. Use the **no** form of this command to set ICMP error messages to OFF.
- Use the **`show ip icmp`** command to display the status (enabled or disabled) of ICMP error messages.

Configuring RIP

This section provides information about configuring RIP parameters for router interfaces and contains the following topics:

- RIP overview — an overview of the RIP protocol
- Preventing routing loops in RIP — instructions on how to use RIP features to prevent routing loops
- RIP distribution access lists — instructions on how to configure RIP distribution access lists
- RIP limitations — a description of the limitations on the use of RIP on the G350
- RIP commands — a list and description of CLI commands used to configure RIP

RIP overview

The Routing Information Protocol (RIP) enables routers to compute the path that an IP packet should follow. Routers exchange routing information using RIP to determine routes that other routers are connected to. OSPF is a newer protocol that serves a similar purpose. For more information about OSPF, see Overview of OSPF on page 194.

You can configure route redistribution between OSPF, RIP, and static routes. With route redistribution, you can configure the G350 to redistribute routes learned from one protocol into the domain of the other routing protocol. For more information, see Route redistribution on page 197.

RIP is a distance vector protocol. The router decides which path to use on distance or the number of intermediate hops. In order for this protocol to work correctly, all the routers, and possibly the nodes, need to gather information on how to reach each destination in the Internet.

The very simplicity of RIP has a disadvantage however. This protocol does not take into account network bandwidth, physical cost, and data priority. The Avaya G350 Media Gateway supports two versions of RIP:

- RIPv1
- RIPv2

RIPv1

RIPv1 is the original version of the RIP protocol. The RIPv1 protocol imposes some limitations on the network design with regard to subnetting. When operating RIPv1, you must not configure variable length subnetwork masks (VLMS). Each IP network must have a single mask, implying that all subnetworks in a given IP network are of the same size. Also, when operating RIPv1, you must not configure supernets. RIPv1 is defined in RFC 1058.

RIPv2

RIPv2 is a newer version of the RIP routing protocol. RIPv2 solves some of the problems associated with RIPv1. The most important change in RIPv2 is the addition of a subnetwork mask field which allows RIPv2 to support variable length subnetworks. RIPv2 also includes an authentication mechanism similar to the one used in OSPF. RIPv2 is defined in RFC 2453. Table 9: RIPv1 vs. RIPv2 on page 191 summarizes the differences between RIP and RIP2.

Table 9: 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)

Preventing routing loops in RIP

You can use the following features in RIP to help avoid routing loops:

- Split-horizon
- Poison-reverse

The split-horizon technique prevents information about routes from exiting the router interface through which the information was received. This prevents small routing loops. Use the **`ip rip split-horizon`** command 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 explicitly indicate that a network or subnet is unreachable. Poison-reverse updates are sent to defeat large routing loops. Use the **`ip rip poison-reverse`** command 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.

Up to 99 RIP distribution access lists can be configured on the Avaya G350 Media Gateway.

For example: To configure RIP distribution access list number 10 permitting distribution and learning of network 10.10.0.0:

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 list created in Step 1 by performing the following procedure within the **`router rip`** context:

   - Enter the **`distribution-list 10 in`** command to apply list number 10 created in Step 1 on all updates received on all interfaces.
   - Enter the **`distribution-list 10 in FastEthernet 6/1`** command to apply Access List 10 on updates received on interface ‘FastEthernet 6/1’.
   - Enter the **`distribution-list 10 out`** command to apply Access List 10 to all advertised updates.
   - 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).

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 G350 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.

RIP commands

Use the following commands to configure RIP. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`default-metric`** command to set the interface RIP route metric value. Use the **no** form of this command to restore the default value.
- Use the **`distribution-list`** command to apply a distribution policy rule for incoming or outgoing routing information in route updates. Use the **no** form of this command to deactivate the rule.
- Use the **`ip rip authentication key`** command to set the authentication string used on the interface. Use the **no** form of this command to clear the password.
- Use the **`ip rip authentication mode`** command to specify the type of authentication used in RIP Version 2 packets. Use the **no** form of this command to restore the default value, none.
- Use the **`ip rip default-route-mode`** command to enable learning of the default route received by the RIP protocol. The default state is talk-listen. Use the **no** form of this command to disable listening to default routes.
- Use the **`ip rip poison-reverse`** command to enable split-horizon with poison-reverse on an interface. Use the **no** form of this command to disable the poison-reverse mechanism.
- Use the **`ip rip rip-version`** command to specify the RIP version running on the interface.
- Use the **`ip rip send-receive-mode`** command to set the RIP send and receive modes on an interface. Use the **no** form of this command to set the RIP to talk, that is, to send reports.
- Use the **`ip rip split-horizon`** command 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.

- Use the **network** command to specify a list of networks on which the RIP is running. Use the **no** form of this command to remove an entry from the list of networks.
- Use the **redistribute** command to redistribute routing information from other protocols into RIP. Use the **no** form of this command to restore the default value, disable redistribution by RIP.
- Use the **router rip** command to enable RIP and to enter the router configuration context. Use the **no** form of this command to restore the default value, disabling RIP.
- Use the **timers basic** command to set RIP timers. Use the **no** form of this command to set the RIP timers to their default values.

Configuring OSPF

This section provides information about configuring OSPF parameters for router interfaces and contains the following topics:

- Overview of OSPF — an overview of OSPF
- OSPF dynamic cost — a description of OSPF cost calculation, with instructions on how to manually configure the cost of an OSPF interface
- OSPF limitations — a description of the limitations on the use of OSPF on the G350
- OSPF commands — a list and descriptions of CLI commands used to configure OSPF on the G350

Overview of OSPF

The Open Shortest Path First (OSPF) protocol enables routers to compute the path that an IP packet should follow. Routers exchange routing information with OSPF to determine where to send each IP packet on its next hop. RIP is an older protocol that serves a similar purpose. For more information about RIP, see RIP overview on page 190.

OSPF is based on the shortest-path-first or link-state algorithm. It was introduced to overcome the limitations of RIP in increasingly complex network designs. OSPF uses the cost of a path as the criterion for comparing paths. In contrast, RIP uses the number of hops as the criterion for comparing paths. Also, updates are sent when there is a topological change in the network, rather than every 30 seconds as with RIP.

The advantage of shortest-path-first algorithms is that under stable conditions, there are less frequent updates (thereby saving bandwidth). They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity, when routers continuously increment the hop count to a particular network. These algorithms make a stable network. The disadvantage of shortest-path-first algorithms is that they require a lot of CPU power and memory.

In OSPF, routers use link-state updates to send routing information to all nodes in a network by calculating the shortest path to each node. This calculation is based on a topography of the network constructed by each node. Each router sends that portion of the routing table that describes the state of its own links, and it also sends the complete routing structure (topography).

You can configure route redistribution between OSPF, RIP, and static routes. With route redistribution, you can configure the G350 to redistribute routes learned from one protocol into the domain of the other routing protocol. For more information, see Route redistribution on page 197.

OSPF dynamic cost

An OSPF interface on the G350 can dynamically set a Cost. The Cost represents the price assigned to each interface for purposes of determining the shortest path.

By default the OSPF interface Cost is calculated based on the interface bandwidth, according to the following formula:

Cost = 100,000/bandwidth (in kbps)

The result is that the higher the bandwidth, the lower the Cost.

To manually configure the Cost of an OSPF interface, use the **`ip ospf cost`** command from the interface context. By using this option, dynamic bandwidth updates do not change the Cost. Use the **`no ip ospf cost`** command to return to dynamic cost calculation on an interface.

Use the **`bandwidth`** command from the Interface context to manually adjust the interface's bandwidth If Cost is being determined dynamically, this configured bandwidth and not the actual interface bandwidth, is used to calculate Cost.

OSPF limitations

You can configure the G350 as an OSPF Autonomous System Boundary Router (ASBR) using route redistribution. The G350 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 G350 cannot be configured to be an OSPF area border router itself.

The G350 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.

OSPF commands

Use the following commands to configure OSPF. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`area`** command to configure the OSPF area ID of the router. Use the **no** form of the command to delete the OSPF area id.
- Use the **`default-metric`** command to set the interface OSPF route metric value. Use the **no** form of this command to restore the default value.
- Use the **`ip ospf authentication-key`** command to configure the interface authentication password. Use the **no** form of this command to remove the OSPF password.
- Use the **`ip ospf cost`** command to configure the interface metric. Use the **no** form of this command to set the cost to its default value.
- Use the **`ip ospf dead-interval`** command to configure the interval before declaring the neighbor as dead. Use the **no** form of this command to set the dead-interval to its default value.
- Use the **`ip ospf hello-interval`** command to specify the time interval between hello packets sent by the router. Use the **no** form of this command to set the hello-interval to its default value.
- Use the **`ip ospf network point-to-multipoint`** command to specify the network type for the interface. Use the **no** form of the command to return the interface to the default value.
- Use the **`ip ospf priority`** command to configure interface priority used in DR election. Use the **no** form of this command to set the OSPF priority to its default value.
- Use the **`ip ospf router-id`** command to configure the router ID. Use the **no** form of this command to return the router ID to its default value.
- Use the **`network`** command to enable OSPF in a network. Use the **no** form of this command to disable OSPF in a network. The default value is disabled.
- Use the **`passive-interface`** command to suppress OSPF routing updates on an interface. This is used to allow interfaces to be flooded into the OSPF domain as OSPF routes rather than external routes.

  Note:

  You must also use the **`network`** command, in conjunction with the **`passive-interface`** command, to make the network passive.

- Use the **`redistribute`** command to redistribute routing information from other protocols into OSPF. Use the **no** form of this command to disable redistribution by OSPF.

- Use the **`router ospf`** command to enable OSPF protocol on the system and to enter the router configuration context. Use the **no** form of this command to restore the default value, disable OSPF globally.
- Use the **`show ip ospf`** command to display general information about OSPF routing.
- Use the **`show ip ospf database`** command to display lists of information related to the OSPF database for a specific router.
- Use the **`show ip ospf interface`** command to display the OSPF-related interface information.
- Use the **`show ip ospf neighbor`** command to display OSPF neighbor information on a per-interface basis.
- Use the **`timers spf`** command to configure the delay between runs of OSPF's (SPF) calculation. Use the **no** form of this command to restore the default value.

Route redistribution

Route redistribution is the interaction of multiple routing protocols. OSPF and RIP can be operated concurrently in the G350. In this case, you can configure the G350 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 G350 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 G350 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 G350 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.

Use the **`redistribute`** command in the Router RIP context to configure route redistribution into RIP. Use the **`redistribute`** command in the Router OSPF context to configure route redistribution into OSPF.

Export default metric

The Avaya G350 Media 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 this 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.

Configuring VRRP

This section provides information about configuring VRRP to provide router redundancy and load balancing and includes the following topics:

- Overview of VRRP — an overview of the VRRP protocol
- VRRP configuration example — an example of a VRRP configuration with one main router and one backup router
- VRRP commands — a list and descriptions of CLI commands used to configure VRRP

Overview of 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 backup 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.

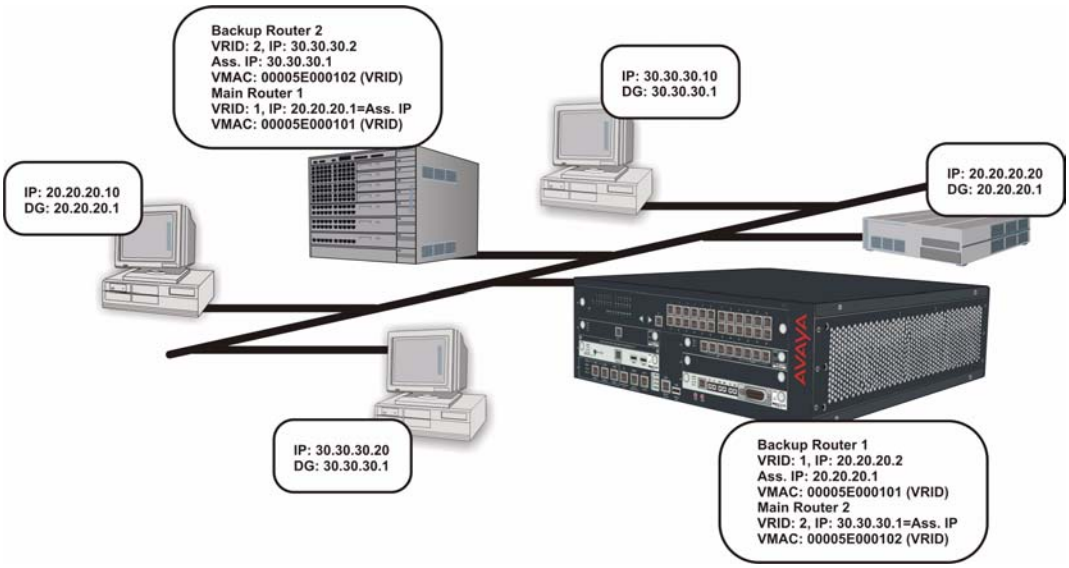
In VRRP, two or more physical routers can be associated with a virtual router, thus achieving extreme reliability. In a VRRP environment, host stations interact with the virtual router. The stations are not aware that this router is a virtual router, and are not affected when a new router takes over 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:

Figure 15: VRRP configuration example



There is one main router on IP subnet 20.20.20.0, such as a G350, P333R, C460, or any router that supports VRRP, and a backup router. You can configure more backup routers.

- The G350 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 sense 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 need to perform this manually if needed.

VRRP commands

Use the following commands to configure VRRP. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`ip vrrp`** command to create a virtual router on an interface. Use the **no** form of this command to delete a virtual router.
- Use the **`ip vrrp address`** command to assign an IP address to a virtual router. Use the **no** form of this command to remove an IP address from a virtual router.
- Use the **`ip vrrp auth-key`** command to set the virtual router simple password authentication key for the virtual router ID. Use the **no** form of this command to disable simple password authentication for the virtual router instance.
- Use the **`ip vrrp override addr owner`** command to 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). Use the **no** form of this command to discard these packets.
- Use the **`ip vrrp preempt`** command to configure a router to preempt a lower priority master for the virtual router ID. Use the **no** form of this command to disable preemption for a virtual router instance. By default, preemption is enabled.
- Use the **`ip vrrp primary`** command to set the primary address used as the source address of VRRP packets for the virtual router ID. Use the **no** form of this command to restore the default primary address for a virtual router instance. By default, the primary address is selected automatically by the device.
- Use the **`ip vrrp priority`** command to set the virtual router priority value used when selecting a master router. Use the **no** form of this command to restore the default value.
- Use the **`ip vrrp timer`** command to set the virtual router advertisement timer value for the virtual router ID. Use the **no** form of this command to restore the default value.

- Use the **`router vrrp`** command to enable VRRP routing. Use the **no** form of this command to disable VRRP routing.
- Use the **`show ip vrrp`** command to display VRRP information.

Configuring fragmentation

This section provides information about configuring fragmentation on the G350 router and contains the following topics:

- Overview of fragmentation — an overview of fragmentation and reassembly on the G350 router
- Reassembly parameters — a description of the fragmentation parameters you can configure
- Fragmentation commands — a list and descriptions of CLI commands used to configure fragmentation

Overview of fragmentation

The G350 supports IP fragmentation and reassembly. The G350 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 G350 supports fragmentation of IP packets according to RFC 791, and reassembly of IP packets destined only to its interfaces.

Reassembly parameters

Reassembly is associated with the following user-configurable parameters:

- **Fragment Size** — The maximum number of concurrently reassembled packets:
  Range: 0 to 200. Default: 100.
- **Fragment Timeout** — The maximum time, in seconds, to wait for a packet to be reassembled:
  Range: 5 to 120. Default: 10.
- **Fragment Chain** — The maximum number of fragments allowed per packet:
  Range: 2 to 2048. Default: 64.

Fragmentation commands

Use the following commands to configure fragmentation and reassembly. For more information about these commands, see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **`clear fragment`** command to clear the fragment database and restore its default values.
- Use the **`fragment chain`** command to set the maximum number of fragments that can comprise a single IP packet destined to the router. Use the **no** form of this command to set the fragment chain to its default value.
- Use the **`fragment size`** command to set the maximum number of fragmented IP packets destined to the router to reassemble at any given time. Use the **no** form of this command to set the fragment size to its default value.
- Use the **`fragment timeout`** command to set the maximum number of seconds to reassemble a fragmented IP packet destined to the router. Use the **no** form of this command to set the fragment timeout to its default value.
- Use the **`fragments`** command to set the treatment for IP fragmentation packets entering on an interface.
- Use the **`show fragment`** command to display information regarding fragmented IP packets that are destined to a router.

Chapter 17: Configuring IPSec VPN

This chapter provides information about configuring IPSec VPN in the G350, and contains the following sections:

- Overview of IPSec VPN — an overview of VPN and IPSec technology
- Configuring a site-to-site IPSec VPN — instructions on how to configure IPSec VPN in the G350
- IPSec VPN maintenance — instructions on displaying and clearing IPSec VPN data, as well as viewing the IPSec VPN log
- Typical installations — illustrations of IPSec VPN typical applications

Overview of 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 IPSec. IPSec (IP Security) 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 IKE (Internet Key Exchange) protocol to exchange key information between the two nodes (called peers). Each peer maintains SAs (security associations) 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 G350 IPSec VPN feature is designed to support site-to-site topologies, in which the two peers are Gateways.

Configuring a site-to-site IPSec VPN

To configure a site-to-site IPSec VPN, two devices (the G350 and a peer Gateway) must be configured symmetrically. The following sections provide an overview of IPSec VPN configuration, followed by detailed step-by-step instructions.

Overview of IPSec VPN configuration

The basic IPSec VPN building blocks define how to secure packets, as follows:

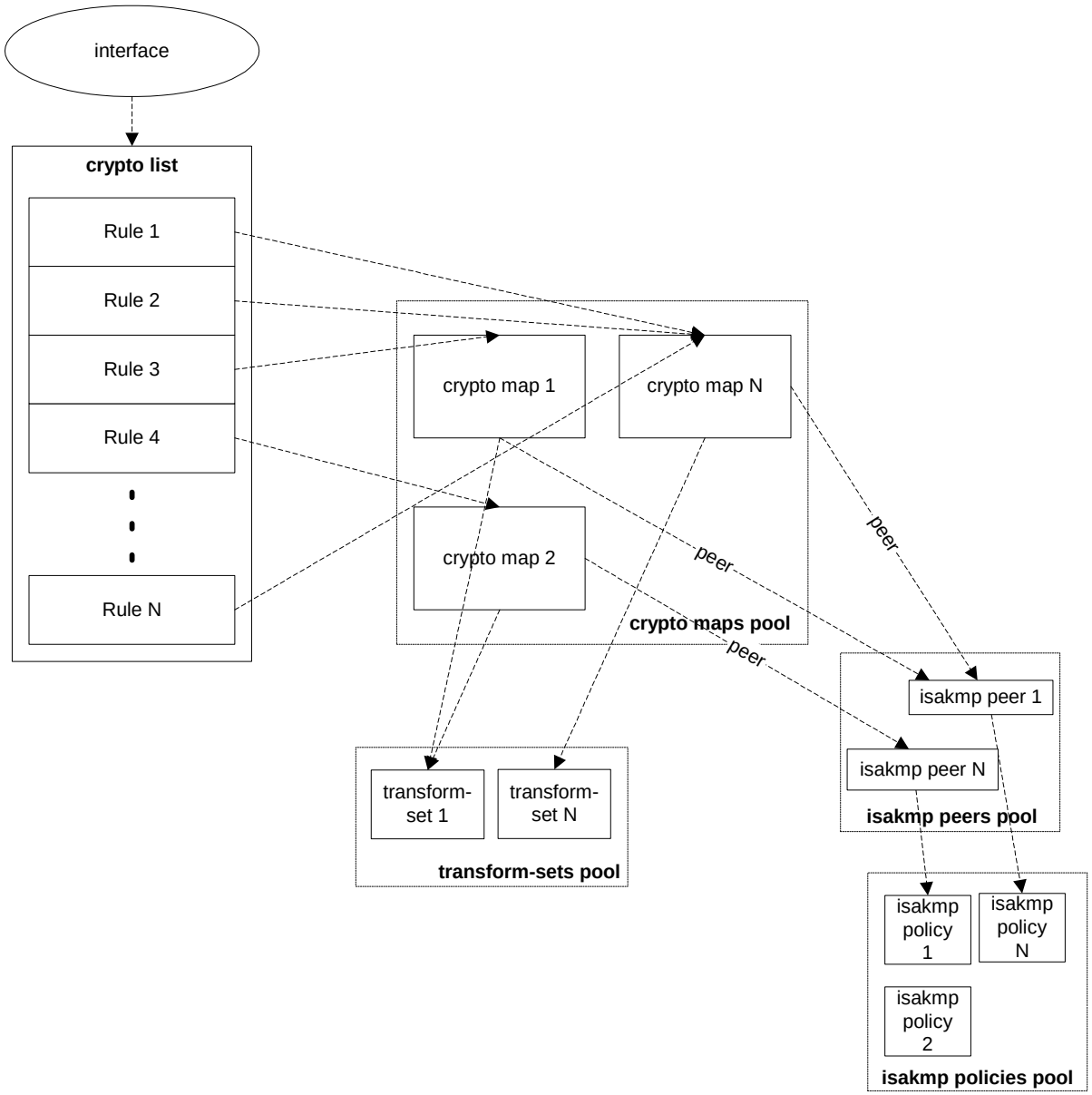
- *ISAKMP policies* – define parameters for IKE phase 1 negotiation
- *Transform-sets* – define parameters for IKE phase 2 negotiation

Once the building blocks are defined, IPSec VPN is implemented using a crypto-list. The crypto-list defines, for the interface it 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. The peer, in turn, points to an ISAKMP policy.

The following diagram illustrates IPSec VPN components and their relationships:

Figure 16: IPSec VPN Configuration Model



Configuring IPSec VPN consists of the following steps:

1. Prerequisite – coordinating with the VPN peer.
2. Installing the VPN license file.
3. Configuring ISAKMP policies.
4. Configuring transform-sets.
5. Configuring ISAKMP peer information.
6. Configuring crypto maps.
7. Configuring crypto-lists.
8. Configuring interfaces.

Note:

The order of configuration is important.

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 G350 contains default ISAKMP policy settings.

The following figure illustrates the IPSec VPN workflow. Note that mandatory commands are indicated in bold.

Figure 17: IPSec VPN Configuration Workflow

```
crypto isakmp policy
   description
   encryption
   hash
   group
   authentication
   lifetime

crypto ipsec transform-set
   set pfs
   set security-association lifetime seconds
   set security-association lifetime kilobytes

crypto isakmp peer address
   description
   isakmp-policy
   pre-shared-key

crypto map
   description
   set transform-set
   set peer
   set dscp

ip crypto list
   local address
   ip-rule
      source-ip
      destination-ip
      protect crypto map
   ip-rule-default
      protect

interface fastethernet 10/2
   crypto ipsec df-bit
   crypto ipsec minimul pmtu
   ip crypto-group
```

The following sections describe the various configuration steps in detail.

Prerequisite – coordinating with the VPN peer

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. The basic parameters include:

- The IKE phase 1 parameters (as defined in the ISAKMP policy, see Configuring ISAKMP policies on page 209)
- The IKE phase 2 parameters (as defined in the transform-set, see Configuring transform-sets on page 210)
- The pre-shared key (see Configuring ISAKMP peer information on page 211)
- Which packets should be secured (as defined in the crypto-list, see Configuring crypto-lists on page 214)
- The peer addresses – for each peer, the local address entered in the crypto-list (see Configuring crypto-lists on page 214) should match the ISAKMP peer address in the other peer (see Configuring ISAKMP peer information on page 211).

See IPSec VPN logging on page 219 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.

Installing the VPN license file

To enable IPSec VPN you must obtain and install a VPN license. To obtain a VPN license, please contact your Avaya representative.

You can install the VPN license via any of the following:

- FTP
- TFTP
- SCP

Note:

You must have *admin* permissions to install a VPN license.

To install the license file:

1. Use one of the following CLI commands:
   - **`copy ftp license-file`** ***`filename ip`***
   - **`copy tftp license-file`** ***`filename ip`***
   - **`copy scp license-file`** ***`filename ip`***

     where:
     - ***`filename`*** – the filename, including the full path
     - ***`ip`*** – the ip address of the ftp/tftp/scp server.

   For example: `copy tftp license-file g350.lic 198.87.134.153`
2. Optionally use the **`show download license-file status`** CLI command to view the status of the download process.
3. Use the **`show license status`** CLI command to verify that the license was installed.
4. Use the **`copy running-config startup-config`** command to save your current configuration.
5. Reset the G350 using the **`reset`** CLI command.

Configuring ISAKMP policies

An ISAKMP policy defines the IKE phase 1 parameters.

Important:
You must define at least one ISAKMP policy.

Note:
You can configure up to 20 ISAKMP policies.

To configure an ISAKMP policy:

1. Enter ISAKMP policy context and create an ISAKMP policy, using the **`crypto isakmp policy`** CLI command.

```
G350-001# crypto isakmp policy 1
G350-001(config-isakmp:1)#
```

2. Configure the following ISAKMP policy parameters:
   - **`description`**: the description of the ISAKMP policy
   - **`encryption`**: the encryption algorithm for the ISAKMP policy: `des`, `3des`, or `aes` (default: `des`)

- **hash**: the hash (authentication) algorithm for the ISAKMP policy: `sha` or `md5` (default: `md5`)
- **group**: the Diffie-Hellman group for the ISAKMP policy: `1` or `2` (default: `1`)
- **authentication**: the authentication of the ISAKMP policy pre-shared secret: `pre-share`
- **lifetime**: the lifetime of the ISAKMP SA, in seconds

```
G350-001(config-isakmp:1)# description "lincroft ike"
Done!
G350-001(config-isakmp:1)# encryption des
Done!
G350-001(config-isakmp:1)# hash md5
Done!
G350-001(config-isakmp:1)# group 1
Done!
G350-001(super-isakmp:1)# authentication pre-share
Done!
G350-001(config-isakmp:1)# lifetime 60000
Done!
```

3. Exit the ISAKMP policy context using the **exit** CLI command.

```
G350-001(config-isakmp:1)# exit
G350-001#
```

Configuring transform-sets

A transform-set defines the IKE phase 2 parameters. It specifies the encryption and authentication algorithms to be used for, sets a security association lifetime, and specifies whether PFS is enabled and which DH group it uses.

Note:

You can define up to 20 transform-sets.

To configure a transform-set:

1. Enter transform-set context and create a new transform-set by using the **crypto ipsec transform-set** CLI command. The command variables include:
   - The name of the transform-set
   - The encryption algorithm used by the transform-set: `esp-des`, `esp-3des`, `esp-aes` or `esp-null` (no encryption)
   - The authentication algorithm used by the transform-set: `esp-md5-hmac` or `esp-sha-hmac`.

Important:
You must define at least one transform-set.

```
G350-001# crypto ipsec transform-set ts1 esp-3des esp-md5-hmac
G350-001(config-transform:ts1)#
```

2. Configure the following transform-set parameters:
   - **`set pfs`**: specifies whether each IKE phase 2 negotiation will employ PFS (Perfect Forward Secrecy), 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`**.
   - **`set security-association lifetime seconds:`** the security association lifetime in seconds using the CLI command
   - **`set security-association lifetime kilobytes:`** the security association lifetime in kilobytes

```
G350-001001(config-transform:ts1ts1)# set pfs group2
Done!
G350-001(config-transform:ts1)# set security-association lifetime seconds
7200
Done!
G350-001(config-transform:ts1)# set security-association lifetime
kilobytes 268435456
```

3. Exit the crypto transform-set context using the **`exit`** CLI command.

```
G350-001(config-transform:ts1)# exit
G350-001#
```

Configuring ISAKMP peer information

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.

Important:
It is mandatory to define at least one ISAKMP peer.

Note:
You can define up to 50 ISAKMP peers.

To configure peer information:

1. Enter the ISAKMP peer context and define an ISAKMP peer by its address, using the **crypto isakmp peer** CLI command.

```
G350-001# crypto isakmp peer address 149.49.70.1
G350-001(config-peer:149.49.70.1)#
```

2. Enter a description for the peer.

```
G350-001(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** CLI command.

   Important:
   isakmp policy is a mandatory parameter.

```
G350-001(config-peer:149.49.70.1)# isakmp-policy 1
Done!
```

4. Enter the preshared key for peer authentication using the **pre-shared-key** CLI command.

   Important:
   pre-shared-key is a mandatory parameter.

```
G350-001(config-peer:149.49.70.1)# pre-shared-key GNpi1odGNBrB5z4GJL
Done!
```

   Or

   Obtain a suggested key from the gateway using the **crypto isakmp suggest-key** CLI command and then enter it using the **pre-shared-key** CLI command. Note that you must exit the ISAKMP peer context before using the **crypto isakmp suggest-key** command, and re-enter ISAKMP peer context to use the **pre-shared-key** command. The suggested key-length can vary from 8-127 characters, and the default is 32 characters.

```
G350-001(config-peer:149.49.70.1)# exit

G350-001# crypto isakmp suggest-key 24
The suggest key: yjsYIz9ikcwaq0FUPTF3CIrw

G350-001# crypto isakmp peer address 149.49.70.1

G350-001(config-peer:149.49.70.1) pre-shared-key yjsYIz9ikcwaq0FUPTF3CIrw
Done!
```

5. Exit the peer context using the **exit** CLI command.

```
G350-001(config-peer:149.49.70.1)# exit
G350-001#
```

Configuring crypto maps

A crypto map points to a transform-set and to a peer (which in turn points to an ISAKMP policy). These components 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 50 crypto maps.

To configure a crypto map:

1. Enter crypto map context and create a crypto map by using the **crypto map** CLI command.

```
G350-001# crypto map 1
G350-001(config-crypto:1)#
```

2. Configure the following crypto map parameters:
   - **description**: the description of the crypto map
   - **set peer**: the remote peer
   - **set transform set**: the specific transform-set to which this crypto map points
   - **set dscp**: the static DSCP value in the DS field of the tunneled packet. The default setting is **no set dscp**, which specifies that the DSCP is copied from the DS field of the original packet.

Important:
set peer and **set transform set** are mandatory parameters.

```
G350-001(config-crypto:1)# description "vpn lincroft branch"
Done!
G350-001(config-crypto:1)# set peer 149.49.60.60
Done!
G350-001(config-crypto:1)# set transform-set ts1
Done!
G350-001(config-crypto:1)# set dscp 38
Done!
```

3. Exit crypto map context using the **exit** CLI command.

```
G350-001(config-crypto:1)# exit
G350-001#
```

Configuring crypto-lists

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/mask). A crypto-list is activated on an interface. The G350 can have multiple crypto-lists activated on different interfaces.

To configure a crypto-list:

1. Enter the crypto-list context and create a crypto-list by using the **crypto-list** CLI command.

   Important:
   It is mandatory to create at least one crypto-list.

```
G350-001# ip crypto-list 901
G350-001(Crypto 901)#
```

2. Configure the following parameters:
   - **local address**: the local IP address for the IPSec tunnels derived from this crypto list.

     Important:
     local address is a mandatory parameter.
   - **name**: the name of the crypto list
   - **owner**: the owner of the crypto list
   - **cookie**: the list cookie for this crypto list. This parameter is used by QoS Manager.

```
G350-001(Crypto 901)# local address 192.168.49.1
Done!
G350-001(Crypto 901)# name “Public Network via ADSL”
Done!
G350-001(Crypto 901)# owner lou
Done!
G350-001(Crypto 901)# cookie 1
Done!
```

3. Enter the ip-rule context and define an ip-rule using the **`ip-rule`** CLI command.

   Important:
   It is mandatory to create at least one ip-rule.

```
G350-001(Crypto 901Crypto 901)# ip-rule 10
G350-001(Crypto 901/ip rule 10)#
```

4. Configure the following ip-rule parameters:
   - **`source ip`**: the requested source IP address to match
   - **`destination ip`**: the requested destination IP address to match
   - Define the action: specify whether to protect traffic that matches the source and destination addresses:
     - **`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.

```
G350-001(Crypto 901/ip rule 10)# source-ip 10.1.0.0 0.0.255.255
Done!
G350-001(Crypto 901/ip rule 10)# destination-ip any
Done!
G350-001(Crypto 901/ip rule 10)# protect crypto map 1
Done!
```

5. Exit ip-rule context using the **`exit`** CLI command.

```
G350-001(Crypto 901/ip rule 10)# exit
G350-001(Crypto 901)#
```

6. Repeat steps 3, 4 and 5 for every ip-rule you wish to define in the crypto-list.
7. Create a last ip-rule using the **`ip-rule default`** command. This rule specifies which action to take if a packet matches non of the previous rules. Within this ip-rule context, define only whether to `protect` or `no protect` traffic.

```
G350-001(Crypto 901Crypto 901)# ip-rule default
G350-001(Crypto 901/ip rule default)# protect crypto map 1
Done!
```

8. Exit ip-rule context using the **`exit`** CLI command.

```
G350-001(Crypto 901/ip rule default)# exit
G350-001(Crypto 901)#
```

9. Exit crypto-list context using the **exit** CLI command.

```
G350-001(Crypto 901)# exit
G350-001#
```

Configuring interfaces

A crypto-list is activated on an interface. G-350 can have multiple crypto-lists activated on different interfaces.

To configure an interface:

1. Enter interface context using the **interface** CLI command.

```
G350-001# interface Serial 2/1
G350-001(if: Serial 2/1)#
```

2. Configure the following interface parameters:
   - **ip crypto-group**: the crypto-list to be activated on this interface

     Important:
     ip crypto-group is a mandatory parameter.
   - **crypto ipsec minimal pmtu**: This command is intended for advanced users only. It sets the minimal PMTU value which can be applied to an SA when the G350 participates in Path MTU Discovery (PMTUD) for the tunnel pertaining to that SA.
   - **crypto ipsec df-bit copy**: This command is intended for advanced users only. It sets the Don't-Fragment bit to either `clear` or `copy` mode:
     - `copy` – the DF bit of the encapsulated packet is copied from the original packet, and Path MTU Discovery (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.

```
G350-001(if: Serial 2/1)# ip crypto-group 901
Done!
G350-001(if: Serial 2/1)# crypto ipsec minimal pmtu 500
Done!
G350-001(if: Serial 2/1)# crypto ipsec df-bit copy
Done!
```

3. Exit the interface context using the **exit** CLI command.

```
G350-001(if: Serial 2/1)# exit
G350-001#
```

Deactivating crypto lists to modify IPSec VPN parameters

Most IPSec VPN parameters cannot be modified if they are linked to an active crypto list. To modify a parameter linked to an active crypto list, you must first deactivate the list using the **no ip crypto-group** CLI 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:

```
G350-001# interface Serial 2/1
G350-001(if: Serial 2/1)# no ip crypto-group
Done!
```

After modifying IPSec VPN parameters as desired, re-activate the crypto list on the interface using the **ip crypto-group *crypto-list-id*** CLI command. For example:

```
G350-001# interface Serial 2/1
G350-001(if: Serial 2/1)# ip crypto-group 901
Done!
```

IPSec VPN maintenance

You can display IPSec VPN configuration and status, and clear IPSec VPN data, using certain **show** and **clear** CLI 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.

The following sections describe these options.

Displaying IPSec VPN configuration

You can use the following **show** CLI commands to display IPSec VPN configuration. For a full description of the commands and their output fields see *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

- Use the **show crypto ipsec transform-set** command to display configuration for a specified transform-set or all transform-sets.
- Use the **show crypto isakmp policy** command to display ISAKMP policy configuration.
- Use the **show crypto isakmp peer** command to display crypto ISAKMP peer configuration.
- Use the **show crypto map** command to display all or specific crypto map configurations.
- Use the **show ip crypto-list *list#*** command to display the configuration of a specific crypto-list.
- Use the **show ip crypto-list** command to display all crypto-lists.
- Use the **show ip active-lists** command to display the crypto-lists active on each interface.

Displaying IPSec VPN status

You can use the following **show** CLI commands to display IPSec VPN status. For a full description of the commands and their output fields see the CLI Reference Guide.

- Use the **show crypto isakmp sa** command to display ISAKMP SA database status.
- Use the **show crypto ipsec sa [detail]** CLI command to display the IPsec SA database status.
- Use the **show crypto ipsec sa address** CLI command to display the IPsec SA configuration by peer IP address.

- Use the **`show crypto ipsec sa list`** ***`list-id`*** **`[rule`** ***`rule-id`***] **`[detail]`** CLI command to display the IPsec SA configuration by list ID and rule ID.

  Tip:

  The **`detail`** option in the various **`show crypto ipsec sa`** CLI 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.

- Use the **`clear crypto sa counters`** command to clear the crypto SA counters.

IPSec VPN intervention

You can use the following **`clear`** CLI commands to intervene in IPSec VPN configuration:

- Use the **`clear crypto sa`** command to clear all IPSec SAs (security association structures).
- Use the **`clear crypto isakmp`** command to flush a specific entry in the ISAKMP database or the entire ISAKMP database.

  Note:

  If you wish to clear both an ISAKMP connection and the IPSec SAs, the recommended order of operations is:
  First clear the IPSec SAs using the **`clear crypto sa all`** command, then clear the ISAKMP SA using the **`clear crypto isakmp`** command.

IPSec VPN logging

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.

To view the IPSec VPN syslog:

1. Use the **`set logging session enable`** command to enable syslog on the session.

```
G350-001# set logging session enable
Done!
CLI-Notification: write: set logging session enable
```

2. Use the **`set logging session condition ISAKMP Debug`** command to view all ISAKMP messages of Debug level and above.

```
G350-001# set logging session condition ISAKMP Debug
Done!
CLI-Notification: write: set logging session condition ISAKMP Debug
```

3. Use the **`set logging session condition IPSEC Debug`** command to view all IPSec messages of Debug level and above.

```
G350-001# set logging session condition IPSEC Debug
Done!
CLI-Notification: write: set logging session condition IPSEC Debug
```

4. Initiate a session, for example by pinging the peer device.

```
G350-001# ping 135.64.102.109
```

The logging information will detail the IKE negotiations, including the ISAKMP SA and IPSec SA configuration of the peers. For 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

The following sections describe the typical IPSec VPN installations.

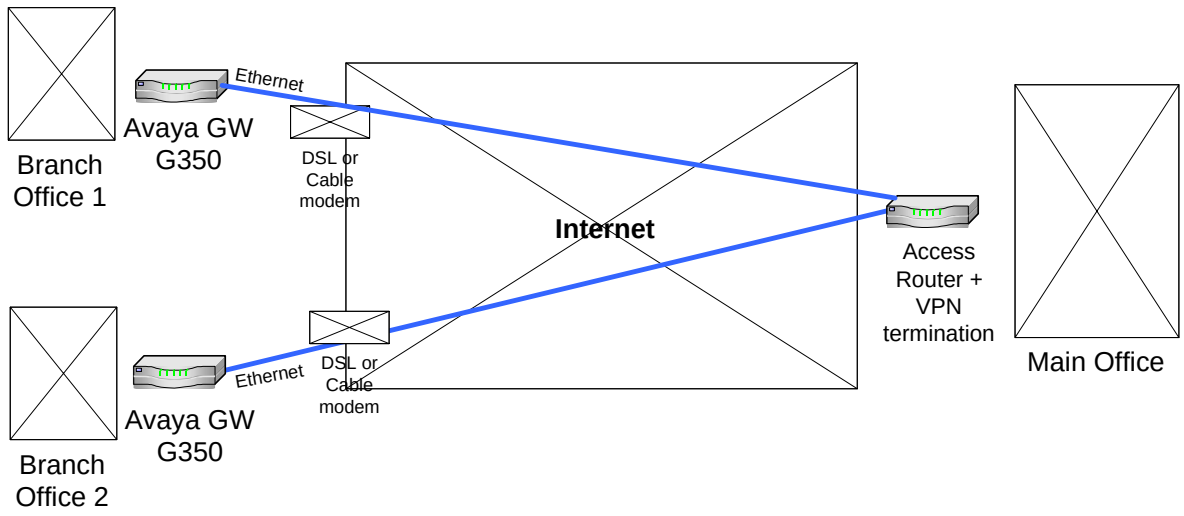
Simple VPN topology: VPN hub and spokes

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.

Figure 18: Simple VPN topology: VPN hub and spokes



Configuring the simple VPN topology

This section describes how to configure the simple VPN topology, followed by a detailed configuration example.

To configure the simple VPN topology

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 anyone is encrypted, using tunnel mode IPSec, with the remote peer being the Main Office (the VPN Hub)
   - ACL is configured on the Internet interface to allow only the VPN / ICMP traffic, as follows:

     Ingress:

     1. IKE from remote tunnel endpoint to local tunnel endpoint -> Permit
     2. ESP from remote tunnel endpoint to local tunnel endpoint -> Permit
     3. ICMP from anyone to local tunnel endpoint -> Permit

     Note:
     This allows PMTUD application to work.

     4. All allowed services from anyone to any local subnet -> Permit

     Note:
     Due to the definition of the VPN Policy, this will be allowed only if traffic comes over ESP.

     5. Default -> Deny

     Egress:

     1. IKE from local tunnel endpoint to remote tunnel endpoint -> Permit
     2. ESP from local tunnel endpoint to remote tunnel endpoint -> Permit
     3. ICMP from local tunnel endpoint to anyone -> Permit
        Note: This allows the PMTUD application to work.
     4. All allowed services from any local subnet to anyone -> Permit
        Note: This traffic is tunnelled using VPN.
     5. Default -> Deny
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, with the remote peer being the VPN Spoke (Branch Internet address).

Configuration example

```
crypto isakmp policy 1
         encryption aes
         hash sha
         group 2
         exit
crypto isakmp peer address <Main Office Public Internet Static IP Address>
         pre-shared-key  <secret key>
         isakmp-policy 1
         exit
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
         set pfs 2
         exit
 crypto map 1
         set peer <Main OfficeMain Office Public Internet Static IP
Address>
         set transform-set ts1
         exit
 ip crypto-list 901
      local-address <Branch Office Public Internet Static IP Address>
      ip-rule 10
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip  any
               protect crypto map 1
               exit
     ip-rule 20
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip  any
               protect crypto map 1
               exit
     ip-rule default
               no protect
               exit
     exit
ip access-control-list 301
      ip-rule 10
               source-ip host <Main Office Public Internet Static IP
                                                              Address>
               destination-ip host <Branch Office Public Internet Static
                                                         IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 20
               source-ip host <Main Office Public Internet Static IP
                                                               Address>
               destination-ip host <Branch Office Public Internet Static
                                                         IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
```

```
      ip-rule 30
               source-ip         any
              destination-ip host  <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol icmp
               composite-operation  Permit
               exit
      ip-rule 40
               source-ip         any
               destination-ip <Branch Subnet1> <Branch Subnet1 Mask>
               composite-operation  Permit
               exit
      ip-rule 50
               source-ip         any
               destination-ip <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 host <Main Office Public Internet Static IP
                                                            Address>
               destination-ip host <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 20
               source-ip host <Main Office Public Internet Static IP
                                                            Address>
               destination-ip host <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
      ip-rule 30
               destination-ip  any
               source-ip host  <Branch Office Public Internet Static IP
                                                            Address>
               ip-protocol icmp
               composite-operation  Permit
               exit
      ip-rule 40
               destination-ip any
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               composite-operation  Permit
               exit
```

```
      ip-rule 50
               destination-ip any
               source-ip <Branch Subnet1> <Branch Subnet1 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 10/2
         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 acl-group      in    301
         ip acl-group      out 302
         exit

ip default-gateway  FastEthernet 10/2 high
```

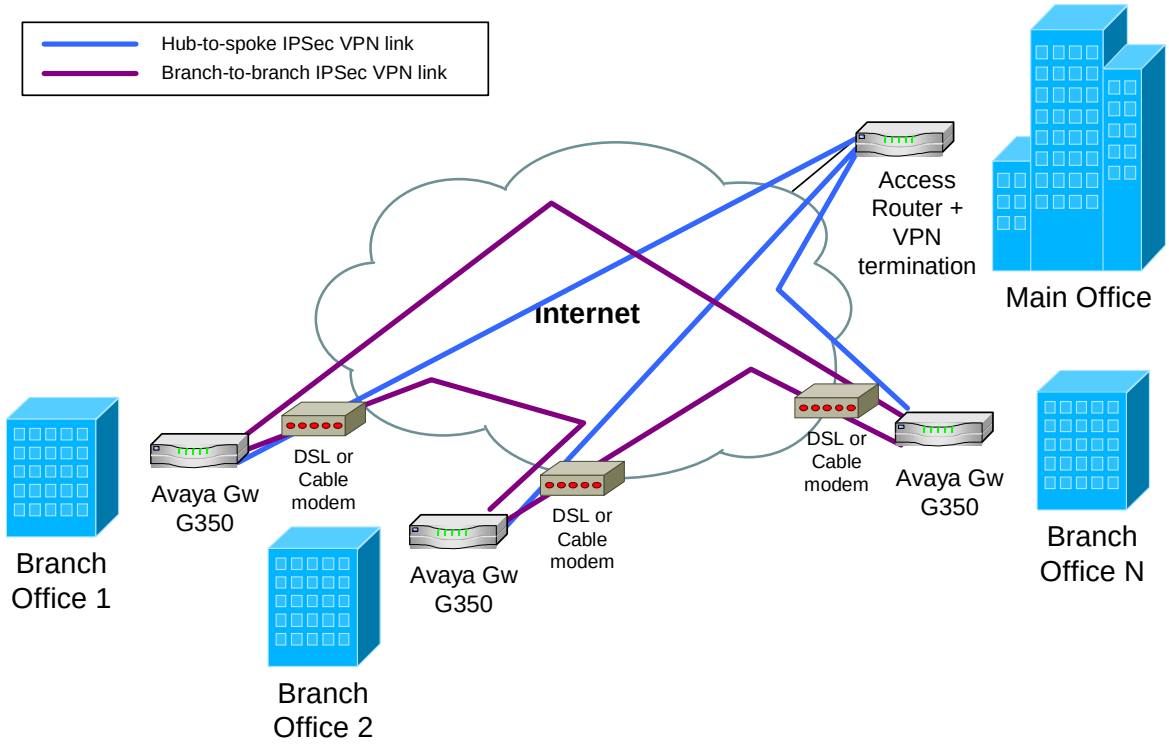
Full or partial mesh

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.

Figure 19: Full or partial mesh



Configuring the mesh VPN topology

This section describes how to configure the mesh VPN topology, followed by a detailed configuration example.

To configure the mesh VPN topology:

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 anyone -> encrypt, using tunnel mode IPSec, with the remote peer being the Main Office (VPN hub).
   - ACL is configured on the Internet interface to allow only the VPN / ICMP traffic, as follows

     Ingress:

     1. IKE from Main Office IP to Branch IP -> Permit
     2. ESP from Main Office IP to Branch IP -> Permit
     3. IKE from Second Branch IP to Branch IP -> Permit
     4. ESP from Second Branch IP to Branch IP -> Permit
     5. ICMP from anyone to local tunnel endpoint -> Permit
        Note: This allows the PMTUD application to work.
     6. All allowed services from anyone to any local subnet -> Permit
        Note: Due to the definition of the VPN Policy, this will be allowed only if traffic comes over ESP.
     7. Default -> Deny

     Egress:

     1. IKE from Branch IP to Main Office IP -> Permit
     2. ESP from Branch IP to Main Office IP -> Permit
     3. IKE from Branch IP to Second Branch IP -> Permit
     4. ESP from Branch IP to Second Branch IP -> Permit
     5. ICMP from local tunnel endpoint to anyone -> Permit
        Note: This allows the PMTUD application to work.
     6. All allowed services from any local subnet to anyone -> Permit
        Note: This traffic is tunnelled using VPN.
     7. Default -> Deny

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 anyone -> encrypt, using tunnel mode IPSec, with the remote peer being the Main Office (VPN hub)
   - ACL is configured on the Internet interface to allow only the VPN / ICMP traffic, as follows:

     Ingress:

     1. IKE from Main Office IP to Branch IP -> Permit
     2. ESP from Main Office IP to Branch IP -> Permit
     3. IKE from First Branch IP to Branch IP -> Permit
     4. ESP from First Branch IP to Branch IP -> Permit
     5. ICMP from anyone to local tunnel endpoint -> Permit
        Note: This allows PMTUD application to work.
     6. All allowed services from anyone to any local subnet -> Permit
        Note: Due to the definition of the VPN Policy, this will be allowed only if traffic comes over ESP.
     7. Default -> Deny

     Egress:

     1. IKE from Branch IP to Main Office IP -> Permit
     2. ESP from Branch IP to Main Office IP -> Permit
     3. IKE from Branch IP to First Branch IP -> Permit
     4. ESP from Branch IP to First Branch IP -> Permit
     5. ICMP from local tunnel endpoint to anyone -> Permit
        Note: This allows the PMTUD application to work.
     6. All allowed services from any local subnet to anyone -> Permit
        Note: This traffic is tunnelled using VPN.
     7. Default -> Deny
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 anyone to branch local subnets -> encrypt, using tunnel mode IPSec, with the remote peer being the VPN Spoke (Branch Internet address).

Configuration example

Note:

The commands appearing in bold are the CLI commands that add the mesh capabilities to the simple hub-and-spokes configuration.

1. Configure Branch Office 1:

```
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

     ip-rule default
               no protect
               exit
     exit

ip access-control-list 301
      ip-rule 1
              source-ip        host <Second Branch Office Public Internet
                                                     Static IP Address>
               destination-ip host  <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 2
              source-ip        host <Second Branch Office Public Internet
                                                     Static IP Address>
               destination-ip host  <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
      ip-rule 10
               source-ip         host <Main Office Public Internet
                                                    Static IP Address>
               destination-ip host  <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
```

```
      ip-rule 20
               source-ip         host <Main Office Public Internet
                                                Static IP Address>
              destination-ip host  <Branch Office Public Internet Static
                                                        IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
      ip-rule 30
               source-ip         any
              destination-ip host  <Branch Office Public Internet Static
                                                        IP Address>
               ip-protocol icmp
               composite-operation  Permit
               exit
      ip-rule 40
               source-ip         any
               destination-ip <Branch Subnet1> <Branch Subnet1 Mask>
               composite-operation  Permit
               exit
      ip-rule 50
               source-ip         any
               destination-ip <Branch Subnet2> <Branch Subnet2 Mask>
               composite-operation  Permit
               exit
      ip-rule default
               composite-operation  deny
               exit
      exit

ip access-control-list 302
      ip-rule 1
               source-ip           host  <Branch Office Public Internet
                                                Static IP Address>
              destination-ip   host <Second Branch Office Public Internet
                                                Static IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 2
               source-ip           host  <Branch Office Public Internet
                                                Static IP Address>
              destination-ip   host <Second Branch Office Public Internet
                                                Static IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
```

```
ip-rule 10
         source-ip           host  <Branch Office Public Internet
                                                Static IP Address>
         destination-ip    host <Main Office Public Internet
                                               Static IP Address>
         ip-protocol udp
         udp destination-port  Ike
         composite-operation  Permit
         exit
ip-rule 20
         source-ip host  <Branch Office Public Internet Static IP
                                                          Address>
         destination-ip    host <Main Office Public Internet
                                                Static IP Address>
         ip-protocol esp
         composite-operation  Permit
         exit
ip-rule 30
         destination-ip  any
         source-ip host  <Branch Office Public Internet Static IP
                                                          Address>
         ip-protocol icmp
         composite-operation  Permit
         exit
ip-rule 40
         destination-ip         any
         source-ip <Branch Subnet1> <Branch Subnet1 Mask>
         composite-operation  Permit
         exit
ip-rule 50
         destination-ip         any
         source-ip <Branch Subnet1> <Branch Subnet1 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 10/2
         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 acl-group      in    301
         ip acl-group      out 302
         exit

ip default-gateway  FastEthernet 10/2 high
```

2. Configure Branch Office 2:

```
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
     ip-rule default
               no protect
               exit
     exit


ip access-control-list 301
      ip-rule 1
               source-ip host <First Branch Office Public Internet
                                                 Static IP Address>
               destination-ip host <Branch Office Public Internet Static
                                                       IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 2
               source-ip host <First Branch Office Public Internet
                                                 Static IP Address>
               destination-ip host <Branch Office Public Internet Static
                                                       IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
      ip-rule 10
               source-ip host <Main Office Public Internet
                                                 Static IP Address>
               destination-ip host <Branch Office Public Internet Static
                                                       IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
```

```
      ip-rule 20
               source-ip host <Main Office Public Internet Static IP
                                                              Address>
               destination-ip host <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
      ip-rule 30
               source-ip         any
               destination-ip host <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol icmp
               composite-operation  Permit
               exit
      ip-rule 40
               source-ip         any
               destination-ip <Branch Subnet1> <Branch Subnet1 Mask>
               composite-operation  Permit
               exit
      ip-rule 50
               source-ip         any
               destination-ip <Branch Subnet2> <Branch Subnet2 Mask>
               composite-operation  Permit
               exit
      ip-rule default
               composite-operation  deny
               exit
      exit

ip access-control-list 302
      ip-rule 1
               source-ip host  <Branch Office Public Internet
                                                 Static IP Address>
               destination-ip host <First Branch Office Public Internet
                                                 Static IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 2
               source-ip host  <Branch Office Public Internet
                                                 Static IP Address>
               destination-ip host <First Branch Office Public Internet
                                                 Static IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
```

```
ip-rule 10
         source-ip host  <Branch Office Public Internet
                                                Static IP Address>
         destination-ip host <Main Office Public Internet
                                                Static IP Address>
         ip-protocol udp
         udp destination-port  Ike
         composite-operation  Permit
         exit
ip-rule 20
         source-ip           host  <Branch Office Public Internet
                                                Static IP Address>
         destination-ip    host <Main Office Public Internet
                                                Static IP Address>
         ip-protocol esp
         composite-operation  Permit
         exit
ip-rule 30
         destination-ip  any
         source-ip host  <Branch Office Public Internet
                                                Static IP Address>
         ip-protocol icmp
         composite-operation  Permit
         exit
ip-rule 40
         destination-ip         any
         source-ip <Branch Subnet1> <Branch Subnet1 Mask>
         composite-operation  Permit
         exit
ip-rule 50
         destination-ip         any
         source-ip <Branch Subnet1> <Branch Subnet1 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 10/2
         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 acl-group      in    301
         ip acl-group      out 302
         exit

ip default-gateway  FastEthernet 10/2 high
```

Hub-and-spoke with hub redundancy/load sharing

A branch with a G350 can connect to two VPN Hub sites, in a way that will provide either redundancy or load sharing.

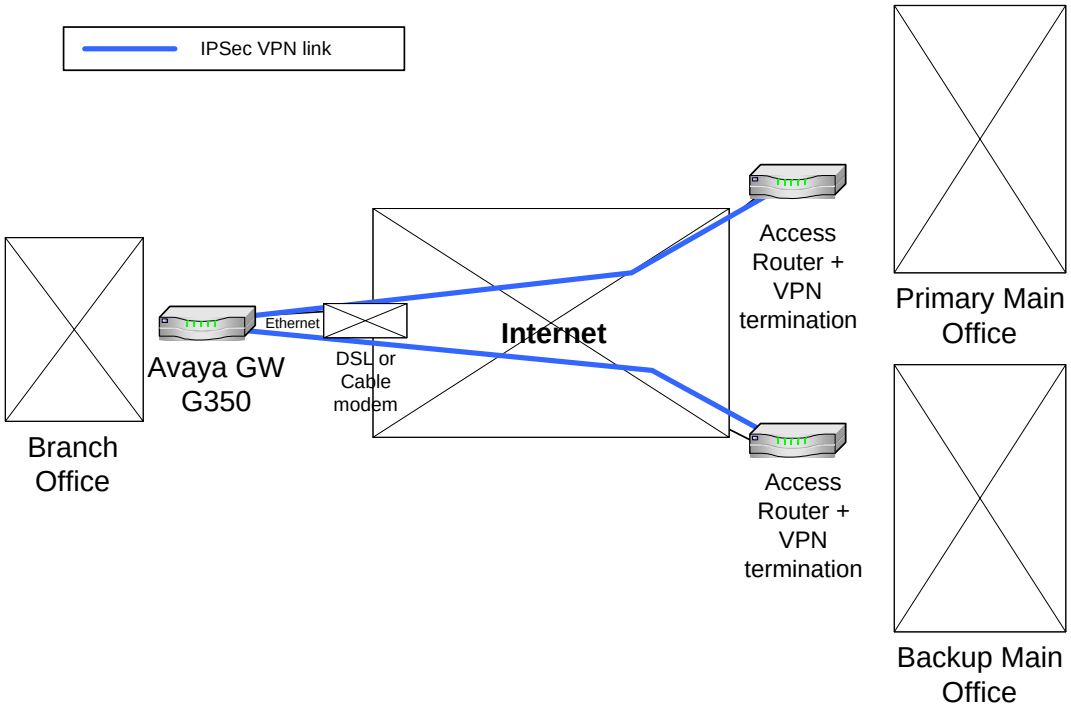
In this topology, the G350 is connected through its 10/100 WAN Ethernet port to a DSL modem.

- Two GRE tunnel interfaces are defined:
  - 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
- Two VPNs are defined.
- Connectivity to the networks in Primary/Backup Main Office is determined through GRE keep alives. 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.

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 in the “down” state.
- Load sharing – Both tunnel interfaces are active. Routing protocols (RIP or OSPF) route traffic to destinations based on route cost & availability, as follows:
  For two routes of equal cost to the same destination, one through Primary Main Office and one through Backup Main Office, OSPF will automatically distribute traffic through both routes, effectively sharing load between routes.

Figure 20: Hub-and-spoke with hub redundancy/load sharing



Configuring the VPN hub redundancy/load sharing topologies

This section describes how to configure the VPN Hub Redundancy/Load sharing topologies, followed by a detailed configuration example.

To configure the VPN Hub Redundancy/Load sharing topologies:

1. Configure the Branch Office as follows:
   - 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.
   - ACL is configured on the Internet interface to allow only the VPN / ICMP traffic, as follows:

     Ingress:

     1. IKE (UDP/500) from remote tunnel endpoints to local tunnel endpoint -> Permit
     2. ESP/AH from remote tunnel endpoint to local tunnel endpoint -> Permit

3. Allowed ICMP from anyone to local tunnel endpoint -> Permit
4. Default -> Deny

Egress:

1. IKE (UDP/500) from local tunnel endpoint to remote tunnel endpoint -> Permit
2. All allowed services from any local subnet to anyone -> Permit
3. Allowed ICMP from local tunnel endpoint to anyone -> Permit
4. Default -> Deny

- Dynamic routing (OSPF or RIP) is configured to run over local data interfaces (data VLANs) and on the GRE interfaces.

2. Configure the VPN Hubs (Main Offices) 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.
- The GRE tunnel interface is configured for the branch.
- Dynamic routing (OSPF or RIP) is configured to run over the GRE interface to the branch.

Configuration 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 10
              source-ip host <Primary Main Office Public Internet Static
                                                          IP Address>
              destination-ip host  <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 20 takke
              source-ip host <Primary Main Office Public Internet Static
                                                          IP Address>
               destination-ip host <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
      ip-rule 30
               source-ip host <Backup Main Office Public Internet Static
                                                          IP Address>
              destination-ip host  <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 40
               source-ip host <Backup Main Office Public Internet Static
                                                          IP Address>
              destination-ip host  <Branch Office Public Internet Static
                                                          IP Address>
               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 host <Primary Main Office GRE Tunnel
                                                end point IP Address>
             destination-ip host <Branch GRE Tunnel end point IP Address>
              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 10
               source-ip host <Branch Office Public Internet Static
                                                        IP Address>
               destination-ip host <Primary Main Office Public Internet
                                                 Static IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 20
               ip-protocol esp
               composite-operation  Permit
               exit
      ip-rule 30
               source-ip host <Branch Office Public Internet Static
                                                        IP Address>
               destination-ip host  <Backup Main Office Public Internet
                                                 Static IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 40
               source-ip host <Branch Office Public Internet Static
                                                        IP Address>
               destination-ip host <Backup Main Office Public Internet
                                                 Static IP Address>
               ip-protocol esp
               composite-operation Permit
               exit
      ip-rule 50
               source-ip host <Branch Office Public Internet Static
                                                        IP Address>
               destination-ip any
               ip-protocol icmp
      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 10/2
     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 acl-group      in   301
     ip acl-group      out 302
     exit

interface Tunnel 1
; The following two backup commands specify redundant mode.
; To specify load-sharing mode, omit them.
    backup interface Tunnel 2
    backup delay 20 15
    keepalive 10 3
    tunnel source  <Branch GRE Tunnel end point IP Address>
    tunnel destination <Primary MainPrimary Main Office GRE Tunnel end
point IP
                                                              Address>
    ip address 10.10.10.1 255.255.255.252
    exit
interface Tunnel 2
   keepalive 10 3
   tunnel source  <Branch GRE Tunnel end point IP Address>
   tunnel destination <Backup Main Office GRE Tunnel end point IP
                                                              Address>
   ip address 20.20.20.1 255.255.255.252
   exit
```

```
ip route <Primary Main Offfice GRE Tunnel end point IP Address>
                                    255.255.255.255 FastEthernet 10/2 high
ip route <Backup Main Offfice GRE Tunnel end point IP Address>
                                    255.255.255.255 FastEthernet 10/2 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
```

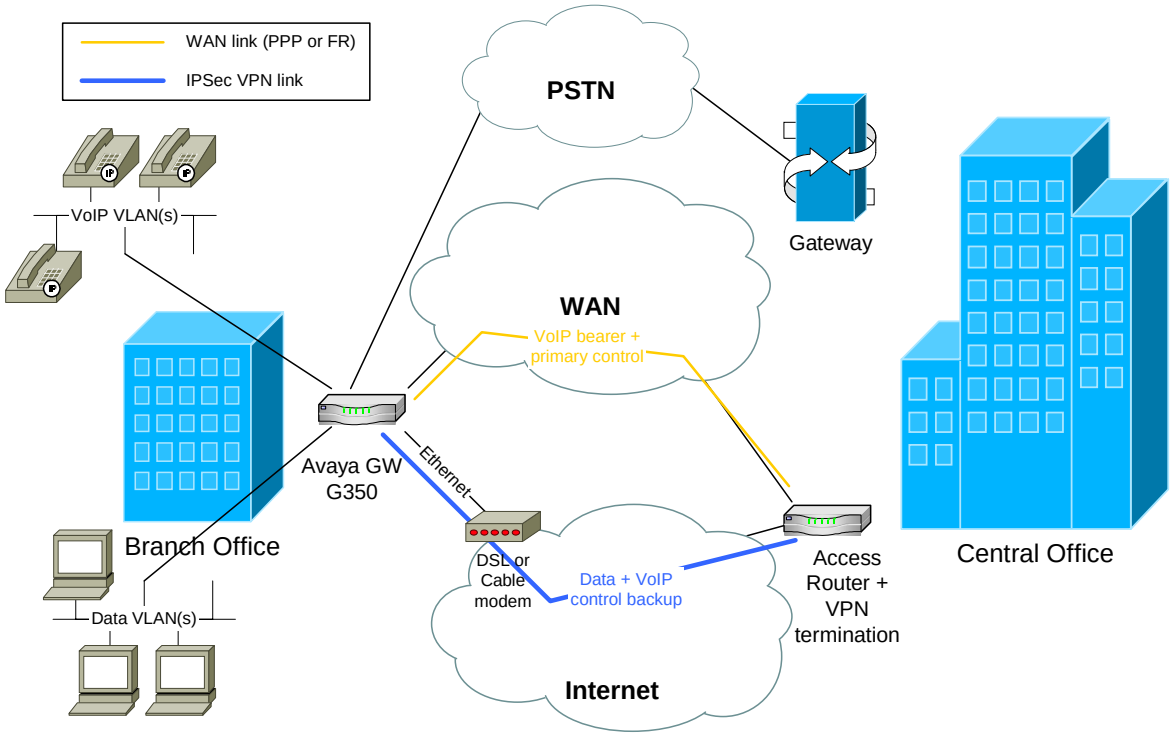
Full solution: hub-and-spoke with VPN for data and VoIP control backup

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 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.

Figure 21: 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

This section describes how to configure Hub-and-spoke with VPN for data and VoIP control backup, followed by a detailed configuration example.

To configure Hub-and-spoke with VPN for data and VoIP control backup:

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.
   - ACL is configured on the Internet interface to allow only the VPN tunnel and ICMP traffic, as follows:

     Ingress:

     1. IKE (UDP/500) from remote tunnel endpoint to local tunnel endpoint -> Permit
     2. ESP/AH from remote tunnel endpoint to local tunnel endpoint -> Permit
     3. Remote GRE tunnel endpoint to local GRE tunnel endpoint -> Permit

4. Allowed ICMP from anyone to local tunnel endpoint -> Permit
5. Default -> Deny

Egress:

1. IKE (UDP/500) from local tunnel endpoint to remote tunnel endpoint -> Permit
2. Local GRE tunnel endpoint to remote GRE tunnel endpoint -> Permit
3. All allowed services from any local subnet to anyone -> Permit
4. Allowed ICMP from local tunnel endpoint to anyone -> Permit
5. Default -> Deny

- 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

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.
   - Policy Based Routing (PBR) portion for the branch is configured as follows, on most interfaces:
     - Destination IP = branch VoIP subnet(s) or GW address (PMI), DSCP = bearer -> Route: WAN
     - Destination IP = branch VoIP subnet(s) 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.

Configuration 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
     ip-rule default
               no protect
               exit
     exit

ip access-control-list 301
      ip-rule 10
               source-ip host <Main Office Public Internet Static IP
                                                              Address>
               destination-ip host <Branch Office Public Internet Static
                                                            IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
```

```
      ip-rule 20
               source-ip host <Main Office Public Internet Static IP
                                                              Address>
               destination-ip host <Branch Office Public Internet Static
                                                          IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
     ip-rule 30
               source-ip any
               destination-ip host <Branch Office Public Internet Static
                                                          IP Address>
               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 host <Branch Office Public Internet Static IP
                                                              Address>
               destination-ip host <Main Office Public Internet Static
                                                          IP Address>
               ip-protocol udp
               udp destination-port  Ike
               composite-operation  Permit
               exit
      ip-rule 20
               source-ip host <Branch Office Public Internet Static IP
                                                              Address>
               destination-ip host <Main Office Public Internet Static
                                                          IP Address>
               ip-protocol esp
               composite-operation  Permit
               exit
```

```
      ip-rule 30
               source-ip host  <Branch Office Public Internet Static IP
                                                                Address>
               destination-ip any
               ip-protocol icmp
      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 10/2
     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 acl-group      in   301
     ip acl-group      out 302
     exit
```

```
interface Serial  2/1
     ip address <Branch Office serial IP address> <Branch Office serial
                                                                net mask>
     exit

ip next-hop-list 1
    next-hop-interface 1 Serial 2/1
    exit
ip next-hop-list 2
    next-hop-interface 1 Serial 2/1
    next-hop-interface 2 FastEthernet 10/2
    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
```

Chapter 18: Configuring policy

This chapter provides information about configuring QoS policy on the G350 and contains the following sections:

- Policy overview — an overview of QoS policy configuration
- Defining policy lists — instructions on how to configure policy lists
- Attaching policy lists to an interface — instructions on how to attach a policy list to an interface
- Device-wide policy lists — instructions on how to attach a policy list to all interfaces
- Defining global rules — instructions on how to configure rules that are executed before the list is evaluated
- Defining rules — instructions on how to configure rules, including an overview of rule criteria
- Composite operations — a description of composite operations and instructions on how to configure composite operations
- DSCP table — a description of the DSCP table, with examples
- Displaying and testing policy lists — instructions on how to view the configuration of policy lists and test their effects on simulated IP packets

Policy overview

This section provides an overview of policy lists on the G350 and includes the following topics:

- Access control lists — a description of access control lists, which control which packets are authorized to pass through an interface
- QoS lists — a description of QoS lists, which can change the value of the QoS field in a packet
- Policy-based routing — an overview of policy-based routing, which is described in more detail in Configuring policy-based routing on page 273
- Managing policy lists — an overview of how to manage policy lists on the G350

Access control lists

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 G350:

- 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

Access lists have the following parts:

- **Global rules** — a set of rules that are executed before the list is evaluated
- **Rule list** — a list of filtering rules and actions for the G350 to take when a packet matches the rule. Match actions on this list are pointers to the composite operation table.
- **Actions (composite operation table)** — a table that describes actions to be performed when a packet matches a rule. The table includes pre-defined actions such as permit and deny. You can configure more complex rules. See Composite operations on page 266.

QoS lists

You can use QoS lists to change the DSCP and Ethernet IEEE 802.1p CoS fields in packets. When a packet matches a rule on the QoS list, the G350 sets one or both of the QoS fields in the packet. The following table shows these QoS fields:

Layer	QoS field	Allowed values
2	802.1p	0–7
3	DSCP	0–63

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 lists have the following parts:

- **Rule list** — a list of filtering rules and actions for the G350 to take when a packet matches the rule. Match actions on this list are pointers to the composite operation table.
- **Actions (composite operation table)** — a table that describes actions to be performed when a packet matches a rule. The table includes pre-defined actions such as permit and deny. You can configure more complex rules. See Composite operations on page 266.
- **DSCP map** — a table that contains DSCP code points and match action pairs. Match actions are pointers to the composite operation table.

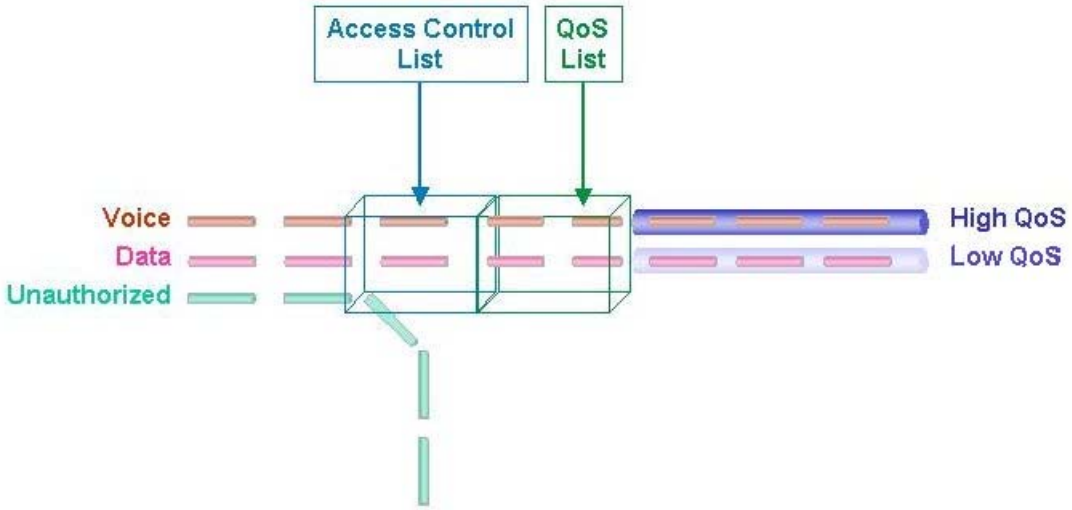
Policy-based routing

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 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 Configuring policy-based routing on page 273.

Managing policy lists

You can manage policy lists on the Avaya G350 Media 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. Figure 22: Policy lists on page 255 illustrates the operation of policy lists on the Avaya G350 Media Gateway:

Figure 22: Policy lists



Defining policy lists

This section provides information on how to define policy lists and includes the following topics:

- Creating and editing a policy list — instructions on how to create or edit a policy list
- Defining list identification attributes — instructions on how to configure the attributes of a policy list, such as a list name, owner, and cookie
- Default actions — lists the default action the G350 takes when no rule in the policy list matches the packet
- Deleting a policy list — instructions on how to delete a policy list

Creating and editing a policy list

To create or edit a policy list, you must 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, type **`ip access-control-list`**, followed by a list number in the range 300-399. The G350 includes one pre-configured access control list. The pre-configured access control list is list number 300. Thus, to create a new access control list, you can type the following command:

```
ip access-control-list 301
```

To create or edit a QoS list, type **`ip qos-list`**, followed by a list number in the range 400-499. The G350 includes one pre-configured QoS list. The pre-configured QoS list is list number 400. Thus, to create a new QoS list, you can type the following command:

```
ip qos-list 401
```

Once you have entered the list context, you can perform the following actions:

- **Configure rules** — see Defining rules on page 261
- **Configure composite operations** — see Composite operations on page 266
- **Configure DSCP mapping (Qos lists only)** — see DSCP table on page 269

Defining list identification attributes

The following policy list attributes are used by Avaya QoS Manager software to identify policy lists:

- Name
- Owner
- Cookie

To define these attributes:

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`** — defines a list name (text string). The default value is *owner*.
   - **`owner`** — defines a list owner (text string). The default value is *list#<listnumber>*.
   - **`cookie`** — defines a list cookie (integer). The Avaya QoS Manager uses the cookie attribute internally. Normally, you should not change this attribute.

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`**.

To view the attributes, use the **`show list`** command in the context of the list.

Default actions

When no rule matches a packet, the G350 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

To delete an access control list, type **`no ip access-control-list`**, followed by the number of the list you want to delete. To delete a QoS list, type no **`ip qos-list`**, followed by the number of the list you want to delete.

Attaching policy lists to an interface

The following policy lists are attached to each interface on the Avaya G350 Media Gateway:

- Ingress Access Control List
- Ingress QoS List
- Egress Access Control List
- Egress QoS List

Note:

You can also attach PBR lists to certain interfaces, but PBR lists are not attached to any interface by default.

When a packet enters the G350 through an interface, the G350 applies the policy lists in the following order:

1. Apply the Ingress Access Control List.

   If the Ingress Access Control List does not drop the packet:

2. Apply the Ingress QoS List.
3. Apply the PBR list (if any).
4. The packet enters the G350 through the interface.

When a packet exits the G350 through an interface, the G350 applies the policy lists in the following order:

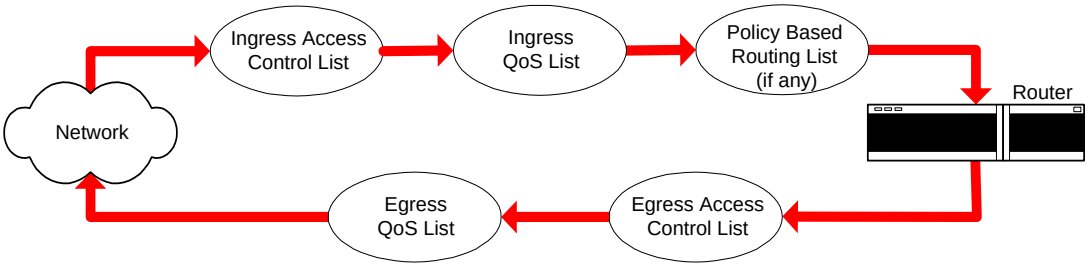
1. Apply the Egress Access Control List.

   If the Egress Access Control List does not drop the packet:

2. Apply the Egress QoS List.
3. The packet exits the G350 through the interface.

Figure 23: Applying Policy Lists to Packets on page 258 illustrates the order in which the G350 applies policy lists to packets.

Figure 23: Applying Policy Lists to Packets



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 G350. You can choose the Ingress QoS List and the Egress QoS List from among the QoS lists that are configured on the G350.

To attach an access control list to an interface as its Ingress Access Control List, enter the interface context and type **`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 type **`ip access-group`** ***`list number`*** **`out`**.

To attach a QoS list to an interface as its Ingress QoS List, enter the interface context and type **`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 type **`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.

```
G350-001# interface Vlan 2
G350-001(if:Vlan 2)# ip access-group 301 in
Done!
G350-001(if:Vlan 2)# ip qos-group 401 out
Done!
```

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 typing the following commands:

```
G350-001(super)# interface Vlan 1
G350-001(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 G350 using one command. To do this, attach a list to the Loopback 1 interface. For more information, see Attaching policy lists to an interface on page 258.

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 G350 applies the lists in the following order:

- Incoming packets:
  a. Apply the ingress policy lists that are attached to the interface.
  b. Apply the device-wide ingress policy lists.
- Outgoing packets:
  a. Apply the device-wide egress policy lists.
  b. Apply the egress policy lists that are attached to the interface.

Defining global rules

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 Defining rules on page 261.

The G350 applies global rules before applying individual rules.

To define a global rule:

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-fragments-out`** — applies to outgoing packets that contain IP fragments
   - **`ip-options-in`** — applies to incoming packets that contain IP options
   - **`ip-options-out`** — applies to outgoing packets that contain IP options

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, type the command **`show composite-operation`** in the context of the access control list.

The following example defines a rule in Access Control List 301 that denies access to all incoming packets that contain IP fragments:

```
G350-001(super)# ip access-control-list 301
G350-001(super/ACL 301)# ip-fragments-in Deny
Done!
```

Defining rules

This section provides information on how to configure rules in a policy list and contains the following topics:

- Overview of rule criteria — an overview of the criteria that can be used in configuring policy rules
- Editing and creating rules — instructions on how to edit or create a policy rule
- Rule criteria — instructions on how to configure a policy rule's criteria

Overview of rule criteria

You can configure policy rules to match packets based on one or more of the following criteria:

- Source IP address, or a range of addresses
- Destination IP address or a range of addresses
- IP protocol, such as TCP, UDP, ICMP, IGMP
- Source TCP or UDP port or a range of ports
- Destination TCP or UDP port or a range of ports
- ICMP type and code

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

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.

To enter a rule context:

1. Enter the context of the list in which you want to create or edit a rule.
2. Type the command **ip-rule**, followed by the number of the rule you want to create or edit. For example, to create rule 1, type **ip-rule 1**.

To view the existing rules in a list, enter the list's context and type **ip show-rule**. Each list starts with a default rule. Each new rule has the same default parameters as the default rule. The default rule appears as follows:

```
Index Protocol IP  Wildcard         Port            Operation
----- -------- --- ---------------- --------------- ------------ ----
Deflt Any      Src Any              Any             Permit
Dst   Any          Any
```

This rule permits all packets.

Rule criteria

This section describes the rule criteria you can define and includes the following topics:

- IP protocol — instructions on how to define the protocol to which the rule applies
- Source and destination IP address — instructions on how to define the source and destination IP addresses to which the rule applies
- Source and destination port range — instructions on how to define the source and destination port ranges to which the rule applies
- ICMP type and code — instructions on how to define packet matching by ICMP type or code
- TCP Establish bit (access control lists only) — instructions on how to define packet matching for TCP packets by whether the ack bit is burned on

IP protocol

To specify the IP protocol to which the rule applies, use the **ip-protocol** command, followed by the name of an IP protocol. If you want the rule to apply to all protocol, 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.

The following command specifies the UDP protocol for rule 1 in QoS list 401:

```
G350-001(QoS 401/rule 1)# ip-protocol udp
```

The following command specifies any IP protocol except IGMP for rule 3 in access control list 302:

```
G350-001(ACL 302/ip rule 3)# no ip-protocol igmp
```

Source and destination IP address

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. The IP range criteria can be any of the following:

- a range — type two IP addresses to set a range of IP addresses to which the rule applies
- a 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
- any — 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.

The following command specifies a source IP address of 10.10.10.20 for rule 1 in access control list 301:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(ACL 350/ip rule 6)# source-ip 64.*.24.*
```

Source and destination port range

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

This command also sets the IP protocol parameter to TCP or UDP.

The port name or number range criteria can be any of the following:

- a range — type **`range`**, followed by two port numbers, to set a range of port numbers to which the rule applies
- equal — type **`eq`**, followed by a port name or number, to set a port name or port number to which the rule applies
- 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
- 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
- any — type **`any`** to apply the rule to all port names and port numbers

Use the **no** form of the appropriate command to specify that the rule does not apply to the ports defined by the command.

The following command specifies a source TCP port named *telnet* for rule 1 in access control list 301:

```
G350-001(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:

```
G350-001(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:

```
G350-001(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:

```
G350-001(ACL 304/ip rule 7)# no tcp source-port eq http
```

ICMP type and code

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. To apply the rule to all ICMP packets except the specified type and code, use the **no** form of this command.

The following command specifies an ICMP echo reply packet for rule 1 in QoS list 401:

```
G350-001(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:

```
G350-001(ACL 321/ip rule 5)# no icmp 1 2
```

TCP Establish bit (access control lists only)

Use the **tcp established** command to specify that the rule only applies to packets that are part of an established TCP session. Use the **no** form of this command to specify that the rule applies to all TCP packets. In either case, the command also sets the IP protocol parameter to TCP.

The following command specifies that rule 6 in access control list 301 only matches packets that are part of an established TCP session:

```
G350-001(ACL 301/ip rule 6)# tcp established
```

Operation

Use the **operation** command, followed by the name of a composite operation, to specify an operation for the G350 to perform on a packet when the packet matches the rule. For an explanation of composite operations, see Composite operations on page 266.

The operation field for access control lists has a default value of *Permit*. See Pre-configured composite operations for access control lists on page 266.

The operation field for QoS lists has a default value of *Trust-DSCP-CoS*. See Pre-configured composite operations for QoS lists on page 267.

The following command specifies that rule 4 in access control list 302 drops packets that match the rule, and causes the G350 to send a trap and reset the connection when the packet is dropped:

```
G350-001(ACL 304/ip rule 4)# operation Deny-Notify-Rst
```

Note:

Composite operation names are case-sensitive.

Composite operations

This section describes composite operations and includes the following topics:

- Overview of composite operations — an overview of composite operations and how they are used
- Pre-configured composite operations for access control lists — a list and descriptions of the pre-configured composite operations that you can use in access control list rules
- Pre-configured composite operations for QoS lists — a list and descriptions of the pre-configured composite operations that you can use in QOS list rules
- Configuring composite operations — instructions on how to configure additional composite operations
- Composite operation example — an example of configuring a composite operation and attaching it to a rule

Overview of composite operations

A composite operation is a set of operations that the G350 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 G350 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 G350 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 G350 to send a trap when it drops a packet
- **Reset Connection** — determines whether the operation causes the G350 to reset the connection when it drops a packet

Pre-configured composite operations for QoS lists

Table 10: Pre-configured QoS list composite operations on page 267 lists the pre-configured entries in the composite operation table for rules in a QoS list:

Table 10: Pre-configured QoS list composite operations

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 great 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

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.

To create or edit a composite operation:

1. Enter the context of a QoS list.
2. Type the **`composite-operation`** command, 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`** — determines the value to which the rule resets the packet's DSCP field. To ignore the DSCP field, use the argument **`no change`**, or use the command **`no dscp`**.
   - **`cos`** — determines the value to which the rule resets the packet's CoS field. To ignore the CoS field, use the argument **`no change`**, or use the command **`no cos`**.
4. Use the **`name`** command, 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.

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 G350 changes the value of the DSCP field in the packet to 5.

```
G350-001# ip qos-list 402
G350-001(QoS 402)# composite-operation 12
G350-001(QoS 402/cot 12)# name dscp5
Done!
G350-001(QoS 402/cot 12)# dscp 5
Done!
G350-001(QoS 402/cot 12)# cos no-change
Done!
G350-001(QoS 402/cot 12)# exit
G350-001(QoS 402)# ip-rule 3
G350-001(QoS 402/rule 3)# composite-operation dscp5
Done!
```

DSCP table

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 267.

QoS rules on the list take precedence over the DSCP table. If a QoS rule other than the default matches the packet, the G350 does not apply the DSCP table to the packet. The G350 applies only the operation specified in the QoS rule.

To change an entry in the DSCP table:

1. Enter the context of a QoS list.
2. Type the command **`dscp-table`**, followed by the number of the DSCP value for which you want to change its composite operation.
3. Type the command **`composite-operation`**, followed by the name of the composite operation you want to execute for packets with the specified DSCP value.

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.

```
G350-001# ip qos-list 401
G350-001(QoS 401)# dscp-table 33
G350-001(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.

```
G350-001(super)# ip qos-list 402
G350-001(super/QoS 402)# composite-operation 12
G350-001(super/QoS 402/CompOp 12)# name dscp5
Done!
G350-001(super/QoS 402/CompOp 12)# dscp 5
Done!
G350-001(super/QoS 402/CompOp 12)# cos No-Change
Done!
G350-001(super/QoS 402/CompOp 12)# exit
G350-001(super/QoS 402)# dscp-table 7
G350-001(super/QoS 402/dscp 7)# composite-operation dscp5
Done!
```

Displaying and testing policy lists

To verify access control lists and QoS lists, you can view the configuration of the lists. You can also test the effect of the lists on simulated IP packets.

Displaying policy lists

To view information about policy lists and their components, use the following commands. Many of 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 access control list context:
  - **`show composite-operation`** — displays a list of all composite operations configured for the list
  - **`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 access control list 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 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 QoS list 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 QoS list DSCP table context:
  - **`show dscp-table`** — displays the parameters of the current DSCP table entry
- In QoS list composite operation context:
  - **`show composite-operation`** — displays the parameters of the current composite operation

Simulating packets

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. You must 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 G350 Media Gateway CLI Reference*, 555-245-202.

The following command simulates the effect of applying QoS list number 401 to a packet entering the G350 through interface VLAN 2:

```
G350-001(if:Vlan 2)# ip simulate 401 in CoS1 dscp46 10.1.1.1
10.2.2.2 tcp 1182 20
```

The simulated packet has the following 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

When you run the **ip simulate** command, the G350 displays the effect of the policy rules on the simulated packet. For example:

```
G350-001(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
```

Chapter 19: Configuring policy-based routing

This chapter provides information about configuring policy-based routing on the G350 and contains the following sections:

- Policy-based routing overview — an overview of policy-based routing
- Applications — a description of common policy-based routing applications
- Configuring Policy-Based Routing — instructions on how to configure policy-based routing
- PBR Rules — instructions on how to configure rules
- Next Hop Lists — instructions on how to configure next hop lists
- Editing and Deleting PBR lists — instructions on how to modify and delete PBR lists
- Displaying PBR lists — instructions on how to view the configuration of PBR lists
- Application example — an example of a policy-based routing application

Policy-based routing overview

Policy-based routing allows 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 G350 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 Figure 23: Applying Policy Lists to Packets on page 258.

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 G350 device itself, as explained below.

Note:

Extended keepalive provides the interface with the ability to determine whether a next hop is or is not available. See Extended keepalive on page 99.

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 G350 itself. This includes ping packets to or from the G350, as well as telnet, 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 G350 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 G350, 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.

Applications

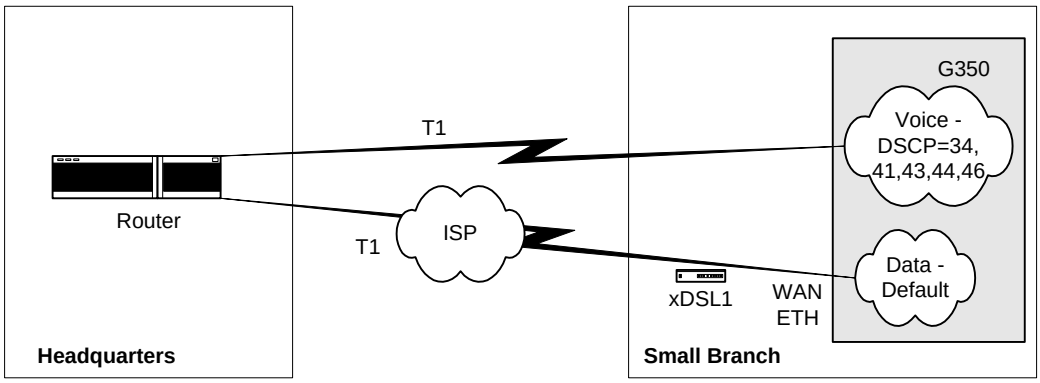
The most common application for policy-based routing is to provide for separate routing of voice and data traffic. It can also be used as a means to provide backup routes for defined traffic types.

Separate routing of voice and data traffic

Although there are many possible applications for policy-based routing, the most common application is to create separate routing for voice and data traffic.

For example, the application shown in Figure 24: Policy-based routing — Voice/Data Division By DSCP on page 275 uses the DSCP field to identify VoIP control packets (DSCP=34, 41), VoIP Bearer RESV packets (DSCP = 43, 44), and VoIP Bearer packets (DSCP = 46). Policy-based routing sends these packets over the T1 WAN line, and sends other packets over the Internet. This saves bandwidth on the more expensive serial interface.

Figure 24: Policy-based routing — Voice/Data Division By DSCP



Backup

You can utilize policy-based routing to define backup routes for defined classes of traffic. If the first route on the next hop list fails, the packets are routed to a subsequent hop. When necessary, you can use the NULL interface to drop packets when the primary next hop fails. For example, voice packets are usually sent over a WAN line, and not the Internet. You can configure a PBR list to drop voice packets when the WAN line is down.

Configuring Policy-Based Routing

This section provides step-by-step instructions for configuring policy-based routing on an interface. For a full example of a policy-based routing configuration, see Application example on page 283.

To configure policy-based routing:

1. Define PBR lists.

   In general context, type **ip pbr-list**, followed by a list number in the range 800-899. For example:

   ```
   G350-001(super)# ip pbr-list 802
   G350-001(super-PBR 802)#
   ```

   To assign a name to the list, use the **name** command, followed by a text string, in the PBR list context. The default name is *list #<list number>*. For example:

   ```
   G350-001(super-PBR 802)# name "voice"
   Done!
   G350-001(super-PBR 802)#
   ```

   To assign an owner to the list, use the **owner** command, followed by a text string, in the PBR list context. The default owner is *other*. For example:

   ```
   G350-001(super-PBR 802)# owner "tom"
   Done!
   G350-001(super-PBR 802)#
   ```

2. Define PBR rules.

   In the PBR list context, use the **ip-rule** command, followed by the number of the rule, to define a rule for the PBR list. Repeat this command to define additional rules. A rule contains (i) criteria that is matched against the packet, and (ii) a next hop list. When a packet matches the criteria specified in the rule, the rule's next hop list determines how the packet is routed. Each PBR list can have up to 1,500 rules. The first rule that matches the packet determines the packet's routing.

   It is important to include a destination address, or range of addresses, in PBR rules to better classify the traffic to be routed. For an illustration, see Application example on page 283.

   Note:

   It is recommended to leave a gap between rule numbers, in order to leave room for inserting additional rules at a later time. For example, ip-rule 10, ip-rule 20, ip-rule 30.

The following example creates rule 1, which routes packets going to IP address 149.49.43.210 with a DSCP value of 34 according to next hop list 1. The next step explains how to define a next hop list. For additional details about PBR rules, see PBR Rules on page 279.

```
G350-001(super-PBR 802)# ip-rule 1
G350-001(super-PBR 802/ip rule 1)# next-hop list 1
Done!
G350-001(super-PBR 802/ip rule 1)# destination-ip host 149.49.43.210
Done!
G350-001(super-PBR 802/ip rule 1)# dscp 43
Done!
G350-001(super-PBR 802/ip rule 1)#
```

Note:

Rules do not include a default next hop list. Thus, if you do not include a next hop list in the rule, the packet is routed according to destination-based routing, i.e., the ordinary routing that would apply without policy-based routing.

3. Define next hop lists.

Use the **`exit`** command twice to return to general context. In general context, define all the next hop lists that you have used in PBR rules.

Note:

You can also perform this step before defining PBR lists and rules.

Use the **`ip next-hop-list`** command, followed by the number of the list, to define a next hop list. In the next hop list context, use the following commands to define the next hops in the list:

- Use the **`next-hop-ip`** command, followed by the index number of the entry in the next hop list, to define an IP address as a next hop.
- Use the **`next-hop-interface`** command, followed by the index number of the entry in the next hop list, to define an interface as a next hop.

You can also use the **`name`** command to assign a name to the next hop list.

Note:

You cannot use a Fast Ethernet interface as an entry on a next hop list unless the interface was previously configured to use PPPoE encapsulation or a GRE tunnel. See Configuring PPPoE on page 91 and Configuring GRE tunneling on page 166.

A next hop list can include the value NULL0. When the next hop is NULL0, the G350 drops the packet.

The following example creates next hop list 1, named *"Voice to HQ"*, with three entries:

- The first entry is IP address 172.16.1.221.
- The second entry is Serial interface 2/1:1.

- The third entry is NULL, which means the packet is dropped.

```
G350-001(super)# ip next-hop-list 1
G350-001(super-next hop list 1)#name "Voice_to_HQ"
Done!
G350-001(super-next hop list 1)#next-hop-ip 1 172.16.1.221
Done!
G350-001(super-next hop list 1)#next-hop-interface 2 Serial 2/1:1
Done!
G350-001(super-next hop list 1)#next-hop-interface 3 Null0
Done!
G350-001(super-next hop list 1)#
```

For additional details about next hop lists, see Next Hop Lists on page 280

4. Apply the PBR list to an interface.

   Use the **exit** command to return to general context. From general context, enter the interface to which you want to apply the PBR list. In the interface context, use the **ip pbr-group** command, followed by the number of the PBR list, to attach the list to the interface. The list will be applied to packets entering the interface.

   The following example applies PBR list 802 to VLAN 2.

```
G350-001(super)# interface Vlan 2
G350-001(super-if:Vlan 2)# ip pbr-group 802
Done!
G350-001(super-if:Vlan 2)#
```

5. Apply the PBR list to the Loopback interface.

   The following example applies PBR list 802 to the Loopback interface.

```
G350-001(super)# interface Loopback 1
G350-001(super-if:Loopback 1)# ip pbr-group 802
Done!
G350-001(super-if:Loopback 1)# exit
G350-001(super)#
```

6. Type the **copy running-config startup-config** command. This saves the new policy-based routing configuration in the startup configuration file.

PBR Rules

Each PBR list can have up to 1,500 rules. The first rule that matches the packet specifies the next hop list for the packet. If no rule matches the packet, the packet is routed according to the default rule.

This section provides information on how to configure rules in a PBR list and contains the following topics:

- Overview of rule criteria — an overview of the criteria that can be used in configuring PBR rules
- Modifying rules — instructions on how to create and edit a PBR rule
- Rule criteria — instructions on how to configure a PBR rule's criteria

Overview of rule criteria

You can configure policy rules to match packets based on one or more of the following criteria:

- Source IP address, or a range of addresses
- Destination IP address or a range of addresses
- IP protocol, such as TCP, UDP, ICMP, IGMP
- Source TCP or UDP port or a range of ports
- Destination TCP or UDP port or a range of ports
- ICMP type and code
- DSCP field

Use IP wildcards to specify a range of source or destination IP addresses. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard correspond to bits in the IP address that can vary. Note that this is the opposite of how bits are used in a subnet mask.

Note:

When you use destination and source ports in a PBR rule, policy-based routing does not catch fragments.

Note:

It is recommended to leave a gap between rule numbers, in order to leave room for inserting additional rules at a later time. For example, ip-rule 10, ip-rule 20, ip-rule 30.

Modifying rules

To modify a policy-based routing rule, you must enter the context of the rule and redefine the rule criteria.

To enter a rule context:

1. Enter the context of the PBR list to which the rule belongs.
2. Type the command **`ip-rule`**, followed by the number of the rule you want to modify. For example, to create rule 1, type **`ip-rule 1`**.

To view the rules that belong to a PBR list, enter the list's context and type **`ip show-rule`**.

Rule criteria

The rule criteria for PBR rules are largely the same as the rule criteria for other policy list rules. Refer to Rule criteria on page 262.

In addition, PBR rules can use the packet's DSCP field as a rule criteria. 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.

Unlike other policy lists, PBR lists do not use composite operations. Thus, there is no **`operation`** command in the context of a PBR rule. Instead, PBR lists use next hop lists. For an explanation of next hop lists, see Next Hop Lists on page 280.

Use the **`next-hop list`** command, followed by the list number of a next hop list, to specify a next hop list for the G350 to apply to packets that match the rule. You can specify *Destination Based Routing* instead of a next hop list, in which case the G350 applies destination-based routing to a packet when the packet matches the rule.

If the next hop list specified in the rule does not exist, the G350 applies destination-based routing to packets that match the rule.

Next Hop Lists

PBR rules include a next hop list. When the rule matches a packet, the G350 routes the packet according to the specified next hop list.

This section describes next hop lists and contains the following topics:

- Next hop list overview — an overview of next hop lists
- Modifying next hop lists — instructions on how to modify a next hop list

Next hop list overview

Each next hop list can include up to 20 entries. An entry in a next hop list can be either an IP address or an interface. The G350 attempts to route the packet to the first available destination on the next hop list. If every destination on the list is unavailable, the G350 routes the packet according to destination-based routing.

Modifying next hop lists

To modify a next hop list, you must enter the context of the next hop list. To enter a next hop list context, type the command **`ip next-hop-list`**, followed by the number of the list you want to edit. For example, to modify next hop list 1, type **`ip next-hop-list 1`**.

To show the next hops in an existing list, enter the context of the next hop list and type **`show next-hop`**.

To add entries to a next hop list:

1. Enter the context of the next hop list.
2. Use one of the following commands:
   - To enter an IP address as a next hop, use the **`next-hop-ip`** command, followed by the index number of the entry and the IP address. For example, the command **`next-hop-ip 2 149.49.200.2`** sets the IP address 149.49.200.2 as the second entry on the next hop list.
   - To enter an interface as a next hop, use the **`next-hop-interface`** command, followed by the index number of the entry and the name of the interface. For example, the command **`next-hop-interface 3 Serial 5/1:1.1`** sets VLAN 2 as the third entry on the next hop list.

To delete an entry from a next hop list:

1. Enter the context of the next hop list.
2. Use one of the following commands:
   - To delete an IP address, use the **`no next-hop-ip`** command, followed by the index number of the entry you want to delete. For example, the command **`no next-hop-ip 2`** deletes the second entry from the next hop list.
   - To delete an interface, use the **`no next-hop-interface`** command, followed by the index number of the entry you want to delete. For example, the command **`no next-hop-interface 3`** deletes the third entry from the next hop list.

Editing and Deleting PBR lists

You cannot delete or modify a PBR list when it is attached to an interface. In order to delete or modify a PBR list, you must first remove the list from the interface. You can then delete or modify the list. After modifying the list, you can reattach the list to the interface.

To remove a list from an interface, use the **no** form of the **ip pbr-group** command in the interface context. The following example removes the PBR list from the Vlan 2 interface.

```
G350-001(super)# interface Vlan 1
G350-001(super-if:Vlan 1)# no ip pbr-group
Done!
G350-001(super-if:Vlan 1)#
```

To modify a PBR list, type **ip pbr-list**, followed by the number of the list you want to modify, to enter the list context. Redefine the parameters of the list.

To delete a PBR list, use the **exit** command to return to general context and type **no ip pbr-list**, followed by the number of the list you want to delete.

Displaying PBR lists

To view information about PBR lists and their components, use the following commands. Many of these commands produce different results in different contexts.

- In general context:
  - **show ip pbr-list** — displays a list of all configured PBR lists, with their list numbers and names and their owners
  - **show ip pbr-list *list number*** — displays the list number and name of the specified PBR list
  - **show ip pbr-list all detailed** — displays all the parameters of all configured PBR lists
  - **show ip pbr-list *list number* detailed** — displays all the parameters of the specified PBR list
  - **show ip active-lists** — displays a list of each G350 interface to which a PBR list is attached, along with the number and name of the PBR list
  - **show ip active-lists *list number*** — displays a list of each G350 interface to which the specified PBR list is attached, along with the number and name of the PBR list
  - **show ip next-hop-list all** — displays the number and name of all next hop lists
  - **show ip next-hop-list *list number*** — displays the number and name of the specified next hop list

- In PBR list context:
  - **`show list`** — displays all the parameters of the current PBR list
  - **`show ip-rule`** — displays the parameters of all rules configured for the current list
  - **`show ip-rule rule number`** — displays the parameters of the specified rule
- In next hop list context:
  - **`show next-hop`** — displays the next hop entries in the current next hop list and their current status

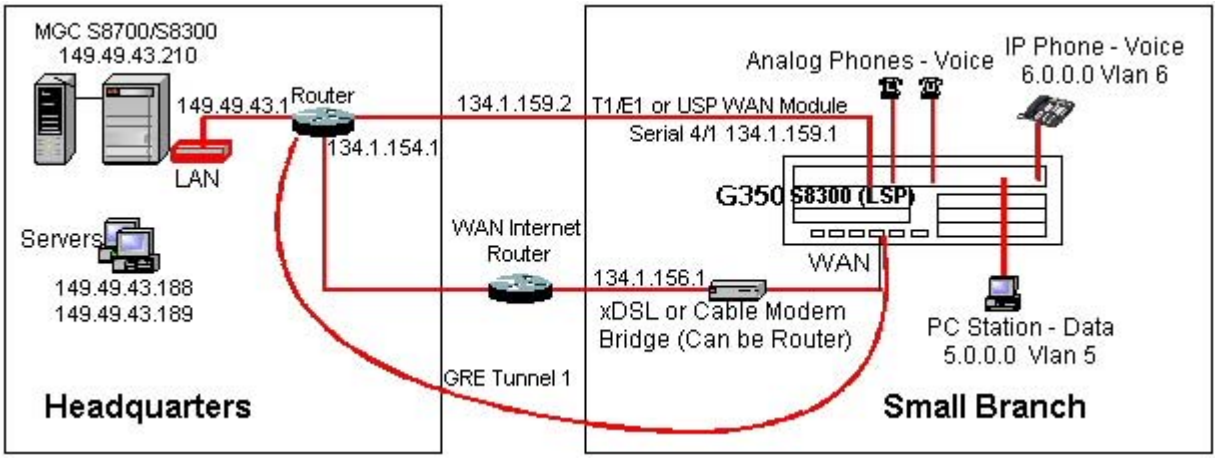
Application example

The following example creates a policy-based routing scheme in which:

- Voice traffic is routed over a serial interface. If the interface is down, the traffic is dropped.
- Data traffic is routed over a GRE tunnel. If the tunnel is down, the traffic is routed over the serial interface. If both interfaces are down, the traffic is dropped.

Figure 25: Sample policy-based routing application on page 283 illustrates the sample application described below.

Figure 25: Sample policy-based routing application



This example includes a voice VLAN (6) and a data VLAN (5). The PMI is on VLAN 6. The G350 is managed by a remote Media Gateway Controller (MGC) with the IP address 149.49.43.210. The G350 also includes a local S8300 in LSP mode.

IP phones are located on the same subnet as the PMI. Therefore, there is no routing between the PMI and the IP phones.

In this example, the object of policy-based routing is to route all voice traffic over the E1/T1 line, which is more expensive but provides the superior QoS necessary for voice traffic. Remaining traffic is to be routed over the more inexpensive Internet connection.

It is assumed that the IP phones on VLAN 6 establish connections with other IP phones on the same subnet, sending signalling packets to the MGC, and bearer packets directly to other IP phones or to the G350.

The policy-based routing configuring starts with PBR list 801. This list requires all voice packets addressed to the MGC (149.49.43.210) with DSCP values that indicate voice transmission (34, 41, 43, 44, and 46) to be routed according to next hop list 1. This list directs packets to the T1/E1 interface (Serial 4/1). If that interface is down, the packets are dropped.

In this example, it is important to include the destination IP address in each rule. This is because without the destination address, calls from IP phones on VLAN 6 to a Softphone on VLAN 5 will be routed by the PBR list to the E1/T1 line, rather than being sent directly to VLAN 5 via the G350.

The following is the configuration for the application described above:

```
G350-001(super)# ip pbr-list 801
G350-001(super-PBR 801)# name "Voice"
Done!
G350-001(super-PBR 801)# ip-rule 1
G350-001(super-PBR 801/ip rule 1)# next-hop list 1
Done!
G350-001(super-PBR 801/ip rule 1)# destination-ip 149.49.123.0 0.0.0.255
Done!
G350-001(super-PBR 801/ip rule 1)# dscp 34
Done!
G350-001(super-PBR 801/ip rule 1)# exit
G350-001(super-PBR 801)# ip-rule 10
G350-001(super-PBR 801/ip rule 10)# next-hop list 1
Done!
G350-001(super-PBR 801/ip rule 10)# destination-ip 149.49.123.0 0.0.0.255
Done!
G350-001(super-PBR 801/ip rule 10)# dscp 41
Done!
G350-001(super-PBR 801/ip rule 10)# exit
Done!
G350-001(super-PBR 801/ip rule 20)# destination-ip 149.49.123.0 0.0.0.255
Done!
G350-001(super-PBR 801/ip rule 20)# dscp 43
Done!
G350-001(super-PBR 801/ip rule 20)# exit
G350-001(super-PBR 801)# ip-rule 30
G350-001(super-PBR 801/ip rule 30)# next-hop list 1
Done!
G350-001(super-PBR 801/ip rule 30)# destination-ip 149.49.123.0 0.0.0.255
Done!
G350-001(super-PBR 801/ip rule 30)# dscp 44
Done!
G350-001(super-PBR 801/ip rule 30)# exit
```

```
G350-001(super-PBR 801)# ip-rule 40
G350-001(super-PBR 801/ip rule 40)# next-hop list 1
Done!
G350-001(super-PBR 801/ip rule 40)# destination-ip 149.49.123.0 0.0.0.255
Done!
G350-001(super-PBR 801/ip rule 40)# dscp 46
Done!
G350-001(super-PBR 801/ip rule 40)# exit
G350-001(super-PBR 801)# exit
G350-001(super)#
```

The next group of commands configures next hop list 1, which was included in the rules configured above. Next hop list 1 sends packets that match the rule in which it is included to the E1/T1 line (serial interface 4/1). If that interface is not available, the next hop list requires the packet to be dropped (Null0). This is because the QoS on the Internet interface is not adequate for voice packets. It would also be possible to include one or more backup interfaces in the next hop list.

```
G350-001(super)# ip next-hop-list 1
G350-001(super-next hop list 1)#name "Voice-To_HQ"
Done!
G350-001(super-next hop list 1)#next-hop-interface 1 Serial 4/1
Done!
G350-001(super-next hop list 1)#next-hop-interface 2 Null0
Done!
G350-001(super-next hop list 1)#exit
G350-001(super)#
```

The next set of commands applies the PBR list to the voice VLAN (6).

```
G350-001(super)# interface Vlan 6
G350-001(super-if:Vlan 6)# ip pbr-group 801
Done!
G350-001(super-if:Vlan 6)# exit
G350-001(super)#
```

The next set of commands applies the PBR list to the Loopback interface. This is necessary to ensure that voice packets generated by the G350 itself are routed via the E1/T1 line. The Loopback interface is a logical interface that is always up. Packets sent from the G350, such as signaling packets, are sent via the Loopback interface. In this example, applying PBR list 801 to the Loopback interface ensures that signaling packets originating from voice traffic are sent via the T1/E1 line.

```
G350-001(super)# interface Loopback 1
G350-001(super-if:Loopback 1)# ip pbr-group 801
Done!
G350-001(super-if:Loopback 1)# exit
G350-001(super)#
```

The next set of commands defines a new PBR list (802). This list will be applied to the data interface (VLAN 5). The purpose of this is to route data traffic through interfaces other than the E1/T1 interface, so that this traffic will not interface with voice traffic.

```
G350-001(super)# ip pbr-list 802
G350-001(super-PBR 802)# name "Data_To_HQ"
Done!
G350-001(super-PBR 802)# ip-rule 1
G350-001(super-PBR 802/ip rule 1)# next-hop list 2
Done!
G350-001(super-PBR 802/ip rule 1)# ip-protocol tcp
Done!
G350-001(super-PBR 802/ip rule 1)# destination-ip host 149.49.43.189
Done!
G350-001(super-PBR 802/ip rule 1)# exit
G350-001(super-PBR 802)# exit
```

The next set of commands creates next hop list 2. This next hop list routes traffic to the GRE tunnel (Tunnel 1). If the GRE tunnel is not available, the next hop list checks the next entry on the list and routes the traffic to the E1/T1 interface (Serial 4/1). If neither interface is available, the traffic is dropped. This allows data traffic to use the E1/T1 interface, but only when the GRE tunnel is not available. Alternatively, the list can be configured without the E1/T1 interface, preventing data traffic from using the E1/T1 interface at all.

```
G350-001(super)# ip next-hop-list 2
G350-001(super-next hop list 2)#name "Data-To_HQ"
Done!
G350-001(super-next hop list 2)#next-hop-interface 1 Tunnel 1
Done!
G350-001(super-next hop list 2)#next-hop-interface 2 Serial 4/1
Done!
G350-001(super-next hop list 2)#next-hop-interface 3 Null0
Done!
G350-001(super-next hop list 2)#exit
G350-001(super)#
```

Finally, the next set of commands applies the PBR list to the data VLAN (5).

```
G350-001(super)# interface Vlan 5
G350-001(super-if:Vlan 6)# ip pbr-group 802
Done!
G350-001(super-if:Vlan 6)# exit
G350-001(super)#
```

Chapter 20: Setting synchronization

If the Avaya G350 Media Gateway contains an MM710 T1/E1 media module, it is advisable to define the MM710 as the primary synchronization source for the G350. In so doing, clock synchronization signals from the Central Office (CO) are used by the MM710 to synchronize all operations of the G350. If no MM710 is present, it is not necessary to set synchronization.

Use the **`set sync interface {primary|secondary} {`*`mmID`*`|[`*`portID`*`]}`** command to define a potential stratum clock source (T1/E1 Media Module, ISDN-BRI), where:

- *mmID* is the Media Module ID of an MM stratum clock source of the form vn, where n is the MM slot number.
- *portID* is the port number for an ISDN clock source candidate. The port ID consists of the slot number of the media module and the number of the port. You can set more than one port. For example: v2 1,3,5-8.

  Note:

  The port ID parameter only applies if the source is a BRI module.

By setting the clock source to primary, normal failover will occur. 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 not recommended to set the clock source to secondary except for testing purposes.

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.

If neither primary nor secondary sources are identified, the local clock becomes the active source.

The following example sets the MM710 media module located in slot 2 of the G350 chassis as the primary clock synchronization source for the Avaya G350 Media Gateway.

```
set sync interface primary v2
set sync source primary
```

If the G350 includes a second MM710 media module, enter the following additional command:

```
set sync interface secondary v3
set sync source secondary
```

If, for any reason, the primary MM710 media module cannot function as the clock synchronization source, the system uses the MM710 media module located in slot 3 of the G350 chassis as the clock synchronization source. If neither MM710 media module can function as the clock synchronization source, the system defaults to the local clock running on the S8300 Media Server.

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.
  - 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

Use the **`show sync timing`** command to display the status of the 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.

Chapter 21: FIPS

This chapter provides information about (i) the G350 cryptographic module's compliance with the Federal Information Processing Standard (FIPS-140-2) for cryptographic modules, and (ii) how to configure the module to work in FIPS mode. This chapter includes the following sections:

- Overview — an overview of the G350 (relating to FIPS compliance)
- Security rules — the security rules enforced by the cryptographic module to implement the security requirements of FIPS
- Password guidelines — the general guidelines for defining passwords
- Managing the module in FIPS-compliant mode — a description of the behavior of the module working in FIPS-approved mode of operation
- Administration procedures — step-by-step instructions on how to enter FIPS mode, failure scenarios, repair actions, and error states

Overview

The G350 device is a multi-chip stand-alone cryptographic module in a commercial grade metal case. The module provides:

- VPN, Voice over Internet Protocol (VoIP) media-gateway services, Ethernet switching, IP routing, and data security for IP traffic
- Status output via LEDs and logs available through the module's management interface
- Network interfaces for data input and output
- A console port

The cryptographic boundary includes all of the components within the physical enclosure of the G350 chassis, without any expansion modules. Figure 26 illustrates these interfaces and defines the cryptographic boundary.

Figure 26: Image of the cryptographic module

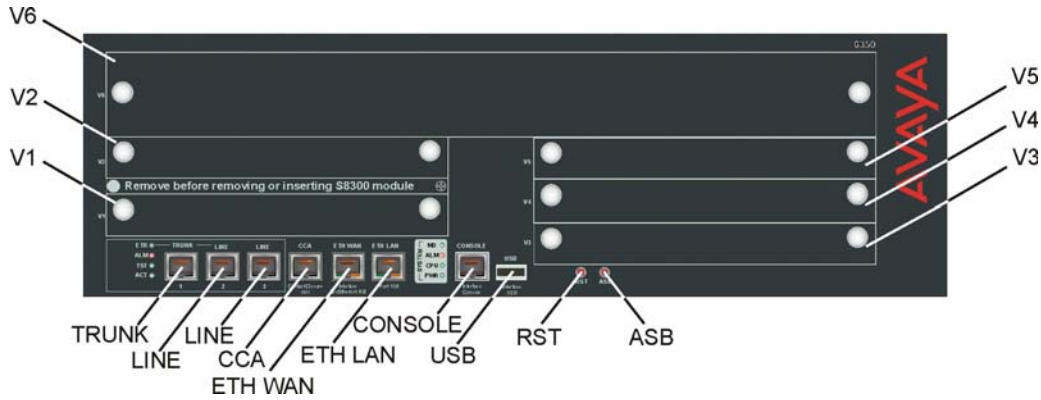


Table 11 and Table 12 describe the functions of the physical and logical fixed ports and the buttons on the G350 front panel.

Table 11: Physical and logical interfaces on the G350 front panel *1 of 2*

Physical interface	Quantity	Description	FIPS 140-2 logical interface	Comments
TRUNK	1	An analog trunk port. Part of an integrated analog media module.	N/A	
Analog LINE, LINE	2	Analog telephone ports of the integrated analog media module. An analog relay between TRUNK and the furthest left LINE port provides Emergency Transfer Relay (ETR) feature.	N/A	
CCA	1	RJ-45 port for ACS (308) contact closure adjunct box	• Power output	Contact Closure Adjunct. Powers two contact-closure relays.
ETH WAN	1	RJ-45 10/100 BASE-TX Ethernet port	• Data input • Data output • Status output • Control input	Supports local area network connectivity
				1 of 2

Table 11: Physical and logical interfaces on the G350 front panel *2 of 2*

Physical interface	Quantity	Description	FIPS 140-2 logical interface	Comments
ETH LAN	1	RJ-45 Ethernet LAN switch port	• Data input • Data output • Status output • Control input	Supports wide area network connectivity
CONSOLE	1	Console port for direct connection of CLI console. RJ-45 connector.	• Control inputs • Status output	Supports cryptographic module administration
USB	1	USB port. Supports the connection of the Multitech MultiModemUSB MT5634ZBA-USB-V92 USB modem.	N/A	
Media Module connectors (V1 to V6)	6	Slots for inserting optional Media Modules	• Data input • Data output • Status output • Control input	Provides the ability to communicate using Voice TDM, Serial/TDM Data, Ethernet, PCI, CPU Device Bus, and facilitates Power, PoE
				2 of 2

Table 12: Buttons on the G350 front panel

Button	Description
RST	Reset button. Resets chassis configuration.
ASB	Alternate Software Bank button. Reboots the G350 with the software image in the alternate bank.

Supported algorithms

The cryptographic module supports the following algorithms in FIPS mode:

Approved Algorithms:

- RSA digital signature verification during firmware upgrades, and license file authentication. Support for RSA defined in PKCS#1 standard. RSA implementation, as defined by ANSI X9.31, is not supported.
- Triple-DES CBC (three key) for IKE encryption and IPSec
- AES (128bit) CBC for IPSec and IKE encryption
- SHA-1 for hashing download image digest, license file digest
- HMAC SHA-1 for message authentication codes for IKE and IPSEC
- DES CBC for encryption of IPSec, and IKE (only supported for communication with legacy systems)
- TDES CBC Encryption of the serial number date for Voice feature activation controlled by the ICC CM server/external blade server

Non-Approved Algorithms:

- Diffie-Hellman for IKE key exchanges
- MD5 for Radius Client role and peer OSPF router authentication

The cryptographic module relies on the implemented deterministic random number generator (DRNG) that is compliant with X9.31 with 128-bit Key, 64bit Seed for generation of all cryptographic keys. The non-deterministic random seed generator is used for the periodic re-seeding of the PRNG.

The cryptographic module may be configured for FIPS mode via execution of the configuration procedure specified in Administration procedures on page 307.

The user can determine if the cryptographic module is running in FIPS vs. non-FIPS mode via:

- Execution of the **`show running-config`** command.
- Verification that the configuration meets the requirements specified in Administration procedures on page 307.
- Verification that the HW version and the firmware version of the module firmware code in banks A and B are FIPS-approved versions.

Non-FIPS mode of operation

In non-FIPS mode, the cryptographic module provides non-FIPS-approved algorithms and uses FIPS-approved algorithms in non-compliant ways, as shown in Table 13:

Table 13: Non-FIPS-approved operations and algorithms

	MD5	HMAC-SHA1	PTLS	TDES	DES	AES	AEA	DH
IKE	X							Group 1
IPSEC	X							
SNMPv3		X		X				
SSH2	X			X	X			Group 786-20 48 bit
VoIP Bearer (Media) Encryption						X	X	
Link Encryption			X			X		

Security level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1: Module security level specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Port and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Operational environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device does not support the loading and execution of un-trusted code. Avaya digitally signs firmware images of the crypto module using RSA SHA1 digital signature. Through this signature, the crypto module verifies the authenticity of any update to its firmware image.

Assumptions of roles

The cryptographic module supports eight distinct operator roles: Cryptographic-Officer, Read/Write User, Read-only User, RADIUS Server, OSPF Router Peer, PPPoE Client, IKE Peer, and Serial Number Peer.

The cryptographic module enforces the separation of roles using operator authentication. Refer to Table 14 for further information.

Table 14: Roles and required identification and authentication *1 of 2*

Role	Type of authentication	Authentication data	Description
Cryptographic-Officer (Admin User)	Identity-based operator authentication	Username and Password. The module stores user identity information internally through the use of an external Radius Server database.	The owner of the cryptographic module who has full access to the module's services
User (Read/Write User)	Identity-based operator authentication	Username and Password. The module stores user identity information internally through the use of an external Radius Server database.	An assistant to the Admin User who has read/write access to a subset of configuration and status indications
Read-only User	Identity-based operator authentication	Username and Password. The module stores user identity information internally through the use of an external Radius Server database.	An assistant to the Admin User who has read-only access to a subset of module configuration and status indications
RADIUS Server	Role-based operator authentication	Shared Radius secret. Gateway authenticates Radius server response by examining the MD5 hash of the shared secret, the request Authenticator, and other response values in a response message.	An entity authenticates to the module for the purpose of permitting/ denying access to services
OSPF Router Peer	Role-based operator authentication	Router peer Secret. Authentication of OSPF protocol executed by examining the authentication field in OSPF packet carrying MD5 hash of the packet and the secret.	An entity authenticates to the module for the purpose of permitting/ denying access to services
			1 of 2

Table 14: Roles and required identification and authentication *2 of 2*

Role	Type of authentication	Authentication data	Description
PPPoE Client	Role-based operator authentication	Chap/Pap Secrets. Simple password authentication is used for PAP-based authentication. Gateway uses MD5 function to hash the challenge and the secret value in the response message to PPPoE Server.	An entity that facilitates connection to the broadband access network using PPP over Ethernet protocol (PPPoE)
IKE Peer	Role-based operator authentication	IKE pre-shared keys	An entity that facilitates IPSec VPNs
Serial Number Peer	Role-based verification	TDES encrypted challenge	Gateway exchanges its serial number with a Server to enable feature activation
			2 of 2

Assumptions concerning user behavior

- Password length:
  - User password: at least eight characters
  - Other passwords: at least six characters
  - PSK (Pre-shared keys) for IKE: at least 13 characters

  SECURITY ALERT:
  The user should refer to Password guidelines on page 306.
- Lock-out after authentication fail after fixed number of log-in attempts (default value is three)
- Device management via direct link to Console port or via IPSec tunnels only
- Commands are documented in the *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

Critical security parameters and private keys

Table 15 describes the CSPs (Critical Security Parameters) defined in the module.

Table 15: Critical security parameters *1 of 3*

Key	Description/Usage	Storage
IKE Pre-shared Keys	This key generates IKE SKEYID_d during pre-sharedkey authentication. The first-time key must be entered manually (via RS232 connected to the PC acting as terminal emulation). Other keys can be defined remotely over encrypted and authenticated IPSEC tunnel.	
HASH_I, HASH_R	Used for generation of SKEYID, SKEYID_d, SKEYID_a, SKEYID_e. Generated for VPN IKE Phase 1 key establishment.	
IKE Pre-Shared Session Key (SKEYID)	Generated for VPN IKE Phase 1 by hashing pre-shared keys with responder/ receiver nonce	DRAM (plaintext)
IKE Ephemeral DH shared secret (g^ab)	Generated for VPN IKE Phase 1 key establishment	
IKE Ephemeral DH private key (a)	The private exponent used in DH exchange. Generated for VPN IKE Phase 1 key establishment.	
IKE Ephemeral DH private key (a)	The private exponent used in DH exchange. Generated for VPN IKE Phase 1 key establishment.	
IKE Session Phase 1 Secret (SKEYID_d)	Phase 1 key used to derive keying material for IPSec SAs	
IKE Session Phase 1 HMAC Key (SKEYID_a)	Key used for integrity and authentication of the ISAKMP SA	DRAM (plaintext)
IKE Session Phase 1 Encrypted Key (SKEYID_e)	Shared key used for extraction of encryption keys protecting the ISAKMP SA	
IKE Session Phase 1 TDES key (SKEYID_e)	Key used for TDES data encryption of ISAKMP SA	DRAM (plaintext)
		1 of 3

Table 15: Critical security parameters *2 of 3*

Key	Description/Usage	Storage
IKE Session Phase 1 DES key	Key used for DES data encryption of ISAKMP SA	
IKE Session Phase 1 AES key	Key used for AES data encryption of ISAKMP SA	
Noncie, Noncer	Phase 2 initiator and responder nonce	
IPSEC SA phase-2 TDES key	Phase 2, basic quick mode	
IPSEC SA phase-2 DES key	Phase 2, basic quick mode	
IPSEC SA phase-2 AES key	Phase 2, basic quick mode	
IPSEC SA phase-2, HMAC keys	Phase 2, basic quick mode	
IPSEC SA phase-2 keys per protocol	Phase 2, basic quick mode	
DH private key phase-2	Phase 2 Diffie Hellman private keys used in PFS for key renewal	
DH shared secret phase-2	Phase 2PFS Diffie Hellman shared secret used in PFS for key renewal	
IPSEC SA phase-2 keys per protocol	Phase 2, basic quick mode	
User password	Used for password authentication of CLI users	
Root password	Used for authentication of default CLI user during first setup	
Radius Secret	Used for hashing password with MD5. One secret common to both Primary and Secondary Radius server.	
PPPoE CHAP/PAP Secret	Used for authentication to PPPoE server	
OSPF Secret	Used for hashing password with MD5. One secret defined per peer router identity.	
SNMPv3 user authentication password	SNMPv3 operator MD5 authentication password used for authenticating to User and Read-Only User roles	
X9.31 PRNG key	Key for X9.31 PRNG	
		2 of 3

Table 15: Critical security parameters *3 of 3*

Key	Description/Usage	Storage
Fixed Serial Number secret	The TDES key used for the first exchange of the serial number and new session key between Gateway and S8300/Blade server entity	
Ephemeral Serial Number secret	The TDES key used for serial number and key renewal. This key is periodically re-negotiated between S8300/Blade server entity and the Gateway.	
		3 of 3

Public keys

Table 16 lists the public keys available in the module:

Table 16: Public keys

Key	Description/Usage
Ephemeral DH phase-1 public keys	Generated for VPN IKE Phase 1 key establishment
Ephemeral DH phase-2 public keys	Generated for VPN IKE Phase 2 PFS key renewal
Image download certificate (Avaya root CA RSA public key)	Used for authentication of software download. The Avaya Root certificate is hard-coded in the Gateway image and is used directly for authentication of the chain of trust of the Avaya Signing Authority that is downloaded together with the software.
License download public key	Used for authentication of license file validity. The license signing authority public key is hard-coded in the Gateway image and is used directly for authentication of the digital signature embedded in the license file.

CSP access rights within roles and services

Table 17 lists the CSP access rights according to role.

Table 17: CSP access rights within roles and services *1 of 2*

Service	Role							
	Crypto-Officer (Admin User)	Read-Write User	Read-0nly User	RADIUS Server	IKE Peer	OSPF Router Peer	PPPoE Client	Serial Number Peer
Enable FIPS mode: Configure the module for the Approved mode of operation	X							
Firmware update: Load firmware images digitally signed by RSA-SHA1 (1024 bit) algorithm	X							
CSPs management: IKE pre-shared keys, OSPF secrets, PPPoE secrets	X	X						
User Management: Add and delete Admin users, Read/Write Users, Read Only Users, Radius Servers	X							
Module configuration: Configure networking capabilities, including bypass capability	X	X						
Reset: Force the module to power cycle via a remote command	X	X						
Read all status indications: obtain all statuses securely via IPSEC, console port, and LEDs on the Gateway's front panel	X							
								1 of 2

Table 17: CSP access rights within roles and services *2 of 2*

Service	Role							
	Crypto-Officer (Admin User)	Read-Write User	Read-0nly User	RADIUS Server	IKE Peer	OSPF Router Peer	PPPoE Client	Serial Number Peer
Read subset of status indications: obtain subset of statuses securely via IPSEC, console port and LEDs on the Gateway's front panel	X	X	X					
Module configuration backup: backup non-CSP related configuration data via IPSEC	X	X						
Module configuration restore: restore configuration data	X							
Zeroization: actively destroy all plaintext CSPs and keys	X							
IKE negotiation uses DH, TDES, HMAC-SHA1, PRNG X9.31	X	X	X		X			
IPSec traffic processing uses AES, TDES, HMAC-SHA1	X	X	X		X			
Serial Number Exchange								X
OSPF Routing						X		
PPPoE connection							X	
RADIUS authentication				X				
								2 of 2

Table 18 shows Role and Service Access to CSPs:

- R – Read: the data item is read into memory.
- W – Write: the data item is written into memory.
- Z – Zeroize: the data item is actively destroyed.

Table 18: Role and service access to CSPs *1 of 3*

Key	Enable FIPS Mode	Firmware Update	CSPs Management	User Management	Module Configuration	Reset	Read all status indications	Module backup	Restore	Zeroization	IKE Negotiation	IPSec traffic processing	Read subset of status indications	OSPF Routing	PPPoE Service	RADIUS Authentication	Serial Number Exchange
PRNG Keys	RW Z					ZW				Z	R						
IKE Preshared Keys	RW Z		W		Z					Z	R						
Pre-shared Session Key (SKEYID)						Z				Z	RW						
Ephemeral DH private key						Z				Z	RW						
Ephemeral DH shared secret						Z				Z	RW						
HASH_I, HASH_R						Z				Z	RW						
IKE Session phase 1 secret (SKEYID_d)						Z				Z	RW						
IKE phase 1 HMAC Key (SKEYID_a)						Z				Z	RW						
IKE Session phase 1 key (SKEYID_e)						Z				Z	RW						
IKE Session phase 1 TDES						Z				Z	RW						
IKE Session phase 1 DES						Z				Z	RW						
IKE Session phase 1 AES						Z				Z	RW						

1 of 3

Table 18: Role and service access to CSPs *2 of 3*

Key	Enable FIPS Mode	Firmware Update	CSPs Management	User Management	Module Configuration	Reset	Read all status indications	Module backup	Restore	Zeroization	IKE Negotiation	IPSec traffic processing	Read subset of status indications	OSPF Routing	PPPoE Service	RADIUS Authentication	Serial Number Exchange
IKE Phase 1 TDES key (SKEYID-e)						Z				Z	RW						
Nonce						Z				Z	W	R					
IPSEC SA phase-2 TDES key						Z				Z	W	R					
IPSEC SA phase-2 AES key	WZ					Z				Z	W	R					
IPSEC SA phased-2 HMAC keys						Z				Z	W	R					
IPSEC SA phase-2 keys per protocol						Z				Z	RW						
Ephemeral DH phase 2 private key						Z				Z	RW						
DH phase 2 shared secret						Z				Z	RW						
User password	WZ	R	R	WZ	R	R	R	R	R	Z			R				
Root password	RW	RW	R	W	R	R	R	R	R	W			R				
OSPF Secret	WZ		WZ		Z					Z				R			
RADIUS Secret	WZ		WZ							Z						R	
PPPoE Chap/ PAP Secret	WZ		W		Z					Z					R		
SNMPv3 authentication password	WZ	R	R	WZ	R	R	R	R	R	Z							
Fixed Serial Number secret		W								Z							R

2 of 3

Table 18: Role and service access to CSPs *3 of 3*

Key	Enable FIPS Mode	Firmware Update	CSPs Management	User Management	Module Configuration	Reset	Read all status indications	Module backup	Restore	Zeroization	IKE Negotiation	IPSec traffic processing	Read subset of status indications	OSPF Routing	PPPoE Service	RADIUS Authentication	Serial Number Exchange
Ephemeral Serial Number secret						Z				Z							
IKE Ephemeral DH public keys						Z				Z	RW						
IKE Ephemeral DH phase 2 public keys						Z				Z	RW						
Avaya root CA RSA public key		RW															
License RSA public key	R	RW															

3 of 3

Security rules

The following are security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. Set the crypto module to FIPS-140-2 mode through the procedure outlined in Entering FIPS mode on page 307.
2. When exiting FIPS-140-2 mode, the crypto-officer should zeroize the CSP.
3. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
4. It is recommended to only encrypt message traffic using DES to support communication with legacy systems.

5. The cryptographic module performs the following tests:
   - Power up Self-Tests:

     Cryptographic algorithm tests:

     - TDES Known Answer Test (tests DES performance as well)
     - AES Known Answer Test
     - SHA-1 Known Answer Test
     - HMAC-SHA-1 Known Answer Test
     - DRNG Known Answer Test
     - RSA Known Answer Test

   Note:

   FIPS 140-2 does not require execution of the Diffie-Hellman Known Answer self-test. A letter of conformance to the corresponding standard will be provided to NIST instead.

   Gateway Software Integrity Test (32 bit CRC verification) and Booter Integrity Test (32 bit CRC verification)

   Critical Functions Tests:

   - NVRAM Integrity test
   - EEPROM Integrity Test

   - Conditional Self-Tests:
     - Continuous Random Number Generator (RNG) test - performed on all RNGs involved in crypto activities in FIPS-approved mode. Performed for PRNG x9.31 and Random Seed Generator.
     - Bypass Test
     - Firmware load test
6. You can instruct the module to perform the power-up self-tests via power cycle.
7. Prior to each use, the internal RNG is tested using the conditional test specified in FIPS 140-2 §4.9.2.
8. Data output is inhibited during key generation, self-tests, zeroization, and error states.
9. The module supports concurrent operators and maintains separation of roles and services.
10. Users can plug-in and use any Avaya Media Module that does not support cryptographic functionality without restriction.
11. Media modules with cryptographic functionality must be evaluated separately against the FIPS 140-2 requirements.

Password guidelines

Below are general guidelines for defining passwords. To maximize security, it is recommended to follow these guidelines or use company guidelines where available.

- Password length
  - User password: at least **eight** characters
  - Other passwords: at least **six** characters
  - PSK (pre-shared keys) for IKE: at least **13** characters
- Use a combination of upper and lower case letters, numbers and symbols.

  Note:

  You may use any printable character, such as ?, ! or *
- Do not use passwords that are easy to guess, such as names, dates, or telephone numbers.
- Keep passwords in a safe place.

Managing the module in FIPS-compliant mode

In FIPS-approved operation mode, all remote configuration activities (Telnet/TFTP/SNMP/FTP) are channeled through a VPN tunnel. The console port is used for local administration. Management through all other interfaces is disabled. In addition, the module will:

- Disable Administration over SSH protocol.
- Disable dial-in via the modem ports (serial and USB).
- Restrict troubleshooting services in the production environment by blocking all non-FIPS compliant dev/tech commands, such as tShell.
- Disable loading and output of configuration files from/to the SCP server.
- Allow loading and output of configuration files from/to the TFTP/FTP server only over a VPN-encrypted tunnel.

SECURITY ALERT:

The “FIPS mode” of operation is permanent. If you do not fulfill all of the steps, you void Gateway FIPS-compliant operation. The same happens if, after entering FIPS mode, you execute an operation that is not consistent with the FIPS-approved mode of operation. Also note that execution of the **`NVRAM Init`** or **`zeroize`** commands clear the above defined FIPS-approved mode configuration and returns the box to factory defaults.

Prerequisites

- Avaya Communication Manager 2.2
- FIPS-ready gateway.
  - Check that the Material Code is 700356249.
  - Use the **`show system`** command and verify that “FIPS ready” is displayed.

```
G350-N(super)# show system
HW Ready for FIPS: yes
```

Administration procedures

Entering FIPS mode

Prerequisites

- User type – crypto officer
- FIPS-approved hardware. Version 3.0.x or higher.
- FIPS-approved G350 firmware. Version 23.12.50 or higher (in both image banks).
- Valid VPN license

To enter FIPS mode:

1. Log in to the device through the local console port.
   - User name: root
   - Password: root

   Note:

   Use the password “root” when the G350 is running with the factory default configuration.

```
Login: root
Password: ****

Password accepted
G350-N(super)#
```

2. Define the PMI (Primary Management Interface) interface.
   - Use the **`interface`** command.

```
G350-N(super)# interface vlan 1
G350-N(super)# icc-vlan
G350-N(super)# ip address 100.100.100.1 255.255.255.0
G350-N(super)# pmi
G350-N(super)# exit
```

3. Reset the device to activate the PMI.
   - Use the **`reset`** command.

```
G350-N(super)# reset
This command will reset the device
*** Reset the device *** - do you want to continue (Y/N)? y

Resetting the device...
GW-A-001(super)#
```

4. Verify that the hardware version of the G350 is a FIPS-approved version:
   a. Use the **`show system`** command.
   b. Check that the following is displayed:

```
G350-N(super)# show system
HW ready for FIPS: Yes
```

5. Verify that both firmware banks contain firmware images that have been FIPS-approved.

   a. Use the **`dir`** command.

```
G350-N(super)# dir
M# file              ver num   file type    file location  file description
-- ----              --------  ----------   -------------  ----------------
1  Voice (Initializing) N/A    SW RT Image  Nv-Ram         Voice (Initializing) -
image
7  Voice (Initializing) N/A    SW RT Image  Nv-Ram         Voice (Initializing) -
image
7  Analog            57        SW RT Image  Nv-Ram         Analog - image
10 startup-config    N/A       Startup Conf Nv-Ram         Startup Config
10 running-config    N/A       Running Conf Ram            Running Config
10 G350-A            3.0.x     SW RT Image  Flash Bank A   Software Image Bank A
10 G350-B            3.0.x     SW Component Flash Bank B   Software Image Bank B
10 G350              1.0.19    SW Web Image Nv-Ram         EmWeb application
10 G350-Booter       3.5.0     SW BootImage Nv-Ram         Booter Image
10 sniffer           N/A       Other        Ram            Sniffer Capture
10 phone-ScriptA     N/A       Phone Script Nv-Ram         N/A
10 phone-ScriptB     N/A       Phone Script Nv-Ram         N/A
10 phone-ImageA      N/A       Phone Image  Ram            N/A
10 phone-ImageB      N/A       Phone Image  Ram            N/A
10 phone-ImageC      N/A       Phone Image  Ram            N/A
10 phone-ImageD      N/A       Phone Image  Ram            N/A
10 dhcp-binding      N/A       DHCP Binding Nv-Ram         Ip Address Binding
```

   b. Check that the value in the “ver num” column for each bank (G350-A and G350-B) is 23.12.50 or higher.

6. Verify successful completion of power-up self-tests.

   - Use the **`show self-test-status`** command.

```
G350-N(super)# show self-test-status
Device successfully passed the power-up self test sequence.
```

7. If a more recent FIPS-approved G350 image is available, download it using the image download procedures.

   - Use the **`copy tftp image`** command.

8. Download the Avaya License file with VPN feature activated if it is not installed.

   - Use the **`copy tftp-license-file`** command.

9. Reset the gateway.

   - Use the **`reset`** command.

```
G350-N(super)# reset
This command will reset the device
*** Reset the device *** - do you want to continue (Y/N)? y

Resetting the device...
GW-A-001(super)#
```

10. Physically disconnect all network interfaces.
    - This ensures that no external activity interferes with the following steps.
11. Disable Signaling Encryption (H.248).
    - Use the **`disable link encryption`** command.

```
G350-N(super)# disable link encryption
```

Note:

You must administer the G350 in CM with the encrypted link *off.* Otherwise, after disabling encryption in the G350, you cannot establish a signaling link later.

12. Disable Avaya Media Encryption (SRTP, AEA, RTP/AES).
    - Use the **`disable media encryption`** command.

```
G350-N(super)# disable media encryption
```

13. Disable the USB and Console modem interfaces

    a. To disable the Console interface, use the **`async mode terminal`** command.

```
G350-N(super)# interface Console
G350-N(super-if:Console)# async mode terminal
Done!
G350-N(super-if:Console)# exit
```

    b. To disable the USB interface, use the **`shutdown`** command.

```
G350-N(super)#interface USB-Modem
G350-N(super-if:USB-Modem)# shutdown
This command will disconnect your current dial-in modem session and block
future  dial-in attempts over this modem interface - do you want to
continue (Y/N)? Y
Done!
G350-N(super-if:USB-Modem)# exit
```

14. To disable the recovery password mechanism, use the **`set terminal recovery password disable`** command.

```
G350-N(super)#set terminal password recovery disable
Done!
```

15. To disable the SSH service, use the **`no ip ssh`** command.

```
G350-001(super)# no ip ssh
This will prevent future remote SSH sessions and disconnect all active SSH
sessions - do you want to continue (Y/N)? y

Shutting down all active sesssions
Done!
```

16. Configure other module parameters:
    - VoIP
    - Media
    - L2 switching
    - E1/T1

    For example:

```
G350-N(super)# hostname "G350"
G350-N(super)# set spantree disable
G350-N(super)# set mgc list 149.49.70.86
G350-N(super)# set mediaserver 149.49.70.86 149.49.70.86 23 telnet
G350-N(super)# set mediaserver 149.49.70.86 149.49.70.86 5023 sat
G350-N(super)# controller t1 2/1
G350-N(super)# linecode b8zs
G350-N(super)# framing esf
G350-N(super)# clock source internal
G350-N(super)# cablelength short 133ft
G350-N(super)# channel-group 1 timeslots 1-20 speed 64
G350-N(super)# exit
```

17. Determine which interfaces will be used for clear-text data, and which for encrypted data.

18. To configure all interfaces, including the IP addresses, use the **`interface`** command. For example:

```
G350-N(super)# interface FastEthernet 10/2
G350-N(if:fastEthernet 10/2)# ip crypto-group 901
Done!
G350-N(if:fastEthernet 10/2)# mtu 1492
Done!
G350-N(if:fastEthernet 10/2)# ip address 10.0.0.1 255.255.255.0
G350-N(if:fastEthernet 10/2)# exit
G350-N(super)#

G350-N(super)# interface Tunnel 1

Line protocol on Interface Tunnel 1, changed state to down
G350-001(super-if:Tunnel 1)#
G350-N(if:Tunnel 1)# tunnel source 10.0.0.1
Done!
G350-N(if:Tunnel 1)# tunnel destination 10.0.0.2
Done!
G350-N(if:Tunnel 1)# ip address 10.20.0.1 255.255.255.252
Done!
G350-N(if:Tunnel 1)# exit
G350-N(super)#

G350-N(super)# interface Serial 2/1:1
G350-N(if: serial 2/1)# encapsulation ppp
Done!
G350-N(if: serial 2/1)# ip address 1.0.0.1 255.255.255.252
G350-N(if: serial 2/1)# exit
G350-N(super)#
```

19. To change the password of the default Crypto-officer
    - Use the **`username`** command to change the root user password to comply with the minimum secret length requirements.

```
G350-001(super)# username root password westminster access-type admin
User account modified.
G350-001(super)#
```

20. Define additional operators for Crypto-officer, User, and Read-Only User roles, as required.
21. Remove all unnecessary users.
    - Use the **`show username`** command to list CLI users.

```
G350-N(super)# show username
User                              Access       Account     Active  Authent.
account                           level        type                method
--------------------------------  -----------  ----------  ------  ----------
root                              admin        local       yes     password
```

- Use the **show snmp user** command to list SNMPv3 users.

```
G350-N(super)# show snmp user
EngineId: 80:00:1a:e9:03:00:04:0d:29:ca:61   (local)
User Name: initial
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonVolatile
Row Status: active
```

- Use the **no username** command to delete CLI users.
- Use the **no snmp-server user** command to delete local SNMP users.

```
G350-N(super)# no snmp-server community
Done!
G350-N(super)# no snmp-server user initial v3
Done!
```

- Use the **no snmp-server remote-user** command to delete remote SNMP users.

```
G350-N(super)# no snmp-server remote-user
Done!
```

22. Define new CLI and SNMPv3 secrets for existing users.
    - Use the **username** command to define new CLI users.

```
G350-N(super)# Username root password root_fips access-type admin
User account modified.
G350-N(super)# username admin password admin_password access-type admin
User account modified
G350-N(super)# username readwrite password rw_password access-type
read-write
User account modified
G350-N(super)# username readonly password ro_password access-type
read-only
User account modified

G350-N(super)# show username
User                              Access       Account     Active  Authent.
account                           level        type                 method
--------------------------------  -----------  ----------  ------  ----------
root                              admin        local       yes     password
admin                             admin        local       yes     password
readwrite                         read-write   local       yes     password
readonly                          read-only    local       yes     password
```

- Use the **`snmp-server user user group auth md5 secret`** command to define new SNMPv3 users or change an existing snmpv3 user authentication password. For example:

```
G350-N(super)# snmp-server remote-user john 00:02:00:81:00:d0:00:4c:18:00
L2Group auth md5 katmandu
```

- Use the **`snmp-server remote user user group auth md5 secret`** command to define new SNMPv3 users or change an existing snmpv3 user authentication password.

```
G350-N(super)# snmp-server user user group auth md5
G350-N(super)# snmp-server engineID 00:04:0d:29:c5:a5
G350-N(super)# snmp-server group initial v3 auth read iso write iso notify
iso
```

23. Remove unnecessary OSPF peers.
    - Use the **`show ip ospf interfaces`** to list all interfaces with OSPF activated.
    - Use the **`no ip ospf message-digest-key`** command to delete an OSPF MD5 key in context of an interface.
24. Configure primary and secondary RADIUS servers (primary/secondary).

```
G350-N(super)# Set radius authentication enable
G350-N(super)# set radius authentication server 200.200.200.20 primary
G350-N(super)# set radius authentication secret fips_test1
G350-N(if:Tunnel 1)# interface tunnel 1
G350-N(if:Tunnel 1)# ip ospf authentication message-digest
G350-N(if:Tunnel 1)# ip ospf message-digest 1 md5 ospf_key1
exit
```

25. Configure the OSPF router peers.

    SECURITY ALERT:
    The OSPF secrets size must be at least six characters, are case sensitive, and accept all printable characters (e.g., question mark, exclamation point, asterisk).

    - Use the **`ip ospf message-digest-key`** command to define a new message key value.

```
G350-N(super)# router ospf
G350-N(router:ospf)# redistribute connected
G350-N(router:ospf)# network 10.20.0.0 0.0.0.3 area 0.0.0.0
exit
```

26. Configure PPPoE peers.

```
G350-N(super)# interface FastEthernet 10/2
G350-N(if:fastEthernet 10/2)# encapsulation  pppoe
G350-N(if:fastEthernet 10/2)# ppp chap hostname "chap_user"
G350-N(if:fastEthernet 10/2)# ppp chap password "chap_password"
G350-N(if:fastEthernet 10/2)# ppp pap sent-username pap_user password
pap_password
exit
```

SECURITY ALERT:
The PPPoE secrets size must be at least six characters, are case sensitive, and accept all printable characters (e.g., question mark, exclamation point, asterisk).

- Use the **`ppp chap password`** command to define a new CHAP secret for PPPoE.

```
G350-N(super-if:console)# ppp chap password mysecret
```

27. Assign a new secret to the RADIUS servers.

SECURITY ALERT:
The RADIUS secrets size must be at least six characters, are case sensitive, and accept all printable characters (e.g., question mark, exclamation point, asterisk).

Use the **`set radius authentication secret`** command to define the RADIUS secret.

```
G350-N(super)# set radius authentication secret hush
```

28. Disable the following management protocols on the internal emb-vlan interface and inhibit output traffic during powerup/error states:
    - TELNET
    - FTP
    - TFTP
    - SNMP

    Use the **`enhanced security`** command.

```
G350-001(super)# enhanced security
Done!
```

29. Define an Access Control list that blocks packets with an IP destination address of any of the G350 interfaces for the following protocols:
    - TELNET
    - FTP

- TFTP
- SNMP

Example:

```
G350-001(super)# ip access-control-list 301
G350-001(super-ACL 301)#
G350-001(super-ACL 301)# ip-rule 15
G350-001(super-ACL 301/ip rule 15)#
G350-001(super-ACL 301/ip rule 15)# composite-operation "Deny"
Done!
G350-001(super-ACL 301/ip rule 15)# ip-protocol tcp
Done!
G350-001(super-ACL 301/ip rule 15)# destination-ip host 10.3.0.3
Done!
G350-001(super-ACL 301/ip rule 15)# tcp source-port eq Telnet
Done!
G350-001(super-ACL 301/ip rule 15)# tcp destination-port eq Telnet
Done!
G350-001(super-ACL 301/ip rule 15)# exit
G350-001(super-ACL 301)# exit
G350-001(super)#
```

30. Activate the ACL on the inbound direction of all clear-text interfaces.
    - Use the **`ip access-group`** command.

```
G350-N(if:clear-text)# ip access-group 310 in
```

31. Configure packet forwarding:
    - static routes. Use the **`ip route`** command.

```
G350-N(super)# ip route 200.200.200.0 24 10.0.0.2 low
G350-N(super)# ip route 149.49.70.0 24 10.0.0.2 low
```

    - dynamic routes learned via RIP and/or OSPF
    - policy based routing lists
32. Configure IKE:
    - Diffie-Hellman group 2 only (1024bits)
    - HMAC-SHA-1
    - 3DES (or DES for interconnection with legacy systems)
      - Use the **`crypto isakmp policy`** command.

```
G350-001(super)# crypto isakmp policy 1
G350-001(super-isakmp:1)#
```

33. Remove unnecessary VPN peers.
    - Use the **`show crypto isakmp key`** command to list all defined pre-shared keys.
    - Use the **`no crypto isakmp key`** command to delete unnecessary VPN peers.
34. Configure VPN peers (pre-shared keys).
    - Use the **`crypto isakmp key`** command to define new VPN peers or assign a new pre-shared key to existing peers.

```
G350-N(super)# crypto isakmp policy  1
G350-N(isakmp-1)# encryption des
G350-N(isakmp-1)# hash sha
G350-N(isakmp-1)# group 2
exit
crypto isakmp key preshared_key1 address 10.0.0.2 isakmp-policy 1
crypto isakmp key preshared_key2 address 1.0.0.2 isakmp-policy 1
```

35. Configure IPSec transfer-sets:
    - HMAC-SHA-1
    - AES
    - 3DES (or DES for interconnection with legacy systems)

    Use the **`crypto ipsec transform-set`** command.

```
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
exit
crypto map 1
G350-N(super)# set transform-set ts1
G350-N(crypto-map)# set peer 10.0.0.2
Done!
G350-N(crypto-map)# exit
G350-N(super)# crypto map 2
G350-N(crypto-map)# set transform-set ts1
G350-N(crypto-map)# set peer 1.0.0.2
Done!
G350-N(crypto-map)# exit
```

36. Define one or more IPSec Crypto lists that provide encryption rules for traffic that needs protection. Make sure that packets with IP source address of any of the G350 interfaces for the following protocols are always encrypted:
    - TELNET
    - FTP
    - TFTP
    - SNMP

    Use the **`ip crypto-list list-id`** command.

```
G350-N(super)# ip crypto-list 901
G350-N(crypto-list-901)# local-address 10.0.0.1
Done!
G350-N(crypto-list-901)# ip-rule 10
Done!
G350-N(crypto-list-901)# protect crypto map 1
Done!
G350-N(crypto-list-901)# source-ip any
Donw!
G350-N(crypto-list-901)# destination-ip any
Done!
exit
exit
G350-N(super)# ip crypto-list 902
G350-N(crypto-list-902)# local-address 1.0.0.1
Done!
G350-N(crypto-list-902)# ip-rule 10
Done!
G350-N(crypto-list-902)# protect crypto map 2
Done!
G350-N(crypto-list-902)# source-ip any
Done!
G350-N(crypto-list-902)# destination-ip any
Done!
exit
```

Note:

TELNET, FTP, TFTP, and SNMP are always ESP with TDES- or AES- encrypted. Null encryption or AH are NOT allowed for such flows.

37. Activate the crypto-lists on the inbound direction of all cipher-text interfaces. For flows that need to be encrypted even if directed to clear-text interfaces, apply crypto lists to all interfaces.

    - Use the **`ip crypto-list list-id`** command in the interface context.

```
G350-N(super)# interface serial 2/1:1
G350-N(if: serial 2/1)# ip crypto-group 902
Done!
G350-N(if: serial 2/1)# exit

G350-N(super)# interface FastEthernet 10/2
G350-N(if:fastEthernet 10/2)# ip crypto-group 901
Done!
G350-N(if:fastEthernet 10/2)# exit
```

38. Save the running config to the startup config.

    - Use the **`copy running-config startup-config`** command *twice* to ensure that configuration primary and backup both are being updated with approved mode configuration.

39. Re-connect network interfaces.

Failure scenarios and repair actions

The G350 initiates power up tests automatically, without the need for operator intervention, and executes tests in the order defined below.

The power-up self-tests are executed during the early boot sequence and before the G350's data output interfaces are enabled and begin transmitting packets.

The power-up self-test order is:

1. Booter Integrity Self test
2. Image Integrity Self test
3. NVRAM Self test
4. PRNG Self-test
5. Crypto Self-tests
6. EEPROM Self-test

The power-up self test progress is output to the Gateway console port.

For each self-test listed, the process that dispatches the self-test execution outputs the name of the test performed and, on completion of the test, the process outputs results – passed or failed.

```
"Booter Integrity power-up self test "Passed"
"Image Banks Integrity power-up self test"   "Failed"
"NVRAM integrity power-up self test" "Passed"
"PRNG integrity power-up self test" "Passed"
"Crypto integrity power-up self test" "Passed"
"EEPROM integrity power-up self test" "Passed"
```

If the G350 fails a conditional or power-up self-test, the module enters the error state. All data output interfaces are immediately blocked.

Error states

Table 19 describes the four error states and the recovery procedure taken by the G350.

Table 19: Error States

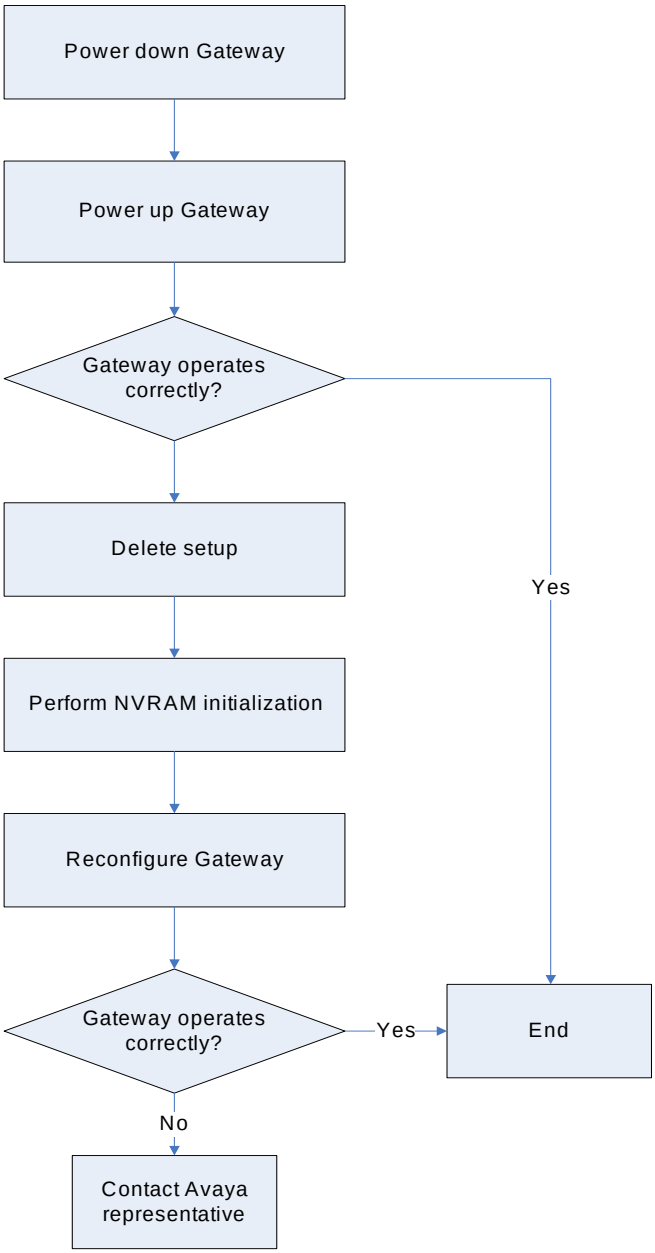
Error State	Cause	Automatic Recovery Procedure
1	Image integrated self-test failure	• Display Error state information that describes the failed self-test. • Run Power-up self-tests and if OK continue normally. • Do key zeroization.
	PRNG non-answer	
	Crypto non-answer	
	EEPROM non-answer	
2	Run-time	• Reset. • Automatically attempt return back to normal operation.
	Conditional PRNG stack	
	Bypass table corruption	
	Image download digital signature validation failure	
3	Booter integrated self-test	• Gateway immediately resets itself. • Gateway reruns the self-tests.
4	NVRAM integrated self-test failure	

Recovering from an error state

In order to recover from Error States 1, 2 and 4, follow the procedure shown in Figure 27:

SECURITY ALERT:
If the G350 does not recover from Error State 3, the secrets and other definitions are retained. If this information is highly sensitive, you should not send the G350 for repair.

Figure 27: Recovering from an error state



Considerations

The following rules apply in FIPS-approved mode:

- SSHv2 service must be shut down
- Media encryption must be shut down
- H.248 signalling must be shut down
- The Announcement FTP server shall not be used for upload/download G350 executable files or for file transfer of security related data
- ASG services logon must be shut down
- ASG BP login must be shut down
- SNMPv3 authentication and encryption services must be shut down
- Modem connections to the Console and USB ports must be shut down
- CHAP authentication services must be shut down
- Telnet service must be confined to IPSEC encrypted tunnel
- SNMP service must be confined to IPSEC encrypted tunnel
- TFTP/FTP configuration upload/download service must be confined to IPSEC encrypted tunnel
- FTP configuration upload/download service must be confined to IPSEC encrypted tunnel
- SCP client service must be shut down
- Usage of Diffie-Hellman Group 1 for IKE key negotiation must be suppressed
- Usage of MD5 for IKE must be suppressed
- Usage of MD5 for ESP authentication operation in IPSEC must be suppressed
- Mode change of bypass tables using SNMP MIB interface must be suppressed
- Configuration channel between ICC/LSP (S8300) and Gateway (MGP) must be suppressed

Appendix A: Traps and MIBs

This appendix contains the following sections:

- G350 traps — a list of all G350 traps.
- G350 MIBs — a list of all G350 MIBs.

G350 traps

The following table provides a list of all G350 traps with important information about each trap:

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, ifAdminStatus, ifOperStatus	STD	System	Warning	LinkUp	Agent Interface Up (linkUp Trap) enterprise:$E ($e) on interface $1	A linkUp trap indicates that the entity sending the protocol recognizes that one of the communication links represented in the agent's configuration has come up. The data passed with the event is 1) The name and value of the ifIndex instance for the affected interface. The name of the interface can be retrieved via an snmpget of.1.3.6.1.2.1.2.2.1.2.INST, where INST is the instance returned with the trap.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
linkDown	ifIndex, ifAdminStatus, ifOperStatus	STD	System	Warning	linkDown	Agent Interface Down (linkDown Trap) enterprise:$E ($e) on interface $1	A linkDown trap indicates that the entity that is sending the protocol recognizes a failure in one of the communication links represented in the agent's configuration. The data passed with the event is 1) The name and value of the ifIndex instance for the affected interface. The name of the interface can be retrieved via an snmpget of.1.3.6.1.2.1.2.2.1.2.INST, where INST is the instance returned with the trap.
SNMP_Authen_Failure		P330	SECURITY	Notification	authentic Failure	Incorrect Community Name (authentication Failure Trap) enterprise:$E ($e) args($#):$*	An authentication failure trap indicates that the protocol is not properly authenticated.
risingAlarm	alarmIndex, alarmVariable, alarmSample Type, alarmValue, alarmRising Threshold	RMON	THRES HOLD	Warning	rising Alarm	Rising Alarm: $2 exceeded threshold $5; value = $4. (Sample type = $3; alarm index = $1)	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps
fallingAlarm	alarmIndex, alarmVariable, alarmSample Type, alarmValue, alarmRising Threshold, alarmFalling Threshold	RMON	THRES HOLD	Warning	falling Alarm	Falling Alarm: $2 fell below threshold $5; value = $4. (Sample type = $3; alarm index = $1)	The SNMP trap that is generated when an alarm 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	deleteSWRedu ndancyTrap	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.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
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 enabled/disabled by chLntAgConfigChangeTraps.
lseIntPortCAMLastChange Trap	lseIntPortCAMLastChange	P330	SWITCH FABRIC	Info	lseIntPort CAMLast Change Trap	CAM Change at $1	This trap reports of the occurred configuration changes. It is enabled/ disabled by chLntAgCAMChangeTraps.
duplicateIP Trap	ipNetToMediaPhysAddress, ipNetToMediaNetAddress	P330	ROUTER	Warning	duplicateIPTrap	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 ChangeEvent	ipPolicy Activation EntID, ipPolicy ActivationList, ipPolicy Activationif Index, ipPolicy ActivationSub Context	P330	POLICY	Info	IntPolicyChangeEvent	Module $1 - Active policy list changed to $2	The trap reports a change in the active list specific for a policy-enabled box or module.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
IntPolicy AccessControlViolationFlt	ipPolicy AccessControl ViolationEnt ID, ipPolicy AccessControlViolationSrc Addr, ipPolicy AccessControl ViolationDst Addr, ipPolicy AccessControl Violation Protocol, ipPolicy AccessControl Violation L4SrcPort, ipPolicy AccessControl ViolationL4DstPort, ipPolicy AccessControlViolation Established, ipPolicyRuleID, ipPolicyRule ListID, ipPolicy AccessControlViolationIf Index, ipPolicy AccessControl ViolationSub Ctxt, ipPolicy AccessControl ViolationTime	P330	POLICY	Warning	IntPolicy Access Control ViolationFlt	IP PolicyAccess Control violation, if-index$9 ip-protocol=$4 src-ip=$2 dst-ip=$3 src-port=$5 dst-port=$6 rule-id=$8 rule-list=$$9	This trap reports to the Management station on IP PolicyAccess Control violation. The trap includes in its varbind information about the slot where the event occurred. The id of the rule that was violated in the current rules table, and the quintuplet that identifies the faulty packet. A management application would display this trap and the relevant information in a log entry. This trap will not be sent at intervals smaller than one minute for identical information in the varbinds list variables.
DormantPort Fault	genPortSWRdFault, genPortGroup Id, genPortId	P330	SWITCH FABRIC	Warning	Dormant PortFault	Dormant Port Connection Lost on Module $2 Port $3;	This trap reports the loss of connection on a dormant port.
DormantPort Ok	genPortSWRdFault, genPortGroup Id, genPortId	P330	SWITCH FABRIC	Notification	Dormant PortOk	Dormant Port Connection Returned to Normal on Module $2 Port $3;	This trap reports the return of connection on a dormant port.
InlinePwrFlt	genGroup FaultMask, genGroupId, genGroup BUPSActivity Status	P330	POE	Error	InlinePwr Flt	Module $2 Inline Power Supply failure	This trap reports the failure of an inline power supply.
InlinePwrFltOK	genGroup FaultMask, genGroupId, genGroup BUPSActivity Status	P330	POE	Notification	InlinePwr FltOK	Module $2 Inline Power Supply failure was cleared	This trap reports the correction of a failure on an inline power supply.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
WanPhysical AlarmOn	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1Line Status	WAN	WAN	Critical	Wan Physical AlarmOn	Cable Problem on port $4	An E1/T1/Serial cable was disconnected.
wanPhysical AlarmOff	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1Line Status	WAN	WAN	Notification	wan Physical AlarmOff	Cable Problem on port $4 was cleared	An E1/T1/Serial cable was reconnected.
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.
wanMinorAlarm Off	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1Line Status	WAN	WAN	Notification	wanMinor AlarmOff	Minor Alarm on interface $4 was cleared	Normal BER.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
AvEntFanFlt	entPhysical Index, entPhysical Descr, entPhySensorValue, avEntPhy SensorLo Warning	AVAYA-E NTITY	TEMP		AvEntFan Flt	Fan $2 is Faulty	This trap reports a faulty fan.
AvEntFanOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorLo Warning	AVAYA-E NTITY	TEMP	Notification	AvEntFanOk	Fan $2 is OK	This trap reports the return to function of a faulty fan.
avEnt48vPwr Flt	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY		avEnt48v PwrFlt	48V power supply Fault	This trap reports a problem with a 48V power supply.
avEnt5vPwrFlt	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY		avEnt5v PwrFlt	5V power supply Fault	This trap reports a problem with a 5V power supply.
avEnt3300mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY		avEnt3300mv PwrFlt	3.3V (3300mv) power supply Fault	This trap reports a problem with a 3.3V power supply.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
avEnt2500mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY		avEnt2500mv PwrFlt	2.5V (2500mv) power supply Fault	This trap reports a problem with a 2.5V power supply.
avEnt1800mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY		avEnt1800mv PwrFlt	1.8V (1800mv) power supply Fault	This trap reports a problem with a 1.8V power supply.
avEnt1600mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY		avEnt1600mv PwrFlt	1.6V (1600mv) power supply Fault	This trap reports a problem with a 1.6V power supply.
avEnt48vPwr FltOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY	Notification	avEnt48v PwrFltOk	48V power supply Fault Cleared	This trap reports the correction of a problem with a 48V power supply.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
avEnt5vPwrFltOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY	Notification	avEnt5v PwrFltOk	5V power supply Fault Cleared	This trap reports the correction of a problem with a 5V power supply.
avEnt3300mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY	Notification	avEnt3300mv PwrFlt Ok	3.3V (3300mv) power supply Fault Cleared	This trap reports the correction of a problem with a 3.3V power supply.
avEnt2500mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY	Notification	avEnt2500mvP wrFlt Ok	2.5V (2500mv) power supply Fault Cleared	This trap reports the correction of a problem with a 2.5V power supply.
avEnt1800mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY	Notification	avEnt1800mvP wrFlt Ok	1.8V (1800mv) power supply Fault Cleared	This trap reports the correction of a problem with a 1.8V power supply.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
avEnt1600mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelPos	AVAYA-E NTITY	SUPPLY	Notification	avEnt1600mv PwrFlt Ok	1.6V (1600mv) power supply Fault Cleared	This trap reports the correction of a problem with a 1.6V power supply.
avEntAmbient TempFlt	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, entPhysical ParentRelPos	AVAYA-E NTITY	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.
avEntAmbient TempOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhy SensorHi Warning, entPhysical ParentRelPos	AVAYA-ENTITY	TEMP	Notification	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.

9 of 9

G350 MIBs

The following table provides a list of the MIB files and their associated modules that are supported by the G350:

MIB File	MIB Module
Load.MIB	LOAD-MIB
RFC1315-MIB.my	RFC1315-MIB
Q-BRIDGE-MIB.my	Q-BRIDGE-MIB
ENTITY-MIB.my	ENTITY-MIB

1 of 3

MIB File	MIB Module
IP-FORWARD-MIB.my	IP-FORWARD-MIB
VRRP-MIB.my	VRRP-MIB
UTILIZATION-MANAGEMENT-MIB.my	UTILIZATION-MANAGEMENT-MIB
ENTITY-SENSOR-MIB.my	ENTITY-SENSOR-MIB
RSTP-MIB.my	RSTP-MIB
APPLIC-MIB.MY	APPLIC-MIB
DS1-MIB.my	DS1-MIB
PPP-IP-NCP-MIB.my	PPP-IP-NCP-MIB
RFC1213-MIB.my	RFC1213-MIB
AVAYA-ENTITY-MIB.MY	AVAYA-ENTITY-MIB
Rnd.MIB	RND-MIB
XSWITCH-MIB.MY	XSWITCH-MIB
CROUTE-MIB.MY	CROUTE-MIB
RS-232-MIB.my	RS-232-MIB
RIPv2-MIB.my	RIPv2-MIB
IF-MIB.my	IF-MIB
DS0BUNDLE-MIB.my	DS0BUNDLE-MIB
RFC1406-MIB.my	RFC1406-MIB
DS0-MIB.my	DS0-MIB
POLICY-MIB.MY	POLICY-MIB
BRIDGE-MIB.my	BRIDGE-MIB
CONFIG-MIB.MY	CONFIG-MIB
G700-MG-MIB.MY	G700-MG-MIB
FRAME-RELAY-DTE-MIB.my	FRAME-RELAY-DTE-MIB
IP-MIB.my	IP-MIB
Load12.MIB	LOAD-MIB
	2 of 3

MIB File	MIB Module
PPP-LCP-MIB.my	PPP-LCP-MIB
WAN-MIB.MY	WAN-MIB
SNMPv2-MIB.my	SNMPv2-MIB
USM-MIB.my	USM-MIB
VACM-MIB.my	VACM-MIB
OSPF-MIB.my	OSPF-MIB
Tunnel-MIB.my	TUNNEL-MIB
	3 of 3

The following table provides a list of the MIBs in the Load.MIB file that are supported by the G350 and their OIDs:

Object	OID
genOpModuleId	1.3.6.1.4.1.1751.2.53.1.2.1.1
genOpIndex	1.3.6.1.4.1.1751.2.53.1.2.1.2
genOpRunningState	1.3.6.1.4.1.1751.2.53.1.2.1.3
genOpSourceIndex	1.3.6.1.4.1.1751.2.53.1.2.1.4
genOpDestIndex	1.3.6.1.4.1.1751.2.53.1.2.1.5
genOpServerIP	1.3.6.1.4.1.1751.2.53.1.2.1.6
genOpUserName	1.3.6.1.4.1.1751.2.53.1.2.1.7
genOpPassword	1.3.6.1.4.1.1751.2.53.1.2.1.8
genOpProtocolType	1.3.6.1.4.1.1751.2.53.1.2.1.9
genOpFileName	1.3.6.1.4.1.1751.2.53.1.2.1.10
genOpRunningStateDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.11
genOpLastFailureIndex	1.3.6.1.4.1.1751.2.53.1.2.1.12
genOpLastFailureDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.13
genOpLastWarningDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.14
genOpErrorLogIndex	1.3.6.1.4.1.1751.2.53.1.2.1.15
	1 of 2

Object	OID
genOpResetSupported	1.3.6.1.4.1.1751.2.53.1.2.1.16
genOpEnableReset	1.3.6.1.4.1.1751.2.53.1.2.1.17
genOpNextBootImageIndex	1.3.6.1.4.1.1751.2.53.1.2.1.18
genOpLastBootImageIndex	1.3.6.1.4.1.1751.2.53.1.2.1.19
genOpFileSystemType	1.3.6.1.4.1.1751.2.53.1.2.1.20
genOpReportSpecificFlags	1.3.6.1.4.1.1751.2.53.1.2.1.21
genOpOctetsReceived	1.3.6.1.4.1.1751.2.53.1.2.1.22
genAppFileId	1.3.6.1.4.1.1751.2.53.2.1.1.1
genAppFileName	1.3.6.1.4.1.1751.2.53.2.1.1.2
genAppFileType	1.3.6.‘1.4.1.1751.2.53.2.1.1.3
genAppFileDescription	1.3.6.1.4.1.1751.2.53.2.1.1.4
genAppFileSize	1.3.6.1.4.1.1751.2.53.2.1.1.5
genAppFileVersionNumber	1.3.6.1.4.1.1751.2.53.2.1.1.6
genAppFileLocation	1.3.6.1.4.1.1751.2.53.2.1.1.7
genAppFileDateStamp	1.3.6.1.4.1.1751.2.53.2.1.1.8
genAppFileRowStatus	1.3.6.1.4.1.1751.2.53.2.1.1.9
	2 of 2

The following table provides a list of the MIBs in the RFC1315-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
frDlcmiIfIndex	1.3.6.1.2.1.10.32.1.1.1
frDlcmiState	1.3.6.1.2.1.10.32.1.1.2
frDlcmiAddress	1.3.6.1.2.1.10.32.1.1.3
frDlcmiAddressLen	1.3.6.1.2.1.10.32.1.1.4
frDlcmiPollingInterval	1.3.6.1.2.1.10.32.1.1.5
frDlcmiFullEnquiryInterval	1.3.6.1.2.1.10.32.1.1.6
	1 of 2

Object	OID
frDlcmiErrorThreshold	1.3.6.1.2.1.10.32.1.1.7
frDlcmiMonitoredEvents	1.3.6.1.2.1.10.32.1.1.8
frDlcmiMaxSupportedVCs	1.3.6.1.2.1.10.32.1.1.9
frDlcmiMulticast	1.3.6.1.2.1.10.32.1.1.10
frCircuitIfIndex	1.3.6.1.2.1.10.32.2.1.1
frCircuitDlci	1.3.6.1.2.1.10.32.2.1.2
frCircuitState	1.3.6.1.2.1.10.32.2.1.3
frCircuitReceivedFECNs	1.3.6.1.2.1.10.32.2.1.4
frCircuitReceivedBECNs	1.3.6.1.2.1.10.32.2.1.5
frCircuitSentFrames	1.3.6.1.2.1.10.32.2.1.6
frCircuitSentOctets	1.3.6.1.2.1.10.32.2.1.7
frCircuitReceivedFrames	1.3.6.1.2.1.10.32.2.1.8
frCircuitReceivedOctets	1.3.6.1.2.1.10.32.2.1.9
frCircuitCreationTime	1.3.6.1.2.1.10.32.2.1.10
frCircuitLastTimeChange	1.3.6.1.2.1.10.32.2.1.11
frCircuitCommittedBurst	1.3.6.1.2.1.10.32.2.1.12
frCircuitExcessBurst	1.3.6.1.2.1.10.32.2.1.13
frCircuitThroughput	1.3.6.1.2.1.10.32.2.1.14
frErrIfIndex	1.3.6.1.2.1.10.32.3.1.1
frErrType	1.3.6.1.2.1.10.32.3.1.2
frErrData	1.3.6.1.2.1.10.32.3.1.3
frErrTime	1.3.6.1.2.1.10.32.3.1.4
frTrapState	1.3.6.1.2.1.10.32.4.1
	2 of 2

The following table provides a list of the MIBs in the Q-BRIDGE-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
dot1qVlanVersionNumber	1.3.6.1.2.1.17.7.1.1.1
dot1qMaxVlanId	1.3.6.1.2.1.17.7.1.1.2
dot1qMaxSupportedVlans	1.3.6.1.2.1.17.7.1.1.3
dot1qNumVlans	1.3.6.1.2.1.17.7.1.1.4
dot1qGvrpStatus	1.3.6.1.2.1.17.7.1.1.5
dot1qVlanTimeMark	1.3.6.1.2.1.17.7.1.4.2.1.1
dot1qVlanIndex	1.3.6.1.2.1.17.7.1.4.2.1.2
dot1qVlanFdbId	1.3.6.1.2.1.17.7.1.4.2.1.3
dot1qVlanCurrentEgressPorts	1.3.6.1.2.1.17.7.1.4.2.1.4
dot1qVlanCurrentUntaggedPorts	1.3.6.1.2.1.17.7.1.4.2.1.5
dot1qVlanStatus	1.3.6.1.2.1.17.7.1.4.2.1.6
dot1qVlanCreationTime	1.3.6.1.2.1.17.7.1.4.2.1.7
dot1qVlanStaticName	1.3.6.1.2.1.17.7.1.4.3.1.1
dot1qVlanStaticEgressPorts	1.3.6.1.2.1.17.7.1.4.3.1.2
dot1qVlanForbiddenEgressPorts	1.3.6.1.2.1.17.7.1.4.3.1.3
dot1qVlanStaticUntaggedPorts	1.3.6.1.2.1.17.7.1.4.3.1.4
dot1qVlanStaticRowStatus	1.3.6.1.2.1.17.7.1.4.3.1.5
dot1qNextFreeLocalVlanIndex	1.3.6.1.2.1.17.7.1.4.4
dot1qPvid	1.3.6.1.2.1.17.7.1.4.5.1.1
dot1qPortAcceptableFrameTypes	1.3.6.1.2.1.17.7.1.4.5.1.2
dot1qPortIngressFiltering	1.3.6.1.2.1.17.7.1.4.5.1.3
dot1qPortGvrpStatus	1.3.6.1.2.1.17.7.1.4.5.1.4
dot1qPortGvrpFailedRegistrations	1.3.6.1.2.1.17.7.1.4.5.1.5
dot1qPortGvrpLastPduOrigin	1.3.6.1.2.1.17.7.1.4.5.1.6

The following table provides a list of the MIBs in the ENTITY-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
entPhysicalIndex	1.3.6.1.2.1.47.1.1.1.1.1
entPhysicalDescr	1.3.6.1.2.1.47.1.1.1.1.2
entPhysicalVendorType	1.3.6.1.2.1.47.1.1.1.1.3
entPhysicalContainedIn	1.3.6.1.2.1.47.1.1.1.1.4
entPhysicalClass	1.3.6.1.2.1.47.1.1.1.1.5
entPhysicalParentRelPos	1.3.6.1.2.1.47.1.1.1.1.6
entPhysicalName	1.3.6.1.2.1.47.1.1.1.1.7
entPhysicalHardwareRev	1.3.6.1.2.1.47.1.1.1.1.8
entPhysicalFirmwareRev	1.3.6.1.2.1.47.1.1.1.1.9
entPhysicalSoftwareRev	1.3.6.1.2.1.47.1.1.1.1.10
entPhysicalSerialNum	1.3.6.1.2.1.47.1.1.1.1.11
entPhysicalMfgName	1.3.6.1.2.1.47.1.1.1.1.12
entPhysicalModelName	1.3.6.1.2.1.47.1.1.1.1.13
entPhysicalAlias	1.3.6.1.2.1.47.1.1.1.1.14
entPhysicalAssetID	1.3.6.1.2.1.47.1.1.1.1.15
entPhysicalIsFRU	1.3.6.1.2.1.47.1.1.1.1.16

The following table provides a list of the MIBs in the IP-FORWARD-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
ipCidrRouteNumber	1.3.6.1.2.1.4.24.3
ipCidrRouteDest	1.3.6.1.2.1.4.24.4.1.1
ipCidrRouteMask	1.3.6.1.2.1.4.24.4.1.2
ipCidrRouteTos	1.3.6.1.2.1.4.24.4.1.3

1 of 2

Object	OID
ipCidrRouteNextHop	1.3.6.1.2.1.4.24.4.1.4
ipCidrRouteIfIndex	1.3.6.1.2.1.4.24.4.1.5
ipCidrRouteType	1.3.6.1.2.1.4.24.4.1.6
ipCidrRouteProto	1.3.6.1.2.1.4.24.4.1.7
ipCidrRouteAge	1.3.6.1.2.1.4.24.4.1.8
ipCidrRouteInfo	1.3.6.1.2.1.4.24.4.1.9
ipCidrRouteNextHopAS	1.3.6.1.2.1.4.24.4.1.10
ipCidrRouteMetric1	1.3.6.1.2.1.4.24.4.1.11
ipCidrRouteMetric2	1.3.6.1.2.1.4.24.4.1.12
ipCidrRouteMetric3	1.3.6.1.2.1.4.24.4.1.13
ipCidrRouteMetric4	1.3.6.1.2.1.4.24.4.1.14
ipCidrRouteMetric5	1.3.6.1.2.1.4.24.4.1.15
ipCidrRouteStatus	1.3.6.1.2.1.4.24.4.1.16
	2 of 2

The following table provides a list of the MIBs in theVRRP-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
vrrpNodeVersion	1.3.6.1.2.1.68.1.1.1
vrrpOperVrId	1.3.6.1.2.1.68.1.1.3.1.1
vrrpOperVirtualMacAddr	1.3.6.1.2.1.68.1.1.3.1.2
vrrpOperState	1.3.6.1.2.1.68.1.1.3.1.3
vrrpOperAdminState	1.3.6.1.2.1.68.1.1.3.1.4
vrrpOperPriority	1.3.6.1.2.1.68.1.1.3.1.5
vrrpOperIpAddrCount	1.3.6.1.2.1.68.1.1.3.1.6
vrrpOperMasterIpAddr	1.3.6.1.2.1.68.1.1.3.1.7
vrrpOperPrimaryIpAddr	1.3.6.1.2.1.68.1.1.3.1.8
	1 of 2

Object	OID
vrrpOperAuthType	1.3.6.1.2.1.68.1.1.3.1.9
vrrpOperAuthKey	1.3.6.1.2.1.68.1.1.3.1.10
vrrpOperAdvertisementInterval	1.3.6.1.2.1.68.1.1.3.1.11
vrrpOperPreemptMode	1.3.6.1.2.1.68.1.1.3.1.12
vrrpOperVirtualRouterUpTime	1.3.6.1.2.1.68.1.1.3.1.13
vrrpOperProtocol	1.3.6.1.2.1.68.1.1.3.1.14
vrrpOperRowStatus	1.3.6.1.2.1.68.1.1.3.1.15
vrrpAssoIpAddr	1.3.6.1.2.1.68.1.1.4.1.1
vrrpAssoIpAddrRowStatus	1.3.6.1.2.1.68.1.1.4.1.2
	2 of 2

The following table provides a list of the MIBs in the UTILIZATION-MANAGEMENT-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
genCpuIndex	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.1
genCpuUtilizationEnableMonitoring	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.2
genCpuUtilizationEnableEventGeneration	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.3
genCpuUtilizationHighThreshold	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.4
genCpuAverageUtilization	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.5
genCpuCurrentUtilization	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.6
genCpuUtilizationHistorySampleIndex	1.3.6.1.4.1.6889.2.1.11.1.1.2.1.1
genCpuHistoryUtilization	1.3.6.1.4.1.6889.2.1.11.1.1.2.1.2
genMemUtilizationTotalRAM	1.3.6.1.4.1.6889.2.1.11.1.2.1
genMemUtilizationOperationalImage	1.3.6.1.4.1.6889.2.1.11.1.2.2
genMemUtilizationDynAllocMemUsed	1.3.6.1.4.1.6889.2.1.11.1.2.3.1
genMemUtilizationDynAllocMemMaxUsed	1.3.6.1.4.1.6889.2.1.11.1.2.3.2
genMemUtilizationDynAllocMemAvailable	1.3.6.1.4.1.6889.2.1.11.1.2.3.3
	1 of 2

Object	OID
genMemUtilizationAllocationFailures	1.3.6.1.4.1.6889.2.1.11.1.2.4
genMemUtilizationID	1.3.6.1.4.1.6889.2.1.11.1.2.6.1.1
genMemUtilizationPhyRam	1.3.6.1.4.1.6889.2.1.11.1.2.6.1.2
genMemUtilizationPercentUsed	1.3.6.1.4.1.6889.2.1.11.1.2.6.1.3
	2 of 2

The following table provides a list of the MIBs in the ENTITY-SENSOR-MIB.my file that are supported by the G350 and their OIDs:

Object	
OID	
entPhySensorType	1.3.6.1.2.1.99.1.1.1.1
entPhySensorScale	1.3.6.1.2.1.99.1.1.1.2
entPhySensorPrecision	1.3.6.1.2.1.99.1.1.1.3
entPhySensorValue	1.3.6.1.2.1.99.1.1.1.4
entPhySensorOperStatus	1.3.6.1.2.1.99.1.1.1.5
entPhySensorUnitsDisplay	1.3.6.1.2.1.99.1.1.1.6
entPhySensorValueTimeStamp	1.3.6.1.2.1.99.1.1.1.7
entPhySensorValueUpdateRate	1.3.6.1.2.1.99.1.1.1.8

The following table provides a list of the MIBs in the RSTP-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
dot1dStpVersion	1.3.6.1.2.1.17.2.16
dot1dStpTxHoldCount	1.3.6.1.2.1.17.2.17
dot1dStpPathCostDefault	1.3.6.1.2.1.17.2.18
dot1dStpPortProtocolMigration	1.3.6.1.2.1.17.2.19.1.1
dot1dStpPortAdminEdgePort	1.3.6.1.2.1.17.2.19.1.2
	1 of 2

Object	OID
dot1dStpPortOperEdgePort	1.3.6.1.2.1.17.2.19.1.3
dot1dStpPortAdminPointToPoint	1.3.6.1.2.1.17.2.19.1.4
dot1dStpPortOperPointToPoint	1.3.6.1.2.1.17.2.19.1.5
dot1dStpPortAdminPathCost	1.3.6.1.2.1.17.2.19.1.6
	2 of 2

The following table provides a list of the MIBs in the APPLIC-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
lseIntPortGroupId	1.3.6.1.4.1.81.19.1.2.1.1.1
lseIntPortId	1.3.6.1.4.1.81.19.1.2.1.1.2
lseIntPortCAMLastChange	1.3.6.1.4.1.81.19.1.2.1.1.39
lseIntPortMACAddGroupId	1.3.6.1.4.1.81.19.1.2.2.1.1.1
lseIntPortMACAddPortId	1.3.6.1.4.1.81.19.1.2.2.1.1.2
lseIntPortMACAddLAId	1.3.6.1.4.1.81.19.1.2.2.1.1.3
lseIntPortMACAddList	1.3.6.1.4.1.81.19.1.2.2.1.1.4

The following table provides a list of the MIBs in the DS1-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
dsx1LineIndex	1.3.6.1.2.1.10.18.6.1.1
dsx1IfIndex	1.3.6.1.2.1.10.18.6.1.2
dsx1TimeElapsed	1.3.6.1.2.1.10.18.6.1.3
dsx1ValidIntervals	1.3.6.1.2.1.10.18.6.1.4
dsx1LineType	1.3.6.1.2.1.10.18.6.1.5
dsx1LineCoding	1.3.6.1.2.1.10.18.6.1.6
dsx1SendCode	1.3.6.1.2.1.10.18.6.1.7
	1 of 3

Object	OID
dsx1CircuitIdentifier	1.3.6.1.2.1.10.18.6.1.8
dsx1LoopbackConfig	1.3.6.1.2.1.10.18.6.1.9
dsx1LineStatus	1.3.6.1.2.1.10.18.6.1.10
dsx1SignalMode	1.3.6.1.2.1.10.18.6.1.11
dsx1TransmitClockSource	1.3.6.1.2.1.10.18.6.1.12
dsx1Fdl	1.3.6.1.2.1.10.18.6.1.13
dsx1InvalidIntervals	1.3.6.1.2.1.10.18.6.1.14
dsx1LineLength	1.3.6.1.2.1.10.18.6.1.15
dsx1LineStatusLastChange	1.3.6.1.2.1.10.18.6.1.16
dsx1LineStatusChangeTrapEnable	1.3.6.1.2.1.10.18.6.1.17
dsx1LoopbackStatus	1.3.6.1.2.1.10.18.6.1.18
dsx1Ds1ChannelNumber	1.3.6.1.2.1.10.18.6.1.19
dsx1Channelization	1.3.6.1.2.1.10.18.6.1.20
dsx1CurrentIndex	1.3.6.1.2.1.10.18.7.1.1
dsx1CurrentESs	1.3.6.1.2.1.10.18.7.1.2
dsx1CurrentSESs	1.3.6.1.2.1.10.18.7.1.3
dsx1CurrentSEFSs	1.3.6.1.2.1.10.18.7.1.4
dsx1CurrentUASs	1.3.6.1.2.1.10.18.7.1.5
dsx1CurrentCSSs	1.3.6.1.2.1.10.18.7.1.6
dsx1CurrentPCVs	1.3.6.1.2.1.10.18.7.1.7
dsx1CurrentLESs	1.3.6.1.2.1.10.18.7.1.8
dsx1CurrentBESs	1.3.6.1.2.1.10.18.7.1.9
dsx1CurrentDMs	1.3.6.1.2.1.10.18.7.1.10
dsx1CurrentLCVs	1.3.6.1.2.1.10.18.7.1.11
dsx1IntervalIndex	1.3.6.1.2.1.10.18.8.1.1
dsx1IntervalNumber	1.3.6.1.2.1.10.18.8.1.2

Object	OID
dsx1IntervalESs	1.3.6.1.2.1.10.18.8.1.3
dsx1IntervalSESs	1.3.6.1.2.1.10.18.8.1.4
dsx1IntervalSEFSs	1.3.6.1.2.1.10.18.8.1.5
dsx1IntervalUASs	1.3.6.1.2.1.10.18.8.1.6
dsx1IntervalCSSs	1.3.6.1.2.1.10.18.8.1.7
dsx1IntervalPCVs	1.3.6.1.2.1.10.18.8.1.8
dsx1IntervalLESs	1.3.6.1.2.1.10.18.8.1.9
dsx1IntervalBESs	1.3.6.1.2.1.10.18.8.1.10
dsx1IntervalDMs	1.3.6.1.2.1.10.18.8.1.11
dsx1IntervalLCVs	1.3.6.1.2.1.10.18.8.1.12
dsx1IntervalValidData	1.3.6.1.2.1.10.18.8.1.13
dsx1TotalIndex	1.3.6.1.2.1.10.18.9.1.1
dsx1TotalESs	1.3.6.1.2.1.10.18.9.1.2
dsx1TotalSESs	1.3.6.1.2.1.10.18.9.1.3
dsx1TotalSEFSs	1.3.6.1.2.1.10.18.9.1.4
dsx1TotalUASs	1.3.6.1.2.1.10.18.9.1.5
dsx1TotalCSSs	1.3.6.1.2.1.10.18.9.1.6
dsx1TotalPCVs	1.3.6.1.2.1.10.18.9.1.7
dsx1TotalLESs	1.3.6.1.2.1.10.18.9.1.8
dsx1TotalBESs	1.3.6.1.2.1.10.18.9.1.9
dsx1TotalDMs	1.3.6.1.2.1.10.18.9.1.10
dsx1TotalLCVs	1.3.6.1.2.1.10.18.9.1.11
	3 of 3

The following table provides a list of the MIBs in the PPP-IP-NCP-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
pppIpOperStatus	1.3.6.1.2.1.10.23.3.1.1.1
pppIpLocalToRemoteCompressionProtocol	1.3.6.1.2.1.10.23.3.1.1.2
pppIpRemoteToLocalCompressionProtocol	1.3.6.1.2.1.10.23.3.1.1.3
pppIpRemoteMaxSlotId	1.3.6.1.2.1.10.23.3.1.1.4
pppIpLocalMaxSlotId	1.3.6.1.2.1.10.23.3.1.1.5
pppIpConfigAdminStatus	1.3.6.1.2.1.10.23.3.2.1.1
pppIpConfigCompression	1.3.6.1.2.1.10.23.3.2.1.2

The following table provides a list of the MIBs in the RFC1213-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
sysDescr	1.3.6.1.2.1.1.1
sysObjectID	1.3.6.1.2.1.1.2
sysUpTime	1.3.6.1.2.1.1.3
sysContact	1.3.6.1.2.1.1.4
sysName	1.3.6.1.2.1.1.5
sysLocation	1.3.6.1.2.1.1.6
sysServices	1.3.6.1.2.1.1.7
ifNumber	1.3.6.1.2.1.2.1
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifMtu	1.3.6.1.2.1.2.2.1.4
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
	1 of 5

Object	OID
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8
ifLastChange	1.3.6.1.2.1.2.2.1.9
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifInErrors	1.3.6.1.2.1.2.2.1.14
ifInUnknownProtos	1.3.6.1.2.1.2.2.1.15
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19
ifOutErrors	1.3.6.1.2.1.2.2.1.20
ifOutQLen	1.3.6.1.2.1.2.2.1.21
ifSpecific	1.3.6.1.2.1.2.2.1.22
ipForwarding	1.3.6.1.2.1.4.1
ipDefaultTTL	1.3.6.1.2.1.4.2
ipInReceives	1.3.6.1.2.1.4.3
ipInHdrErrors	1.3.6.1.2.1.4.4
ipInAddrErrors	1.3.6.1.2.1.4.5
ipForwDatagrams	1.3.6.1.2.1.4.6
ipInUnknownProtos	1.3.6.1.2.1.4.7
ipInDiscards	1.3.6.1.2.1.4.8
ipInDelivers	1.3.6.1.2.1.4.9
ipOutRequests	1.3.6.1.2.1.4.10

Object	OID
ipOutDiscards	1.3.6.1.2.1.4.11
ipOutNoRoutes	1.3.6.1.2.1.4.12
ipReasmTimeout	1.3.6.1.2.1.4.13
ipReasmReqds	1.3.6.1.2.1.4.14
ipReasmOKs	1.3.6.1.2.1.4.15
ipReasmFails	1.3.6.1.2.1.4.16
ipFragOKs	1.3.6.1.2.1.4.17
ipFragFails	1.3.6.1.2.1.4.18
ipFragCreates	1.3.6.1.2.1.4.19
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipAdEntBcastAddr	1.3.6.1.2.1.4.20.1.4
ipAdEntReasmMaxSize	1.3.6.1.2.1.4.20.1.5
ipRouteDest	1.3.6.1.2.1.4.21.1.1
ipRouteIfIndex	1.3.6.1.2.1.4.21.1.2
ipRouteMetric1	1.3.6.1.2.1.4.21.1.3
ipRouteMetric2	1.3.6.1.2.1.4.21.1.4
ipRouteMetric3	1.3.6.1.2.1.4.21.1.5
ipRouteMetric4	1.3.6.1.2.1.4.21.1.6
ipRouteNextHop	1.3.6.1.2.1.4.21.1.7
ipRouteType	1.3.6.1.2.1.4.21.1.8
ipRouteProto	1.3.6.1.2.1.4.21.1.9
ipRouteAge	1.3.6.1.2.1.4.21.1.10
ipRouteMask	1.3.6.1.2.1.4.21.1.11
ipRouteMetric5	1.3.6.1.2.1.4.21.1.12
	3 of 5

Object	OID
ipRouteInfo	1.3.6.1.2.1.4.21.1.13
ipNetToMediaIfIndex	1.3.6.1.2.1.4.22.1.1
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToMediaNetAddress	1.3.6.1.2.1.4.22.1.3
ipNetToMediaType	1.3.6.1.2.1.4.22.1.4
ipRoutingDiscards	1.3.6.1.2.1.4.23
snmpInPkts	1.3.6.1.2.1.11.1
snmpOutPkts	1.3.6.1.2.1.11.2
snmpInBadVersions	1.3.6.1.2.1.11.3
snmpInBadCommunityNames	1.3.6.1.2.1.11.4
snmpInBadCommunityUses	1.3.6.1.2.1.11.5
snmpInASNParseErrs	1.3.6.1.2.1.11.6
snmpInTooBigs	1.3.6.1.2.1.11.8
snmpInNoSuchNames	1.3.6.1.2.1.11.9
snmpInBadValues	1.3.6.1.2.1.11.10
snmpInReadOnlys	1.3.6.1.2.1.11.11
snmpInGenErrs	1.3.6.1.2.1.11.12
snmpInTotalReqVars	1.3.6.1.2.1.11.13
snmpInTotalSetVars	1.3.6.1.2.1.11.14
snmpInGetRequests	1.3.6.1.2.1.11.15
snmpInGetNexts	1.3.6.1.2.1.11.16
snmpInSetRequests	1.3.6.1.2.1.11.17
snmpInGetResponses	1.3.6.1.2.1.11.18
snmpInTraps	1.3.6.1.2.1.11.19
snmpOutTooBigs	1.3.6.1.2.1.11.20
snmpOutNoSuchNames	1.3.6.1.2.1.11.21
	4 of 5

Object	OID
snmpOutBadValues	1.3.6.1.2.1.11.22
snmpOutGenErrs	1.3.6.1.2.1.11.24
snmpOutGetRequests	1.3.6.1.2.1.11.25
snmpOutGetNexts	1.3.6.1.2.1.11.26
snmpOutSetRequests	1.3.6.1.2.1.11.27
snmpOutGetResponses	1.3.6.1.2.1.11.28
snmpOutTraps	1.3.6.1.2.1.11.29
snmpEnableAuthenTraps	1.3.6.1.2.1.11.30
	5 of 5

The following table provides a list of the MIBs in the AVAYA-ENTITY-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
avEntPhySensorHiShutdown	1.3.6.1.4.1.6889.2.1.99.1.1.1
avEntPhySensorHiWarning	1.3.6.1.4.1.6889.2.1.99.1.1.2
avEntPhySensorHiWarningClear	1.3.6.1.4.1.6889.2.1.99.1.1.3
avEntPhySensorLoWarningClear	1.3.6.1.4.1.6889.2.1.99.1.1.4
avEntPhySensorLoWarning	1.3.6.1.4.1.6889.2.1.99.1.1.5
avEntPhySensorLoShutdown	1.3.6.1.4.1.6889.2.1.99.1.1.6
avEntPhySensorEventSupportMask	1.3.6.1.4.1.6889.2.1.99.1.1.7

The following table provides a list of the MIBs in the Rnd.MIB file that are supported by the G350 and their OIDs:

Object	OID
genGroupHWVersion	1.3.6.1.4.1.81.8.1.1.24
genGroupConfigurationSymbol	1.3.6.1.4.1.81.8.1.1.21
genGroupHWStatus	1.3.6.1.4.1.81.8.1.1.17

The following table provides a list of the MIBs in the XSWITCH-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
scGenPortGroupId	1.3.6.1.4.1.81.28.1.4.1.1.1
scGenPortId	1.3.6.1.4.1.81.28.1.4.1.1.2
scGenPortVLAN	1.3.6.1.4.1.81.28.1.4.1.1.3
scGenPortPriority	1.3.6.1.4.1.81.28.1.4.1.1.4
scGenPortSetDefaults	1.3.6.1.4.1.81.28.1.4.1.1.5
scGenPortLinkAggregationNumber	1.3.6.1.4.1.81.28.1.4.1.1.9
scGenPortGenericTrap	1.3.6.1.4.1.81.28.1.4.1.1.15
scGenPortLagCapability	1.3.6.1.4.1.81.28.1.4.1.1.20
scGenPortCapability	1.3.6.1.4.1.81.28.1.4.1.1.21
scGenSwitchId	1.3.6.1.4.1.81.28.1.5.1.1.1
scGenSwitchSTA	1.3.6.1.4.1.81.28.1.5.1.1.13
scEthPortGroupId	1.3.6.1.4.1.81.28.2.1.1.1.1
scEthPortId	1.3.6.1.4.1.81.28.2.1.1.1.2
scEthPortFunctionalStatus	1.3.6.1.4.1.81.28.2.1.1.1.27
scEthPortMode	1.3.6.1.4.1.81.28.2.1.1.1.28
scEthPortSpeed	1.3.6.1.4.1.81.28.2.1.1.1.29
scEthPortAutoNegotiation	1.3.6.1.4.1.81.28.2.1.1.1.30
scEthPortAutoNegotiationStatus	1.3.6.1.4.1.81.28.2.1.1.1.31
scEthPortPauseCapabilities	1.3.6.1.4.1.81.28.2.1.1.1.44
scEthPortFlowControl	1.3.6.1.4.1.81.28.2.1.1.1.47

The following table provides a list of the MIBs in the CROUTE-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
ipGlobalsBOOTPRelayStatus	1.3.6.1.4.1.81.31.1.1.1
ipGlobalsICMPErrMsgEnable	1.3.6.1.4.1.81.31.1.1.2
ipGlobalsARPInactiveTimeout	1.3.6.1.4.1.81.31.1.1.3
ipGlobalsPrimaryManagementIPAddress	1.3.6.1.4.1.81.31.1.1.4
ipGlobalsNextPrimaryManagementIPAddress	1.3.6.1.4.1.81.31.1.1.5
ipInterfaceAddr	1.3.6.1.4.1.81.31.1.2.1.1
ipInterfaceNetMask	1.3.6.1.4.1.81.31.1.2.1.2
ipInterfaceLowerIfAlias	1.3.6.1.4.1.81.31.1.2.1.3
ipInterfaceType	1.3.6.1.4.1.81.31.1.2.1.4
ipInterfaceForwardIpBroadcast	1.3.6.1.4.1.81.31.1.2.1.5
ipInterfaceBroadcastAddr	1.3.6.1.4.1.81.31.1.2.1.6
ipInterfaceProxyArp	1.3.6.1.4.1.81.31.1.2.1.7
ipInterfaceStatus	1.3.6.1.4.1.81.31.1.2.1.8
ipInterfaceMainRouterAddr	1.3.6.1.4.1.81.31.1.2.1.9
ipInterfaceARPServerStatus	1.3.6.1.4.1.81.31.1.2.1.10
ipInterfaceName	1.3.6.1.4.1.81.31.1.2.1.11
ipInterfaceNetbiosRebroadcast	1.3.6.1.4.1.81.31.1.2.1.12
ipInterfaceIcmpRedirects	1.3.6.1.4.1.81.31.1.2.1.13
ipInterfaceOperStatus	1.3.6.1.4.1.81.31.1.2.1.14
ipInterfaceDhcpRelay	1.3.6.1.4.1.81.31.1.2.1.15
ripGlobalsRIPEnable	1.3.6.1.4.1.81.31.1.3.1
ripGlobalsLeakOSPFIntoRIP	1.3.6.1.4.1.81.31.1.3.2
ripGlobalsLeakStaticIntoRIP	1.3.6.1.4.1.81.31.1.3.3
ripGlobalsPeriodicUpdateTimer	1.3.6.1.4.1.81.31.1.3.4
ripGlobalsPeriodicInvalidRouteTimer	1.3.6.1.4.1.81.31.1.3.5

Object	OID
ripGlobalsDefaultExportMetric	1.3.6.1.4.1.81.31.1.3.6
ripInterfaceAddr	1.3.6.1.4.1.81.31.1.4.1.1
ripInterfaceMetric	1.3.6.1.4.1.81.31.1.4.1.2
ripInterfaceSplitHorizon	1.3.6.1.4.1.81.31.1.4.1.3
ripInterfaceAcceptDefaultRoute	1.3.6.1.4.1.81.31.1.4.1.4
ripInterfaceSendDefaultRoute	1.3.6.1.4.1.81.31.1.4.1.5
ripInterfaceState	1.3.6.1.4.1.81.31.1.4.1.6
ripInterfaceSendMode	1.3.6.1.4.1.81.31.1.4.1.7
ripInterfaceVersion	1.3.6.1.4.1.81.31.1.4.1.8
ospfGlobalsLeakRIPIntoOSPF	1.3.6.1.4.1.81.31.1.5.1
ospfGlobalsLeakStaticIntoOSPF	1.3.6.1.4.1.81.31.1.5.2
ospfGlobalsLeakDirectIntoOSPF	1.3.6.1.4.1.81.31.1.5.3
ospfGlobalsDefaultExportMetric	1.3.6.1.4.1.81.31.1.5.4
relayVlIndex	1.3.6.1.4.1.81.31.1.6.1.1
relayVlPrimaryServerAddr	1.3.6.1.4.1.81.31.1.6.1.2
relayVlSeconderyServerAddr	1.3.6.1.4.1.81.31.1.6.1.3
relayVlStatus	1.3.6.1.4.1.81.31.1.6.1.4
relayVlRelayAddr	1.3.6.1.4.1.81.31.1.6.1.5
ipRedundancyStatus	1.3.6.1.4.1.81.31.1.9.1
ipRedundancyTimeout	1.3.6.1.4.1.81.31.1.9.2
ipRedundancyPollingInterval	1.3.6.1.4.1.81.31.1.9.3
ipShortcutARPServerStatus	1.3.6.1.4.1.81.31.1.10.1
distributionListRoutingProtocol	1.3.6.1.4.1.81.31.1.12.1.1
distributionListDirection	1.3.6.1.4.1.81.31.1.12.1.2
distributionListIfIndex	1.3.6.1.4.1.81.31.1.12.1.3
distributionListRouteProtocol	1.3.6.1.4.1.81.31.1.12.1.4

2 of 4

Object	OID
distributionListProtocolSpecific1	1.3.6.1.4.1.81.31.1.12.1.5
distributionListProtocolSpecific2	1.3.6.1.4.1.81.31.1.12.1.6
distributionListProtocolSpecific3	1.3.6.1.4.1.81.31.1.12.1.7
distributionListProtocolSpecific4	1.3.6.1.4.1.81.31.1.12.1.8
distributionListProtocolSpecific5	1.3.6.1.4.1.81.31.1.12.1.9
distributionListAccessListNumber	1.3.6.1.4.1.81.31.1.12.1.10
distributionListEntryStatus	1.3.6.1.4.1.81.31.1.12.1.11
ipVRRPAdminStatus	1.3.6.1.4.1.81.31.1.14.1
iphcIfIndex	1.3.6.1.4.1.81.31.1.15.1.1.1
iphcControlTcpAdminStatus	1.3.6.1.4.1.81.31.1.15.1.1.2
iphcTcpSessions	1.3.6.1.4.1.81.31.1.15.1.1.3
iphcNegotiatedTcpSessions	1.3.6.1.4.1.81.31.1.15.1.1.4
iphcControlRtpAdminStatus	1.3.6.1.4.1.81.31.1.15.1.1.5
iphcRtpSessions	1.3.6.1.4.1.81.31.1.15.1.1.6
iphcNegotiatedRtpSessions	1.3.6.1.4.1.81.31.1.15.1.1.7
iphcControlNonTcpAdminStatus	1.3.6.1.4.1.81.31.1.15.1.1.8
iphcNonTcpSessions	1.3.6.1.4.1.81.31.1.15.1.1.9
iphcNegotiatedNonTcpSessions	1.3.6.1.4.1.81.31.1.15.1.1.10
iphcMaxPeriod	1.3.6.1.4.1.81.31.1.15.1.1.11
iphcMaxTime	1.3.6.1.4.1.81.31.1.15.1.1.12
iphcControRtpMinPortNumber	1.3.6.1.4.1.81.31.1.15.1.1.13
iphcControRtpMaxPortNumber	1.3.6.1.4.1.81.31.1.15.1.1.14
iphcControlRtpCompressionRatio	1.3.6.1.4.1.81.31.1.15.1.1.15
iphcControlNonTcpMode	1.3.6.1.4.1.81.31.1.15.1.1.16
ospfXtndIfIpAddress	1.3.6.1.4.1.81.31.1.16.1.1
ospfXtndIfAddressLessIf	1.3.6.1.4.1.81.31.1.16.1.2
	3 of 4

Object	OID
ospfXtndIfPassiveMode	1.3.6.1.4.1.81.31.1.16.1.3
vlConfIndex	1.3.6.1.4.1.81.31.3.1.1.1
vlConfAlias	1.3.6.1.4.1.81.31.3.1.1.2
vlConfStatus	1.3.6.1.4.1.81.31.3.1.1.3
	4 of 4

The following table provides a list of the MIBs in the RS-232-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
rs232Number	1.3.6.1.2.1.10.33.1
rs232PortIndex	1.3.6.1.2.1.10.33.2.1.1
rs232PortType	1.3.6.1.2.1.10.33.2.1.2
rs232PortInSigNumber	1.3.6.1.2.1.10.33.2.1.3
rs232PortOutSigNumber	1.3.6.1.2.1.10.33.2.1.4
rs232PortInSpeed	1.3.6.1.2.1.10.33.2.1.5
rs232PortOutSpeed	1.3.6.1.2.1.10.33.2.1.6
rs232PortInFlowType	1.3.6.1.2.1.10.33.2.1.7
rs232PortOutFlowType	1.3.6.1.2.1.10.33.2.1.8
rs232SyncPortIndex	1.3.6.1.2.1.10.33.4.1.1
rs232SyncPortClockSource	1.3.6.1.2.1.10.33.4.1.2
rs232SyncPortFrameCheckErrs	1.3.6.1.2.1.10.33.4.1.3
rs232SyncPortTransmitUnderrunErrs	1.3.6.1.2.1.10.33.4.1.4
rs232SyncPortReceiveOverrunErrs	1.3.6.1.2.1.10.33.4.1.5
rs232SyncPortInterruptedFrames	1.3.6.1.2.1.10.33.4.1.6
rs232SyncPortAbortedFrames	1.3.6.1.2.1.10.33.4.1.7
rs232SyncPortRole	1.3.6.1.2.1.10.33.4.1.8
rs232SyncPortEncoding	1.3.6.1.2.1.10.33.4.1.9
	1 of 2

Object	OID
rs232SyncPortRTSControl	1.3.6.1.2.1.10.33.4.1.10
rs232SyncPortRTSCTSDelay	1.3.6.1.2.1.10.33.4.1.11
rs232SyncPortMode	1.3.6.1.2.1.10.33.4.1.12
rs232SyncPortIdlePattern	1.3.6.1.2.1.10.33.4.1.13
rs232SyncPortMinFlags	1.3.6.1.2.1.10.33.4.1.14
rs232InSigPortIndex	1.3.6.1.2.1.10.33.5.1.1
rs232InSigName	1.3.6.1.2.1.10.33.5.1.2
rs232InSigState	1.3.6.1.2.1.10.33.5.1.3
rs232InSigChanges	1.3.6.1.2.1.10.33.5.1.4
rs232OutSigPortIndex	1.3.6.1.2.1.10.33.6.1.1
rs232OutSigName	1.3.6.1.2.1.10.33.6.1.2
rs232OutSigState	1.3.6.1.2.1.10.33.6.1.3
rs232OutSigChanges	1.3.6.1.2.1.10.33.6.1.4
	2 of 2

The following table provides a list of the MIBs in the RIPv2-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
rip2GlobalRouteChanges	1.3.6.1.2.1.23.1.1
rip2GlobalQueries	1.3.6.1.2.1.23.1.2
rip2IfStatAddress	1.3.6.1.2.1.23.2.1.1
rip2IfStatRcvBadPackets	1.3.6.1.2.1.23.2.1.2
rip2IfStatRcvBadRoutes	1.3.6.1.2.1.23.2.1.3
rip2IfStatSentUpdates	1.3.6.1.2.1.23.2.1.4
rip2IfStatStatus	1.3.6.1.2.1.23.2.1.5
rip2IfConfAddress	1.3.6.1.2.1.23.3.1.1
rip2IfConfDomain	1.3.6.1.2.1.23.3.1.2
	1 of 2

Object	OID
rip2IfConfAuthType	1.3.6.1.2.1.23.3.1.3
rip2IfConfAuthKey	1.3.6.1.2.1.23.3.1.4
rip2IfConfSend	1.3.6.1.2.1.23.3.1.5
rip2IfConfReceive	1.3.6.1.2.1.23.3.1.6
rip2IfConfDefaultMetric	1.3.6.1.2.1.23.3.1.7
rip2IfConfStatus	1.3.6.1.2.1.23.3.1.8
rip2IfConfSrcAddress	1.3.6.1.2.1.23.3.1.9
	2 of 2

The following table provides a list of the MIBs in the IF-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
ifNumber	1.3.6.1.2.1.2.1
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifMtu	1.3.6.1.2.1.2.2.1.4
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8
ifLastChange	1.3.6.1.2.1.2.2.1.9
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifInErrors	1.3.6.1.2.1.2.2.1.14
	1 of 3

Object	OID
ifInUnknownProtos	1.3.6.1.2.1.2.2.1.15
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19
ifOutErrors	1.3.6.1.2.1.2.2.1.20
ifOutQLen	1.3.6.1.2.1.2.2.1.21
ifSpecific	1.3.6.1.2.1.2.2.1.22
ifName	1.3.6.1.2.1.31.1.1.1.1
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5
ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6
ifHCInUcastPkts	1.3.6.1.2.1.31.1.1.1.7
ifHCInMulticastPkts	1.3.6.1.2.1.31.1.1.1.8
ifHCInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.9
ifHCOutOctets	1.3.6.1.2.1.31.1.1.1.10
ifHCOutUcastPkts	1.3.6.1.2.1.31.1.1.1.11
ifHCOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.12
ifHCOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.13
ifLinkUpDownTrapEnable	1.3.6.1.2.1.31.1.1.1.14
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15
ifPromiscuousMode	1.3.6.1.2.1.31.1.1.1.16
ifConnectorPresent	1.3.6.1.2.1.31.1.1.1.17

Object	OID
ifAlias	1.3.6.1.2.1.31.1.1.1.18
ifCounterDiscontinuityTime	1.3.6.1.2.1.31.1.1.1.19
	3 of 3

The following table provides a list of the MIBs in the DS0BUNDLE-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
dsx0BundleIndex	1.3.6.1.2.1.10.82.3.1.1
dsx0BundleIfIndex	1.3.6.1.2.1.10.82.3.1.2
dsx0BundleCircuitIdentifier	1.3.6.1.2.1.10.82.3.1.3
dsx0BundleRowStatus	1.3.6.1.2.1.10.82.3.1.4

The following table provides a list of the MIBs in the RFC1406-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
dsx1LineIndex	1.3.6.1.2.1.10.18.6.1.1
dsx1IfIndex	1.3.6.1.2.1.10.18.6.1.2
dsx1TimeElapsed	1.3.6.1.2.1.10.18.6.1.3
dsx1ValidIntervals	1.3.6.1.2.1.10.18.6.1.4
dsx1LineType	1.3.6.1.2.1.10.18.6.1.5
dsx1LineCoding	1.3.6.1.2.1.10.18.6.1.6
dsx1SendCode	1.3.6.1.2.1.10.18.6.1.7
dsx1CircuitIdentifier	1.3.6.1.2.1.10.18.6.1.8
dsx1LoopbackConfig	1.3.6.1.2.1.10.18.6.1.9
dsx1LineStatus	1.3.6.1.2.1.10.18.6.1.10
dsx1SignalMode	1.3.6.1.2.1.10.18.6.1.11
dsx1TransmitClockSource	1.3.6.1.2.1.10.18.6.1.12
	1 of 3

Object	OID
dsx1Fdl	1.3.6.1.2.1.10.18.6.1.13
dsx1CurrentIndex	1.3.6.1.2.1.10.18.7.1.1
dsx1CurrentESs	1.3.6.1.2.1.10.18.7.1.2
dsx1CurrentSESs	1.3.6.1.2.1.10.18.7.1.3
dsx1CurrentSEFSs	1.3.6.1.2.1.10.18.7.1.4
dsx1CurrentUASs	1.3.6.1.2.1.10.18.7.1.5
dsx1CurrentCSSs	1.3.6.1.2.1.10.18.7.1.6
dsx1CurrentPCVs	1.3.6.1.2.1.10.18.7.1.7
dsx1CurrentLESs	1.3.6.1.2.1.10.18.7.1.8
dsx1CurrentBESs	1.3.6.1.2.1.10.18.7.1.9
dsx1CurrentDMs	1.3.6.1.2.1.10.18.7.1.10
dsx1CurrentLCVs	1.3.6.1.2.1.10.18.7.1.11
dsx1IntervalIndex	1.3.6.1.2.1.10.18.8.1.1
dsx1IntervalNumber	1.3.6.1.2.1.10.18.8.1.2
dsx1IntervalESs	1.3.6.1.2.1.10.18.8.1.3
dsx1IntervalSESs	1.3.6.1.2.1.10.18.8.1.4
dsx1IntervalSEFSs	1.3.6.1.2.1.10.18.8.1.5
dsx1IntervalUASs	1.3.6.1.2.1.10.18.8.1.6
dsx1IntervalCSSs	1.3.6.1.2.1.10.18.8.1.7
dsx1IntervalPCVs	1.3.6.1.2.1.10.18.8.1.8
dsx1IntervalLESs	1.3.6.1.2.1.10.18.8.1.9
dsx1IntervalBESs	1.3.6.1.2.1.10.18.8.1.10
dsx1IntervalDMs	1.3.6.1.2.1.10.18.8.1.11
dsx1IntervalLCVs	1.3.6.1.2.1.10.18.8.1.12
dsx1TotalIndex	1.3.6.1.2.1.10.18.9.1.1
dsx1TotalESs	1.3.6.1.2.1.10.18.9.1.2

Object	OID
dsx1TotalSESs	1.3.6.1.2.1.10.18.9.1.3
dsx1TotalSEFSs	1.3.6.1.2.1.10.18.9.1.4
dsx1TotalUASs	1.3.6.1.2.1.10.18.9.1.5
dsx1TotalCSSs	1.3.6.1.2.1.10.18.9.1.6
dsx1TotalPCVs	1.3.6.1.2.1.10.18.9.1.7
dsx1TotalLESs	1.3.6.1.2.1.10.18.9.1.8
dsx1TotalBESs	1.3.6.1.2.1.10.18.9.1.9
dsx1TotalDMs	1.3.6.1.2.1.10.18.9.1.10
dsx1TotalLCVs	1.3.6.1.2.1.10.18.9.1.11
	3 of 3

The following table provides a list of the MIBs in the DS0-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
dsx0Ds0ChannelNumber	1.3.6.1.2.1.10.81.1.1.1
dsx0RobbedBitSignalling	1.3.6.1.2.1.10.81.1.1.2
dsx0CircuitIdentifier	1.3.6.1.2.1.10.81.1.1.3
dsx0IdleCode	1.3.6.1.2.1.10.81.1.1.4
dsx0SeizedCode	1.3.6.1.2.1.10.81.1.1.5
dsx0ReceivedCode	1.3.6.1.2.1.10.81.1.1.6
dsx0TransmitCodesEnable	1.3.6.1.2.1.10.81.1.1.7
dsx0Ds0BundleMappedIfIndex	1.3.6.1.2.1.10.81.1.1.8
dsx0ChanMappedIfIndex	1.3.6.1.2.1.10.81.3.1.1

The following table provides a list of the MIBs in the POLICY-MIB.MY file that are supported by the G350 and their OIDs:

Object	OID
ipPolicyListSlot	1.3.6.1.4.1.81.36.1.1.1
ipPolicyListID	1.3.6.1.4.1.81.36.1.1.2
ipPolicyListName	1.3.6.1.4.1.81.36.1.1.3
ipPolicyListValidityStatus	1.3.6.1.4.1.81.36.1.1.4
ipPolicyListChecksum	1.3.6.1.4.1.81.36.1.1.5
ipPolicyListRowStatus	1.3.6.1.4.1.81.36.1.1.6
ipPolicyListDefaultOperation	1.3.6.1.4.1.81.36.1.1.7
ipPolicyListCookie	1.3.6.1.4.1.81.36.1.1.8
ipPolicyListTrackChanges	1.3.6.1.4.1.81.36.1.1.9
ipPolicyListOwner	1.3.6.1.4.1.81.36.1.1.10
ipPolicyListErrMsg	1.3.6.1.4.1.81.36.1.1.11
ipPolicyListTrustedFields	1.3.6.1.4.1.81.36.1.1.12
ipPolicyListScope	1.3.6.1.4.1.81.36.1.1.13
ipPolicyListIpOptionOperation	1.3.6.1.4.1.81.36.1.1.14
ipPolicyListIpFragmentationOperation	1.3.6.1.4.1.81.36.1.1.15
ipPolicyListType	1.3.6.1.4.1.81.36.1.1.16
ipPolicyListEtherTypeDefaultOperation	1.3.6.1.4.1.81.36.1.1.17
ipPolicyRuleSlot	1.3.6.1.4.1.81.36.2.1.1
ipPolicyRuleListID	1.3.6.1.4.1.81.36.2.1.2
ipPolicyRuleID	1.3.6.1.4.1.81.36.2.1.3
ipPolicyRuleSrcAddr	1.3.6.1.4.1.81.36.2.1.4
ipPolicyRuleSrcAddrWild	1.3.6.1.4.1.81.36.2.1.5
ipPolicyRuleDstAddr	1.3.6.1.4.1.81.36.2.1.6
ipPolicyRuleDstAddrWild	1.3.6.1.4.1.81.36.2.1.7
ipPolicyRuleProtocol	1.3.6.1.4.1.81.36.2.1.8
	1 of 6

Object	OID
ipPolicyRuleL4SrcPortMin	1.3.6.1.4.1.81.36.2.1.9
ipPolicyRuleL4SrcPortMax	1.3.6.1.4.1.81.36.2.1.10
ipPolicyRuleL4DestPortMin	1.3.6.1.4.1.81.36.2.1.11
ipPolicyRuleL4DestPortMax	1.3.6.1.4.1.81.36.2.1.12
ipPolicyRuleEstablished	1.3.6.1.4.1.81.36.2.1.13
ipPolicyRuleOperation	1.3.6.1.4.1.81.36.2.1.14
ipPolicyRuleApplicabilityPrecedence	1.3.6.1.4.1.81.36.2.1.15
ipPolicyRuleApplicabilityStatus	1.3.6.1.4.1.81.36.2.1.16
ipPolicyRuleApplicabilityType	1.3.6.1.4.1.81.36.2.1.17
ipPolicyRuleErrMsg	1.3.6.1.4.1.81.36.2.1.18
ipPolicyRuleStatus	1.3.6.1.4.1.81.36.2.1.19
ipPolicyRuleDSCPOperation	1.3.6.1.4.1.81.36.2.1.20
ipPolicyRuleDSCPFilter	1.3.6.1.4.1.81.36.2.1.21
ipPolicyRuleDSCPFilterWild	1.3.6.1.4.1.81.36.2.1.22
ipPolicyRuleIcmpTypeCode	1.3.6.1.4.1.81.36.2.1.23
ipPolicyRuleSrcAddrNot	1.3.6.1.4.1.81.36.2.1.24
ipPolicyRuleDstAddrNot	1.3.6.1.4.1.81.36.2.1.25
ipPolicyRuleProtocolNot	1.3.6.1.4.1.81.36.2.1.26
ipPolicyRuleL4SrcPortNot	1.3.6.1.4.1.81.36.2.1.27
ipPolicyRuleL4DestPortNot	1.3.6.1.4.1.81.36.2.1.28
ipPolicyRuleIcmpTypeCodeNot	1.3.6.1.4.1.81.36.2.1.29
ipPolicyRuleSrcPolicyUserGroupName	1.3.6.1.4.1.81.36.2.1.30
ipPolicyRuleDstPolicyUserGroupName	1.3.6.1.4.1.81.36.2.1.31
ipPolicyControlSlot	1.3.6.1.4.1.81.36.3.1.1
ipPolicyControlActiveGeneralList	1.3.6.1.4.1.81.36.3.1.2
ipPolicyControlAllowedPolicyManagers	1.3.6.1.4.1.81.36.3.1.3

Object	OID
ipPolicyControlCurrentChecksum	1.3.6.1.4.1.81.36.3.1.4
ipPolicyControlMinimalPolicyManagmentVersion	1.3.6.1.4.1.81.36.3.1.5
ipPolicyControlMaximalPolicyManagmentVersion	1.3.6.1.4.1.81.36.3.1.6
ipPolicyControlMIBversion	1.3.6.1.4.1.81.36.3.1.7
ipPolicyDiffServSlot	1.3.6.1.4.1.81.36.4.1.1
ipPolicyDiffServDSCP	1.3.6.1.4.1.81.36.4.1.2
ipPolicyDiffServOperation	1.3.6.1.4.1.81.36.4.1.3
ipPolicyDiffServName	1.3.6.1.4.1.81.36.4.1.4
ipPolicyDiffServAggIndex	1.3.6.1.4.1.81.36.4.1.5
ipPolicyDiffServApplicabilityPrecedence	1.3.6.1.4.1.81.36.4.1.6
ipPolicyDiffServApplicabilityStatus	1.3.6.1.4.1.81.36.4.1.7
ipPolicyDiffServApplicabilityType	1.3.6.1.4.1.81.36.4.1.8
ipPolicyDiffServErrMsg	1.3.6.1.4.1.81.36.4.1.9
ipPolicyQuerySlot	1.3.6.1.4.1.81.36.5.1.1
ipPolicyQueryListID	1.3.6.1.4.1.81.36.5.1.2
ipPolicyQuerySrcAddr	1.3.6.1.4.1.81.36.5.1.3
ipPolicyQueryDstAddr	1.3.6.1.4.1.81.36.5.1.4
ipPolicyQueryProtocol	1.3.6.1.4.1.81.36.5.1.5
ipPolicyQueryL4SrcPort	1.3.6.1.4.1.81.36.5.1.6
ipPolicyQueryL4DestPort	1.3.6.1.4.1.81.36.5.1.7
ipPolicyQueryEstablished	1.3.6.1.4.1.81.36.5.1.8
ipPolicyQueryDSCP	1.3.6.1.4.1.81.36.5.1.9
ipPolicyQueryOperation	1.3.6.1.4.1.81.36.5.1.10
ipPolicyQueryRuleID	1.3.6.1.4.1.81.36.5.1.11
ipPolicyQueryDSCPOperation	1.3.6.1.4.1.81.36.5.1.12
ipPolicyQueryPriority	1.3.6.1.4.1.81.36.5.1.13
	3 of 6

Object	OID
ipPolicyQueryIfIndex	1.3.6.1.4.1.81.36.5.1.14
ipPolicyQuerySubContext	1.3.6.1.4.1.81.36.5.1.15
ipPolicyQueryEtherTypeType	1.3.6.1.4.1.81.36.5.1.16
ipPolicyQueryEtherTypeTrafficType	1.3.6.1.4.1.81.36.5.1.17
ipPolicyQueryIcmpTypeCode	1.3.6.1.4.1.81.36.5.1.18
ipPolicyDiffServControlSlot	1.3.6.1.4.1.81.36.6.1.1
ipPolicyDiffServControlChecksum	1.3.6.1.4.1.81.36.6.1.2
ipPolicyDiffServControlTrustedFields	1.3.6.1.4.1.81.36.6.1.3
ipPolicyDiffServControlValidityStatus	1.3.6.1.4.1.81.36.6.1.4
ipPolicyDiffServControlErrMsg	1.3.6.1.4.1.81.36.6.1.5
ipPolicyAccessControlViolationEntID	1.3.6.1.4.1.81.36.7.1.1
ipPolicyAccessControlViolationSrcAddr	1.3.6.1.4.1.81.36.7.1.2
ipPolicyAccessControlViolationDstAddr	1.3.6.1.4.1.81.36.7.1.3
ipPolicyAccessControlViolationProtocol	1.3.6.1.4.1.81.36.7.1.4
ipPolicyAccessControlViolationL4SrcPort	1.3.6.1.4.1.81.36.7.1.5
ipPolicyAccessControlViolationL4DstPort	1.3.6.1.4.1.81.36.7.1.6
ipPolicyAccessControlViolationEstablished	1.3.6.1.4.1.81.36.7.1.7
ipPolicyAccessControlViolationDSCP	1.3.6.1.4.1.81.36.7.1.8
ipPolicyAccessControlViolationIfIndex	1.3.6.1.4.1.81.36.7.1.9
ipPolicyAccessControlViolationSubCtxt	1.3.6.1.4.1.81.36.7.1.10
ipPolicyAccessControlViolationTime	1.3.6.1.4.1.81.36.7.1.11
ipPolicyAccessControlViolationRuleType	1.3.6.1.4.1.81.36.7.1.12
ipPolicyCompositeOpEntID	1.3.6.1.4.1.81.36.8.1.1
ipPolicyCompositeOpListID	1.3.6.1.4.1.81.36.8.1.2
ipPolicyCompositeOpID	1.3.6.1.4.1.81.36.8.1.3
ipPolicyCompositeOpName	1.3.6.1.4.1.81.36.8.1.4

Object	OID
ipPolicyCompositeOp802priority	1.3.6.1.4.1.81.36.8.1.5
ipPolicyCompositeOpAccess	1.3.6.1.4.1.81.36.8.1.6
ipPolicyCompositeOpDscp	1.3.6.1.4.1.81.36.8.1.7
ipPolicyCompositeOpRSGQualityClass	1.3.6.1.4.1.81.36.8.1.8
ipPolicyCompositeOpNotify	1.3.6.1.4.1.81.36.8.1.9
ipPolicyCompositeOpRowStatus	1.3.6.1.4.1.81.36.8.1.10
ipPolicyCompositeOpErrorReply	1.3.6.1.4.1.81.36.8.1.11
ipPolicyCompositeOpKeepsState	1.3.6.1.4.1.81.36.8.1.12
ipPolicyDSCPmapEntID	1.3.6.1.4.1.81.36.9.1.1
ipPolicyDSCPmapListID	1.3.6.1.4.1.81.36.9.1.2
ipPolicyDSCPmapDSCP	1.3.6.1.4.1.81.36.9.1.3
ipPolicyDSCPmapOperation	1.3.6.1.4.1.81.36.9.1.4
ipPolicyDSCPmapName	1.3.6.1.4.1.81.36.9.1.5
ipPolicyDSCPmapApplicabilityPrecedence	1.3.6.1.4.1.81.36.9.1.6
ipPolicyDSCPmapApplicabilityStatus	1.3.6.1.4.1.81.36.9.1.7
ipPolicyDSCPmapApplicabilityType	1.3.6.1.4.1.81.36.9.1.8
ipPolicyDSCPmapErrMsg	1.3.6.1.4.1.81.36.9.1.9
ipPolicyActivationEntID	1.3.6.1.4.1.81.36.10.1.1
ipPolicyActivationifIndex	1.3.6.1.4.1.81.36.10.1.2
ipPolicyActivationSubContext	1.3.6.1.4.1.81.36.10.1.3
ipPolicyActivationSubContextName	1.3.6.1.4.1.81.36.10.1.4
ipPolicyActivationList	1.3.6.1.4.1.81.36.10.1.5
ipPolicyActivationAclList	1.3.6.1.4.1.81.36.10.1.6
ipPolicyActivationQoSList	1.3.6.1.4.1.81.36.10.1.7
ipPolicyActivationSourceNatList	1.3.6.1.4.1.81.36.10.1.8
ipPolicyActivationDestinationNatList	1.3.6.1.4.1.81.36.10.1.9

Object	OID
ipPolicyActivationAntiSpoofignList	1.3.6.1.4.1.81.36.10.1.10
ipPolicyActivationPBRList	TBD
ipPolicyValidListEntID	1.3.6.1.4.1.81.36.11.1.1.1
ipPolicyValidListIfIndex	1.3.6.1.4.1.81.36.11.1.1.2
ipPolicyValidListSubContext	1.3.6.1.4.1.81.36.11.1.1.3
ipPolicyValidListListID	1.3.6.1.4.1.81.36.11.1.1.4
ipPolicyValidListStatus	1.3.6.1.4.1.81.36.11.1.1.5
ipPolicyValidListErrMsg	1.3.6.1.4.1.81.36.11.1.1.6
ipPolicyValidListIpOption	1.3.6.1.4.1.81.36.11.1.1.7
ipPolicyValidListIpFragmentation	1.3.6.1.4.1.81.36.11.1.1.8
ipPolicyValidRuleEntID	1.3.6.1.4.1.81.36.11.2.1.1
ipPolicyValidRuleIfIndex	1.3.6.1.4.1.81.36.11.2.1.2
ipPolicyValidRuleSubContext	1.3.6.1.4.1.81.36.11.2.1.3
ipPolicyValidRuleListID	1.3.6.1.4.1.81.36.11.2.1.4
ipPolicyValidRuleRuleID	1.3.6.1.4.1.81.36.11.2.1.5
ipPolicyValidRuleStatus	1.3.6.1.4.1.81.36.11.2.1.6
ipPolicyValidRuleApplicabilityType	1.3.6.1.4.1.81.36.11.2.1.7
ipPolicyValidRuleErrMsg	1.3.6.1.4.1.81.36.11.2.1.8
ipPolicyValidDSCPEntID	1.3.6.1.4.1.81.36.11.3.1.1
ipPolicyValidDSCPIfIndex	1.3.6.1.4.1.81.36.11.3.1.2
ipPolicyValidDSCPSubContext	1.3.6.1.4.1.81.36.11.3.1.3
ipPolicyValidDSCPListID	1.3.6.1.4.1.81.36.11.3.1.4
ipPolicyValidDSCPvalue	1.3.6.1.4.1.81.36.11.3.1.5
ipPolicyValidDSCPStatus	1.3.6.1.4.1.81.36.11.3.1.6
ipPolicyValidDSCPApplicabilityType	1.3.6.1.4.1.81.36.11.3.1.7
ipPolicyValidDSCPErrMsg	1.3.6.1.4.1.81.36.11.3.1.8

The following table provides a list of the MIBs in the BRIDGE-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
dot1dBaseBridgeAddress	1.3.6.1.2.1.17.1.1
dot1dBaseNumPorts	1.3.6.1.2.1.17.1.2
dot1dBaseType	1.3.6.1.2.1.17.1.3
dot1dBasePort	1.3.6.1.2.1.17.1.4.1.1
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2
dot1dBasePortCircuit	1.3.6.1.2.1.17.1.4.1.3
dot1dBasePortDelayExceededDiscards	1.3.6.1.2.1.17.1.4.1.4
dot1dBasePortMtuExceededDiscards	1.3.6.1.2.1.17.1.4.1.5
dot1dStpProtocolSpecification	1.3.6.1.2.1.17.2.1
dot1dStpPriority	1.3.6.1.2.1.17.2.2
dot1dStpTimeSinceTopologyChange	1.3.6.1.2.1.17.2.3
dot1dStpTopChanges	1.3.6.1.2.1.17.2.4
dot1dStpDesignatedRoot	1.3.6.1.2.1.17.2.5
dot1dStpRootCost	1.3.6.1.2.1.17.2.6
dot1dStpRootPort	1.3.6.1.2.1.17.2.7
dot1dStpMaxAge	1.3.6.1.2.1.17.2.8
dot1dStpHelloTime	1.3.6.1.2.1.17.2.9
dot1dStpHoldTime	1.3.6.1.2.1.17.2.10
dot1dStpForwardDelay	1.3.6.1.2.1.17.2.11
dot1dStpBridgeMaxAge	1.3.6.1.2.1.17.2.12
dot1dStpBridgeHelloTime	1.3.6.1.2.1.17.2.13
dot1dStpBridgeForwardDelay	1.3.6.1.2.1.17.2.14
dot1dStpPort	1.3.6.1.2.1.17.2.15.1.1
dot1dStpPortPriority	1.3.6.1.2.1.17.2.15.1.2
dot1dStpPortState	1.3.6.1.2.1.17.2.15.1.3

1 of 2

Object	OID
dot1dStpPortEnable	1.3.6.1.2.1.17.2.15.1.4
dot1dStpPortPathCost	1.3.6.1.2.1.17.2.15.1.5
dot1dStpPortDesignatedRoot	1.3.6.1.2.1.17.2.15.1.6
dot1dStpPortDesignatedCost	1.3.6.1.2.1.17.2.15.1.7
dot1dStpPortDesignatedBridge	1.3.6.1.2.1.17.2.15.1.8
dot1dStpPortDesignatedPort	1.3.6.1.2.1.17.2.15.1.9
dot1dStpPortForwardTransitions	1.3.6.1.2.1.17.2.15.1.10
dot1dTpAgingTime	1.3.6.1.2.1.17.4.2
dot1dTpFdbAddress	1.3.6.1.2.1.17.4.3.1.1
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dTpFdbStatus	1.3.6.1.2.1.17.4.3.1.3
	2 of 2

The following table provides a list of the MIBs in the CONFIG-MIB.MY file that are supported by the G350 and their OIDs:

Object	OID
chHWType	1.3.6.1.4.1.81.7.1
chNumberOfSlots	1.3.6.1.4.1.81.7.2
chReset	1.3.6.1.4.1.81.7.7
chLntAgMaxNmbOfMngrs	1.3.6.1.4.1.81.7.9.3.1
chLntAgPermMngrId	1.3.6.1.4.1.81.7.9.3.2.1.1
chLntAgPermMngrAddr	1.3.6.1.4.1.81.7.9.3.2.1.2
chLntAgMngrTraps	1.3.6.1.4.1.81.7.9.3.2.1.3
chLntAgTrapsPermMngrId	1.3.6.1.4.1.81.7.9.3.7.1.1
chLntAgTrapsId	1.3.6.1.4.1.81.7.9.3.7.1.2
chLntAgTrapsEnableFlag	1.3.6.1.4.1.81.7.9.3.7.1.3
chLntAgMaxTrapsNumber	1.3.6.1.4.1.81.7.9.3.100
	1 of 5

Object	OID
chGroupList	1.3.6.1.4.1.81.7.18
chLogFileGroupId	1.3.6.1.4.1.81.7.22.1.1
chLogFileIndex	1.3.6.1.4.1.81.7.22.1.2
chLogFileName	1.3.6.1.4.1.81.7.22.1.3
chLogFileAbsoluteTime	1.3.6.1.4.1.81.7.22.1.4
chLogFileMessage	1.3.6.1.4.1.81.7.22.1.5
chLogFileEncryptedMessage	1.3.6.1.4.1.81.7.22.1.6
genGroupId	1.3.6.1.4.1.81.8.1.1.1
genGroupSWVersion	1.3.6.1.4.1.81.8.1.1.2
genGroupKernelVersion	1.3.6.1.4.1.81.8.1.1.3
genGroupType	1.3.6.1.4.1.81.8.1.1.4
genGroupDescr	1.3.6.1.4.1.81.8.1.1.5
genGroupNumberOfPorts	1.3.6.1.4.1.81.8.1.1.6
genGroupNumberOfIntPorts	1.3.6.1.4.1.81.8.1.1.7
genGroupReset	1.3.6.1.4.1.81.8.1.1.8
genGroupAutoMan	1.3.6.1.4.1.81.8.1.1.9
genGroupFullConfig	1.3.6.1.4.1.81.8.1.1.10
genGroupRedun12	1.3.6.1.4.1.81.8.1.1.11
genGroupRedun34	1.3.6.1.4.1.81.8.1.1.12
genGroupStandAloneMode	1.3.6.1.4.1.81.8.1.1.14
genGroupInterProcCommStatus	1.3.6.1.4.1.81.8.1.1.15
genGroupCommStatus	1.3.6.1.4.1.81.8.1.1.16
genGroupHWStatus	1.3.6.1.4.1.81.8.1.1.17
genGroupSupplyVoltageFault	1.3.6.1.4.1.81.8.1.1.18
genGroupIntTemp	1.3.6.1.4.1.81.8.1.1.19
genGroupSpecificOID	1.3.6.1.4.1.81.8.1.1.20
	2 of 5

Object	OID
genGroupConfigurationSymbol	1.3.6.1.4.1.81.8.1.1.21
genGroupLastChange	1.3.6.1.4.1.81.8.1.1.22
genGroupRedunRecovery	1.3.6.1.4.1.81.8.1.1.23
genGroupHWVersion	1.3.6.1.4.1.81.8.1.1.24
genGroupHeight	1.3.6.1.4.1.81.8.1.1.25
genGroupWidth	1.3.6.1.4.1.81.8.1.1.26
genGroupIntrusionControl	1.3.6.1.4.1.81.8.1.1.27
genGroupThresholdStatus	1.3.6.1.4.1.81.8.1.1.28
genGroupEavesdropping	1.3.6.1.4.1.81.8.1.1.29
genGroupMainSWVersion	1.3.6.1.4.1.81.8.1.1.30
genGroupMPSActivityStatus	1.3.6.1.4.1.81.8.1.1.31
genGroupBUPSActivityStatus	1.3.6.1.4.1.81.8.1.1.32
genGroupPrepareCounters	1.3.6.1.4.1.81.8.1.1.33
genGroupPortLastChange	1.3.6.1.4.1.81.8.1.1.34
genGroupIntPortLastChange	1.3.6.1.4.1.81.8.1.1.35
genGroupFaultMask	1.3.6.1.4.1.81.8.1.1.36
genGroupTypeName	1.3.6.1.4.1.81.8.1.1.37
genGroupAgentSlot	1.3.6.1.4.1.81.8.1.1.38
genGroupMngType	1.3.6.1.4.1.81.8.1.1.39
genGroupNumberOfLogicalPorts	1.3.6.1.4.1.81.8.1.1.40
genGroupNumberOfInterfaces	1.3.6.1.4.1.81.8.1.1.41
genGroupCascadUpStatus	1.3.6.1.4.1.81.8.1.1.42
genGroupCascadDownStatus	1.3.6.1.4.1.81.8.1.1.43
genGroupSTARootPortID	1.3.6.1.4.1.81.8.1.1.44
genGroupCopyPortInstruction	1.3.6.1.4.1.81.8.1.1.45
genGroupLicenseKey	1.3.6.1.4.1.81.8.1.1.46

Object	OID
genGroupLogFileClear	1.3.6.1.4.1.81.8.1.1.47
genGroupBootVersion	1.3.6.1.4.1.81.8.1.1.48
genGroupResetLastStamp	1.3.6.1.4.1.81.8.1.1.49
genGroupSerialNumber	1.3.6.1.4.1.81.8.1.1.50
genGroupShowModuleInformation	1.3.6.1.4.1.81.8.1.1.51
genGroupCascadingUpFault	1.3.6.1.4.1.81.8.1.1.52
genGroupCascadingDownFault	1.3.6.1.4.1.81.8.1.1.53
genGroupPortClassificationMask	1.3.6.1.4.1.81.8.1.1.54
genGroupPSUType	1.3.6.1.4.1.81.8.1.1.55
genGroupPolicyType	1.3.6.1.4.1.81.8.1.1.56
genPortGroupId	1.3.6.1.4.1.81.9.1.1.1
genPortId	1.3.6.1.4.1.81.9.1.1.2
genPortFunctionality	1.3.6.1.4.1.81.9.1.1.3
genPortType	1.3.6.1.4.1.81.9.1.1.4
genPortDescr	1.3.6.1.4.1.81.9.1.1.5
genPortAdminStatus	1.3.6.1.4.1.81.9.1.1.10
genPortFaultMask	1.3.6.1.4.1.81.9.1.1.14
genPortSWRdFault	1.3.6.1.4.1.81.9.1.1.15
genPortVLANMode	1.3.6.1.4.1.81.9.1.1.19
genPortAdminPermission	1.3.6.1.4.1.81.9.1.1.20
genPortName	1.3.6.1.4.1.81.9.1.1.21
genPortClassification	1.3.6.1.4.1.81.9.1.1.22
genPortVLANBindingMode	1.3.6.1.4.1.81.9.1.1.23
softRedundancyId	1.3.6.1.4.1.81.11.1.1.1
softRedundancyName	1.3.6.1.4.1.81.11.1.1.2
softRedundancyGroupId1	1.3.6.1.4.1.81.11.1.1.3

Object	OID
softRedundancyPortId1	1.3.6.1.4.1.81.11.1.1.4
softRedundancyGroupId2	1.3.6.1.4.1.81.11.1.1.5
softRedundancyPortId2	1.3.6.1.4.1.81.11.1.1.6
softRedundancyStatus	1.3.6.1.4.1.81.11.1.1.7
softRedundancyGlobalStatus	1.3.6.1.4.1.81.11.2
softRedundancyMinTimeBetweenSwitchOvers	1.3.6.1.4.1.81.11.4
softRedundancySwitchBackInterval	1.3.6.1.4.1.81.11.5
	5 of 5

The following table provides a list of the MIBs in the G700-MG-MIB.MY file that are supported by the G350 and their OIDs:

Object	OID
cmgHWType	1.3.6.1.4.1.6889.2.9.1.1.1
cmgModelNumber	1.3.6.1.4.1.6889.2.9.1.1.2
cmgDescription	1.3.6.1.4.1.6889.2.9.1.1.3
cmgSerialNumber	1.3.6.1.4.1.6889.2.9.1.1.4
cmgHWVintage	1.3.6.1.4.1.6889.2.9.1.1.5
cmgHWSuffix	1.3.6.1.4.1.6889.2.9.1.1.6
cmgStackPosition	1.3.6.1.4.1.6889.2.9.1.1.7
cmgModuleList	1.3.6.1.4.1.6889.2.9.1.1.8
cmgReset	1.3.6.1.4.1.6889.2.9.1.1.9
cmgHardwareFaultMask	1.3.6.1.4.1.6889.2.9.1.1.10.12
cmgHardwareStatusMask	1.3.6.1.4.1.6889.2.9.1.1.10.13
cmgModuleSlot	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.1
cmgModuleType	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.2
cmgModuleDescription	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.3
cmgModuleName	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.4
	1 of 5

Object	OID
cmgModuleSerialNumber	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.5
cmgModuleHWVintage	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.6
cmgModuleHWSuffix	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.7
cmgModuleFWVersion	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.8
cmgModuleNumberOfPorts	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.9
cmgModuleFaultMask	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.10
cmgModuleStatusMask	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.11
cmgModuleReset	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.12
cmgModuleNumberOfChannels	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.13
cmgGatewayNumber	1.3.6.1.4.1.6889.2.9.1.2.1.1
cmgMACAddress	1.3.6.1.4.1.6889.2.9.1.2.1.2
cmgFWVersion	1.3.6.1.4.1.6889.2.9.1.2.1.3
cmgCurrentIpAddress	1.3.6.1.4.1.6889.2.9.1.2.1.4
cmgMgpFaultMask	1.3.6.1.4.1.6889.2.9.1.2.1.15
cmgQosControl	1.3.6.1.4.1.6889.2.9.1.2.2.1
cmgRemoteSigDscp	1.3.6.1.4.1.6889.2.9.1.2.2.2
cmgRemoteSig802Priority	1.3.6.1.4.1.6889.2.9.1.2.2.3
cmgLocalSigDscp	1.3.6.1.4.1.6889.2.9.1.2.2.4
cmgLocalSig802Priority	1.3.6.1.4.1.6889.2.9.1.2.2.5
cmgStatic802Vlan	1.3.6.1.4.1.6889.2.9.1.2.2.6
cmgCurrent802Vlan	1.3.6.1.4.1.6889.2.9.1.2.2.7
cmgPrimaryClockSource	1.3.6.1.4.1.6889.2.9.1.2.3.1
cmgSecondaryClockSource	1.3.6.1.4.1.6889.2.9.1.2.3.2
cmgActiveClockSource	1.3.6.1.4.1.6889.2.9.1.2.3.3
cmgRegistrationState	1.3.6.1.4.1.6889.2.9.1.3.1
cmgActiveControllerAddress	1.3.6.1.4.1.6889.2.9.1.3.2
	2 of 5

Object	OID
cmgH248LinkStatus	1.3.6.1.4.1.6889.2.9.1.3.3
cmgH248LinkErrorCode	1.3.6.1.4.1.6889.2.9.1.3.4
cmgUseDhcpForMgcList	1.3.6.1.4.1.6889.2.9.1.3.5
cmgStaticControllerHosts	1.3.6.1.4.1.6889.2.9.1.3.6
cmgDhcpControllerHosts	1.3.6.1.4.1.6889.2.9.1.3.7
cmgVoipEngineUseDhcp	1.3.6.1.4.1.6889.2.9.1.4.1
cmgVoipQosControl	1.3.6.1.4.1.6889.2.9.1.4.2
cmgVoipRemoteBbeDscp	1.3.6.1.4.1.6889.2.9.1.4.3.1.1
cmgVoipRemoteEfDscp	1.3.6.1.4.1.6889.2.9.1.4.3.1.2
cmgVoipRemote802Priority	1.3.6.1.4.1.6889.2.9.1.4.3.1.3
cmgVoipRemoteMinRtpPort	1.3.6.1.4.1.6889.2.9.1.4.3.1.4
cmgVoipRemoteMaxRtpPort	1.3.6.1.4.1.6889.2.9.1.4.3.1.5
cmgVoipRemoteRtcpEnabled	1.3.6.1.4.1.6889.2.9.1.4.3.2.1
cmgVoipRemoteRtcpMonitorIpAddress	1.3.6.1.4.1.6889.2.9.1.4.3.2.2
cmgVoipRemoteRtcpMonitorPort	1.3.6.1.4.1.6889.2.9.1.4.3.2.3
cmgVoipRemoteRtcpReportPeriod	1.3.6.1.4.1.6889.2.9.1.4.3.2.4
cmgVoipRemoteRsvpEnabled	1.3.6.1.4.1.6889.2.9.1.4.3.3.1
cmgVoipRemoteRetryOnFailure	1.3.6.1.4.1.6889.2.9.1.4.3.3.2
cmgVoipRemoteRetryDelay	1.3.6.1.4.1.6889.2.9.1.4.3.3.3
cmgVoipRemoteRsvpProfile	1.3.6.1.4.1.6889.2.9.1.4.3.3.4
cmgVoipLocalBbeDscp	1.3.6.1.4.1.6889.2.9.1.4.4.1.1
cmgVoipLocalEfDscp	1.3.6.1.4.1.6889.2.9.1.4.4.1.2
cmgVoipLocal802Priority	1.3.6.1.4.1.6889.2.9.1.4.4.1.3
cmgVoipLocalMinRtpPort	1.3.6.1.4.1.6889.2.9.1.4.4.1.4
cmgVoipLocalMaxRtpPort	1.3.6.1.4.1.6889.2.9.1.4.4.1.5
cmgVoipLocalRtcpEnabled	1.3.6.1.4.1.6889.2.9.1.4.4.2.1

Object	OID
cmgVoipLocalRtcpMonitorIpAddress	1.3.6.1.4.1.6889.2.9.1.4.4.2.2
cmgVoipLocalRtcpMonitorPort	1.3.6.1.4.1.6889.2.9.1.4.4.2.3
cmgVoipLocalRtcpReportPeriod	1.3.6.1.4.1.6889.2.9.1.4.4.2.4
cmgVoipLocalRsvpEnabled	1.3.6.1.4.1.6889.2.9.1.4.4.3.1
cmgVoipLocalRetryOnFailure	1.3.6.1.4.1.6889.2.9.1.4.4.3.2
cmgVoipLocalRetryDelay	1.3.6.1.4.1.6889.2.9.1.4.4.3.3
cmgVoipLocalRsvpProfile	1.3.6.1.4.1.6889.2.9.1.4.4.3.4
cmgVoipSlot	1.3.6.1.4.1.6889.2.9.1.4.5.1.1
cmgVoipMACAddress	1.3.6.1.4.1.6889.2.9.1.4.5.1.2
cmgVoipStaticIpAddress	1.3.6.1.4.1.6889.2.9.1.4.5.1.3
cmgVoipCurrentIpAddress	1.3.6.1.4.1.6889.2.9.1.4.5.1.4
cmgVoipJitterBufferSize	1.3.6.1.4.1.6889.2.9.1.4.5.1.5
cmgVoipTotalChannels	1.3.6.1.4.1.6889.2.9.1.4.5.1.6
cmgVoipChannelsInUse	1.3.6.1.4.1.6889.2.9.1.4.5.1.7
cmgVoipAverageOccupancy	1.3.6.1.4.1.6889.2.9.1.4.5.1.8
cmgVoipHyperactivity	1.3.6.1.4.1.6889.2.9.1.4.5.1.9
cmgVoipAdminState	1.3.6.1.4.1.6889.2.9.1.4.5.1.10
cmgVoipDspFWVersion	1.3.6.1.4.1.6889.2.9.1.4.5.1.11
cmgVoipDspStatus	1.3.6.1.4.1.6889.2.9.1.4.5.1.12
cmgVoipEngineReset	1.3.6.1.4.1.6889.2.9.1.4.5.1.13
cmgVoipFaultMask	1.3.6.1.4.1.6889.2.9.1.4.5.1.14
cmgCcModule	1.3.6.1.4.1.6889.2.9.1.6.1.1.1
cmgCcPort	1.3.6.1.4.1.6889.2.9.1.6.1.1.2
cmgCcRelay	1.3.6.1.4.1.6889.2.9.1.6.1.1.3
cmgCcAdminState	1.3.6.1.4.1.6889.2.9.1.6.1.1.4
cmgCcPulseDuration	1.3.6.1.4.1.6889.2.9.1.6.1.1.5
	4 of 5

Object	OID
cmgCcStatus	1.3.6.1.4.1.6889.2.9.1.6.1.1.6
cmgEtrModule	1.3.6.1.4.1.6889.2.9.1.7.1.1.1
cmgEtrAdminState	1.3.6.1.4.1.6889.2.9.1.7.1.1.2
cmgEtrNumberOfPairs	1.3.6.1.4.1.6889.2.9.1.7.1.1.3
cmgEtrStatus	1.3.6.1.4.1.6889.2.9.1.7.1.1.4
cmgEtrCurrentLoopDetect	1.3.6.1.4.1.6889.2.9.1.7.1.1.5
cmgDynCacStatus	1.3.6.1.4.1.6889.2.9.1.8.1
cmgDynCacRBBL	1.3.6.1.4.1.6889.2.9.1.8.2
cmgDynCacLastUpdate	1.3.6.1.4.1.6889.2.9.1.8.3
	5 of 5

The following table provides a list of the MIBs in the FRAME-RELAY-DTE-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
frDlcmiIfIndex	1.3.6.1.2.1.10.32.1.1.1
frDlcmiState	1.3.6.1.2.1.10.32.1.1.2
frDlcmiAddress	1.3.6.1.2.1.10.32.1.1.3
frDlcmiAddressLen	1.3.6.1.2.1.10.32.1.1.4
frDlcmiPollingInterval	1.3.6.1.2.1.10.32.1.1.5
frDlcmiFullEnquiryInterval	1.3.6.1.2.1.10.32.1.1.6
frDlcmiErrorThreshold	1.3.6.1.2.1.10.32.1.1.7
frDlcmiMonitoredEvents	1.3.6.1.2.1.10.32.1.1.8
frDlcmiMaxSupportedVCs	1.3.6.1.2.1.10.32.1.1.9
frDlcmiMulticast	1.3.6.1.2.1.10.32.1.1.10
frDlcmiStatus	1.3.6.1.2.1.10.32.1.1.11
frDlcmiRowStatus	1.3.6.1.2.1.10.32.1.1.12
frCircuitIfIndex	1.3.6.1.2.1.10.32.2.1.1
	1 of 3

Object	OID
frCircuitDlci	1.3.6.1.2.1.10.32.2.1.2
frCircuitState	1.3.6.1.2.1.10.32.2.1.3
frCircuitReceivedFECNs	1.3.6.1.2.1.10.32.2.1.4
frCircuitReceivedBECNs	1.3.6.1.2.1.10.32.2.1.5
frCircuitSentFrames	1.3.6.1.2.1.10.32.2.1.6
frCircuitSentOctets	1.3.6.1.2.1.10.32.2.1.7
frCircuitReceivedFrames	1.3.6.1.2.1.10.32.2.1.8
frCircuitReceivedOctets	1.3.6.1.2.1.10.32.2.1.9
frCircuitCreationTime	1.3.6.1.2.1.10.32.2.1.10
frCircuitLastTimeChange	1.3.6.1.2.1.10.32.2.1.11
frCircuitCommittedBurst	1.3.6.1.2.1.10.32.2.1.12
frCircuitExcessBurst	1.3.6.1.2.1.10.32.2.1.13
frCircuitThroughput	1.3.6.1.2.1.10.32.2.1.14
frCircuitMulticast	1.3.6.1.2.1.10.32.2.1.15
frCircuitType	1.3.6.1.2.1.10.32.2.1.16
frCircuitDiscards	1.3.6.1.2.1.10.32.2.1.17
frCircuitReceivedDEs	1.3.6.1.2.1.10.32.2.1.18
frCircuitSentDEs	1.3.6.1.2.1.10.32.2.1.19
frCircuitLogicalIfIndex	1.3.6.1.2.1.10.32.2.1.20
frCircuitRowStatus	1.3.6.1.2.1.10.32.2.1.21
frErrIfIndex	1.3.6.1.2.1.10.32.3.1.1
frErrType	1.3.6.1.2.1.10.32.3.1.2
frErrData	1.3.6.1.2.1.10.32.3.1.3
frErrTime	1.3.6.1.2.1.10.32.3.1.4
frErrFaults	1.3.6.1.2.1.10.32.3.1.5
frErrFaultTime	1.3.6.1.2.1.10.32.3.1.6

Object	OID
frTrapState	1.3.6.1.2.1.10.32.4.1
frTrapMaxRate	1.3.6.1.2.1.10.32.4.2
	3 of 3

The following table provides a list of the MIBs in the IP-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
ipForwarding	1.3.6.1.2.1.4.1
ipDefaultTTL	1.3.6.1.2.1.4.2
ipInReceives	1.3.6.1.2.1.4.3
ipInHdrErrors	1.3.6.1.2.1.4.4
ipInAddrErrors	1.3.6.1.2.1.4.5
ipForwDatagrams	1.3.6.1.2.1.4.6
ipInUnknownProtos	1.3.6.1.2.1.4.7
ipInDiscards	1.3.6.1.2.1.4.8
ipInDelivers	1.3.6.1.2.1.4.9
ipOutRequests	1.3.6.1.2.1.4.10
ipOutDiscards	1.3.6.1.2.1.4.11
ipOutNoRoutes	1.3.6.1.2.1.4.12
ipReasmTimeout	1.3.6.1.2.1.4.13
ipReasmReqds	1.3.6.1.2.1.4.14
ipReasmOKs	1.3.6.1.2.1.4.15
ipReasmFails	1.3.6.1.2.1.4.16
ipFragOKs	1.3.6.1.2.1.4.17
ipFragFails	1.3.6.1.2.1.4.18
ipFragCreates	1.3.6.1.2.1.4.19
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1
	1 of 2

Object	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipAdEntBcastAddr	1.3.6.1.2.1.4.20.1.4
ipAdEntReasmMaxSize	1.3.6.1.2.1.4.20.1.5
ipNetToMediaIfIndex	1.3.6.1.2.1.4.22.1.1
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToMediaNetAddress	1.3.6.1.2.1.4.22.1.3
ipNetToMediaType	1.3.6.1.2.1.4.22.1.4
ipRoutingDiscards	1.3.6.1.2.1.4.23
	2 of 2

The following table provides a list of the MIBs in the Load12-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
genOpModuleId	1.3.6.1.4.1.1751.2.53.1.2.1.1
genOpIndex	1.3.6.1.4.1.1751.2.53.1.2.1.2
genOpRunningState	1.3.6.1.4.1.1751.2.53.1.2.1.3
genOpSourceIndex	1.3.6.1.4.1.1751.2.53.1.2.1.4
genOpDestIndex	1.3.6.1.4.1.1751.2.53.1.2.1.5
genOpServerIP	1.3.6.1.4.1.1751.2.53.1.2.1.6
genOpUserName	1.3.6.1.4.1.1751.2.53.1.2.1.7
genOpPassword	1.3.6.1.4.1.1751.2.53.1.2.1.8
genOpProtocolType	1.3.6.1.4.1.1751.2.53.1.2.1.9
genOpFileName	1.3.6.1.4.1.1751.2.53.1.2.1.10
genOpRunningStateDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.11
genOpLastFailureIndex	1.3.6.1.4.1.1751.2.53.1.2.1.12
genOpLastFailureDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.13
	1 of 2

Object	OID
genOpLastWarningDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.14
genOpErrorLogIndex	1.3.6.1.4.1.1751.2.53.1.2.1.15
genOpResetSupported	1.3.6.1.4.1.1751.2.53.1.2.1.16
genOpEnableReset	1.3.6.1.4.1.1751.2.53.1.2.1.17
genOpNextBootImageIndex	1.3.6.1.4.1.1751.2.53.1.2.1.18
genOpLastBootImageIndex	1.3.6.1.4.1.1751.2.53.1.2.1.19
genOpFileSystemType	1.3.6.1.4.1.1751.2.53.1.2.1.20
genOpReportSpecificFlags	1.3.6.1.4.1.1751.2.53.1.2.1.21
genOpOctetsReceived	1.3.6.1.4.1.1751.2.53.1.2.1.22
genAppFileId	1.3.6.1.4.1.1751.2.53.2.1.1.1
genAppFileName	1.3.6.1.4.1.1751.2.53.2.1.1.2
genAppFileType	1.3.6.1.4.1.1751.2.53.2.1.1.3
genAppFileDescription	1.3.6.1.4.1.1751.2.53.2.1.1.4
genAppFileSize	1.3.6.1.4.1.1751.2.53.2.1.1.5
genAppFileVersionNumber	1.3.6.1.4.1.1751.2.53.2.1.1.6
genAppFileLocation	1.3.6.1.4.1.1751.2.53.2.1.1.7
genAppFileDateStamp	1.3.6.1.4.1.1751.2.53.2.1.1.8
genAppFileRowStatus	1.3.6.1.4.1.1751.2.53.2.1.1.9
	2 of 2

The following table provides a list of the MIBs in the PPP-LCP-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
pppLinkStatusPhysicalIndex	1.3.6.1.2.1.10.23.1.1.1.1.1
pppLinkStatusBadAddresses	1.3.6.1.2.1.10.23.1.1.1.1.2
pppLinkStatusBadControls	1.3.6.1.2.1.10.23.1.1.1.1.3
pppLinkStatusPacketTooLongs	1.3.6.1.2.1.10.23.1.1.1.1.4
	1 of 2

Object	OID
pppLinkStatusBadFCSs	1.3.6.1.2.1.10.23.1.1.1.1.5
pppLinkStatusLocalMRU	1.3.6.1.2.1.10.23.1.1.1.1.6
pppLinkStatusRemoteMRU	1.3.6.1.2.1.10.23.1.1.1.1.7
pppLinkStatusLocalToPeerACCMap	1.3.6.1.2.1.10.23.1.1.1.1.8
pppLinkStatusPeerToLocalACCMap	1.3.6.1.2.1.10.23.1.1.1.1.9
pppLinkStatusLocalToRemoteACCompression	1.3.6.1.2.1.10.23.1.1.1.1.12
pppLinkStatusRemoteToLocalACCompression	1.3.6.1.2.1.10.23.1.1.1.1.13
pppLinkStatusTransmitFcsSize	1.3.6.1.2.1.10.23.1.1.1.1.14
pppLinkStatusReceiveFcsSize	1.3.6.1.2.1.10.23.1.1.1.1.15
pppLinkConfigInitialMRU	1.3.6.1.2.1.10.23.1.1.2.1.1
pppLinkConfigReceiveACCMap	1.3.6.1.2.1.10.23.1.1.2.1.2
pppLinkConfigTransmitACCMap	1.3.6.1.2.1.10.23.1.1.2.1.3
pppLinkConfigMagicNumber	1.3.6.1.2.1.10.23.1.1.2.1.4
pppLinkConfigFcsSize	1.3.6.1.2.1.10.23.1.1.2.1.5
	2 of 2

The following table provides a list of the MIBs in the WAN-MIB.MY file that are supported by the G350 and their OIDs:

Object	OID
ds0BundleMemmbersList	1.3.6.1.4.1.6889.2.1.6.1.1.2.1.1
ds0BundleSpeedFactor	1.3.6.1.4.1.6889.2.1.6.1.1.2.1.2
ds1DeviceMode	1.3.6.1.4.1.6889.2.1.6.2.1.1
ifTableXtndIndex	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.1
ifTableXtndPeerAddress	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.2
ifTableXtndVoIPQueue	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.3
ifTableXtndCableLength	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.4
ifTableXtndGain	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.5
	1 of 3

Object	OID
ifTableXtndDescription	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.6
ifTableXtndKeepAlive	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.7
ifTableXtndMtu	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.8
ifTableXtndInvertTxClock	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.9
ifTableXtndDTELoopback	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.10
ifTableXtndIgnoreDCD	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.11
ifTableXtndIdleChars	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.12
ifTableXtndBandwidth	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.13
ifTableXtndEncapsulation	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.14
ifTableXtndOperStatus	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.15
ifTableXtndBackupCapabilities	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.16
ifTableXtndBackupIf	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.17
ifTableXtndBackupEnableDelay	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.18
ifTableXtndBackupDisableDelay	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.19
ifTableXtndPrimaryIf	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.20
ifTableXtndCarrierDelay	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.21
ifTableXtndDtrRestartDelay	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.22
ifTableXtndDtrPulseTime	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.23
ifTableXtndLoadInterval	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.24
ifTableXtndInputRate	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.25
ifTableXtndOutputRate	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.26
ifTableXtndInputLoad	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.27
ifTableXtndOutputLoad	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.28
ifTableXtndReliability	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.29
ifTableXtndCacBBL	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.31
ifTableXtndCacPriority	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.32

2 of 3

Object	OID
ifTableXtndCacifStatus	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.33
frDlcmiXtndIndex	1.3.6.1.4.1.6889.2.1.6.2.4.1.1.1
frDlcmiXtndLMIAutoSense	1.3.6.1.4.1.6889.2.1.6.2.4.1.1.2
frStaticCircuitSubIfIndex	1.3.6.1.4.1.6889.2.1.6.2.4.2.1.1
frStaticCircuitDLCI	1.3.6.1.4.1.6889.2.1.6.2.4.2.1.2
frStaticCircuitDLCIrole	1.3.6.1.4.1.6889.2.1.6.2.4.2.1.3
frStaticCircuitStatus	1.3.6.1.4.1.6889.2.1.6.2.4.2.1.4
frSubIfDlcmiIndex	1.3.6.1.4.1.6889.2.1.6.2.4.3.1.1
frSubIfSubIndex	1.3.6.1.4.1.6889.2.1.6.2.4.3.1.2
frSubIfType	1.3.6.1.4.1.6889.2.1.6.2.4.3.1.3
frSubIfStatus	1.3.6.1.4.1.6889.2.1.6.2.4.3.1.4
	3 of 3

The following table provides a list of the MIBs in the SNMPv2-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
sysDescr	1.3.6.1.2.1.1.1
sysObjectID	1.3.6.1.2.1.1.2
sysUpTime	1.3.6.1.2.1.1.3
sysContact	1.3.6.1.2.1.1.4
sysName	1.3.6.1.2.1.1.5
sysLocation	1.3.6.1.2.1.1.6
sysServices	1.3.6.1.2.1.1.7
snmpInPkts	1.3.6.1.2.1.11.1
snmpInBadVersions	1.3.6.1.2.1.11.3
snmpInBadCommunityNames	1.3.6.1.2.1.11.4
snmpInBadCommunityUses	1.3.6.1.2.1.11.5
	1 of 2

Object	OID
snmpInASNParseErrs	1.3.6.1.2.1.11.6
snmpEnableAuthenTraps	1.3.6.1.2.1.11.30
snmpOutPkts	1.3.6.1.2.1.11.2
snmpInTooBigs	1.3.6.1.2.1.11.8
snmpInNoSuchNames	1.3.6.1.2.1.11.9
snmpInBadValues	1.3.6.1.2.1.11.10
snmpInReadOnlys	1.3.6.1.2.1.11.11
snmpInGenErrs	1.3.6.1.2.1.11.12
snmpInTotalReqVars	1.3.6.1.2.1.11.13
snmpInTotalSetVars	1.3.6.1.2.1.11.14
snmpInGetRequests	1.3.6.1.2.1.11.15
snmpInGetNexts	1.3.6.1.2.1.11.16
snmpInSetRequests	1.3.6.1.2.1.11.17
snmpInGetResponses	1.3.6.1.2.1.11.18
snmpInTraps	1.3.6.1.2.1.11.19
snmpOutTooBigs	1.3.6.1.2.1.11.20
snmpOutNoSuchNames	1.3.6.1.2.1.11.21
snmpOutBadValues	1.3.6.1.2.1.11.22
snmpOutGenErrs	1.3.6.1.2.1.11.24
snmpOutGetRequests	1.3.6.1.2.1.11.25
snmpOutGetNexts	1.3.6.1.2.1.11.26
snmpOutSetRequests	1.3.6.1.2.1.11.27
snmpOutGetResponses	1.3.6.1.2.1.11.28
snmpOutTraps	1.3.6.1.2.1.11.29
	2 of 2

The following table provides a list of the MIBs in the OSPF-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
ospfRouterId	1.3.6.1.2.1.14.1.1
ospfAdminStat	1.3.6.1.2.1.14.1.2
ospfVersionNumber	1.3.6.1.2.1.14.1.3
ospfAreaBdrRtrStatus	1.3.6.1.2.1.14.1.4
ospfASBdrRtrStatus	1.3.6.1.2.1.14.1.5
ospfExternLsaCount	1.3.6.1.2.1.14.1.6
ospfExternLsaCksumSum	1.3.6.1.2.1.14.1.7
ospfTOSSupport	1.3.6.1.2.1.14.1.8
ospfOriginateNewLsas	1.3.6.1.2.1.14.1.9
ospfRxNewLsas	1.3.6.1.2.1.14.1.10
ospfExtLsdbLimit	1.3.6.1.2.1.14.1.11
ospfMulticastExtensions	1.3.6.1.2.1.14.1.12
ospfExitOverflowInterval	1.3.6.1.2.1.14.1.13
ospfDemandExtensions	1.3.6.1.2.1.14.1.14
ospfAreaId	1.3.6.1.2.1.14.2.1.1
ospfAuthType	1.3.6.1.2.1.14.2.1.2
ospfImportAsExtern	1.3.6.1.2.1.14.2.1.3
ospfSpfRuns	1.3.6.1.2.1.14.2.1.4
ospfAreaBdrRtrCount	1.3.6.1.2.1.14.2.1.5
ospfAsBdrRtrCount	1.3.6.1.2.1.14.2.1.6
ospfAreaLsaCount	1.3.6.1.2.1.14.2.1.7
ospfAreaLsaCksumSum	1.3.6.1.2.1.14.2.1.8
ospfAreaSummary	1.3.6.1.2.1.14.2.1.9
ospfAreaStatus	1.3.6.1.2.1.14.2.1.10
ospfLsdbAreaId	1.3.6.1.2.1.14.4.1.1

1 of 3

Object	OID
ospfLsdbType	1.3.6.1.2.1.14.4.1.2
ospfLsdbLsid	1.3.6.1.2.1.14.4.1.3
ospfLsdbRouterId	1.3.6.1.2.1.14.4.1.4
ospfLsdbSequence	1.3.6.1.2.1.14.4.1.5
ospfLsdbAge	1.3.6.1.2.1.14.4.1.6
ospfLsdbChecksum	1.3.6.1.2.1.14.4.1.7
ospfLsdbAdvertisement	1.3.6.1.2.1.14.4.1.8
ospfIfIpAddress	1.3.6.1.2.1.14.7.1.1
ospfAddressLessIf	1.3.6.1.2.1.14.7.1.2
ospfIfAreaId	1.3.6.1.2.1.14.7.1.3
ospfIfType	1.3.6.1.2.1.14.7.1.4
ospfIfAdminStat	1.3.6.1.2.1.14.7.1.5
ospfIfRtrPriority	1.3.6.1.2.1.14.7.1.6
ospfIfTransitDelay	1.3.6.1.2.1.14.7.1.7
ospfIfRetransInterval	1.3.6.1.2.1.14.7.1.8
ospfIfHelloInterval	1.3.6.1.2.1.14.7.1.9
ospfIfRtrDeadInterval	1.3.6.1.2.1.14.7.1.10
ospfIfPollInterval	1.3.6.1.2.1.14.7.1.11
ospfIfState	1.3.6.1.2.1.14.7.1.12
ospfIfDesignatedRouter	1.3.6.1.2.1.14.7.1.13
ospfIfBackupDesignatedRouter	1.3.6.1.2.1.14.7.1.14
ospfIfEvents	1.3.6.1.2.1.14.7.1.15
ospfIfAuthKey	1.3.6.1.2.1.14.7.1.16
ospfIfStatus	1.3.6.1.2.1.14.7.1.17
ospfIfMulticastForwarding	1.3.6.1.2.1.14.7.1.18
ospfIfDemand	1.3.6.1.2.1.14.7.1.19

Object	OID
ospfIfAuthType	1.3.6.1.2.1.14.7.1.20
ospfIfMetricIpAddress	1.3.6.1.2.1.14.8.1.1
ospfIfMetricAddressLessIf	1.3.6.1.2.1.14.8.1.2
ospfIfMetricTOS	1.3.6.1.2.1.14.8.1.3
ospfIfMetricValue	1.3.6.1.2.1.14.8.1.4
ospfIfMetricStatus	1.3.6.1.2.1.14.8.1.5
ospfNbrIpAddr	1.3.6.1.2.1.14.10.1.1
ospfNbrAddressLessIndex	1.3.6.1.2.1.14.10.1.2
ospfNbrRtrId	1.3.6.1.2.1.14.10.1.3
ospfNbrOptions	1.3.6.1.2.1.14.10.1.4
ospfNbrPriority	1.3.6.1.2.1.14.10.1.5
ospfNbrState	1.3.6.1.2.1.14.10.1.6
ospfNbrEvents	1.3.6.1.2.1.14.10.1.7
ospfNbrLsRetransQLen	1.3.6.1.2.1.14.10.1.8
ospfNbmaNbrStatus	1.3.6.1.2.1.14.10.1.9
ospfNbmaNbrPermanence	1.3.6.1.2.1.14.10.1.10
ospfNbrHelloSuppressed	1.3.6.1.2.1.14.10.1.11
ospfExtLsdbType	1.3.6.1.2.1.14.12.1.1
ospfExtLsdbLsid	1.3.6.1.2.1.14.12.1.2
ospfExtLsdbRouterId	1.3.6.1.2.1.14.12.1.3
ospfExtLsdbSequence	1.3.6.1.2.1.14.12.1.4
ospfExtLsdbAge	1.3.6.1.2.1.14.12.1.5
ospfExtLsdbChecksum	1.3.6.1.2.1.14.12.1.6
ospfExtLsdbAdvertisement	1.3.6.1.2.1.14.12.1.7
	3 of 3

The following table provides a list of the MIBs in the TUNNEL-MIB.my file that are supported by the G350 and their OIDs:

Object	OID
tunnelIfLocalAddress	1.3.6.1.2.1.10.131.1.1.1.1.1
tunnelIfRemoteAddress	1.3.6.1.2.1.10.131.1.1.1.1.2
tunnelIfEncapsMethod	1.3.6.1.2.1.10.131.1.1.1.1.3
tunnelIfTOS	1.3.6.1.2.1.10.131.1.1.1.1.4
tunnelIfHopLimit	1.3.6.1.2.1.10.131.1.1.1.1.5
tunnelConfigLocalAddress	1.3.6.1.2.1.10.131.1.1.2.1.1
tunnelConfigRemoteAddress	1.3.6.1.2.1.10.131.1.1.2.1.2
tunnelConfigEncapsMethod	1.3.6.1.2.1.10.131.1.1.2.1.3
tunnelConfigID	1.3.6.1.2.1.10.131.1.1.2.1.4
tunnelConfigStatus	1.3.6.1.2.1.10.131.1.1.2.1.5
ipTunnelIfIndex	1.3.6.1.4.1.81.31.8.1.1.1
ipTunnelIfChecksum	1.3.6.1.4.1.81.31.8.1.1.2
ipTunnelIfKey	1.3.6.1.4.1.81.31.8.1.1.3
ipTunnelIfkeyMode	1.3.6.1.4.1.81.31.8.1.1.4
ipTunnelIfAgingTimer	1.3.6.1.4.1.81.31.8.1.1.5
ipTunnelIfMTUDiscovery	1.3.6.1.4.1.81.31.8.1.1.6
ipTunnelIfMTU	1.3.6.1.4.1.81.31.8.1.1.7
ipTunnelIfKeepaliveRate	1.3.6.1.4.1.81.31.8.1.1.8
ipTunnelIfKeepaliveRetries	1.3.6.1.4.1.81.31.8.1.1.9

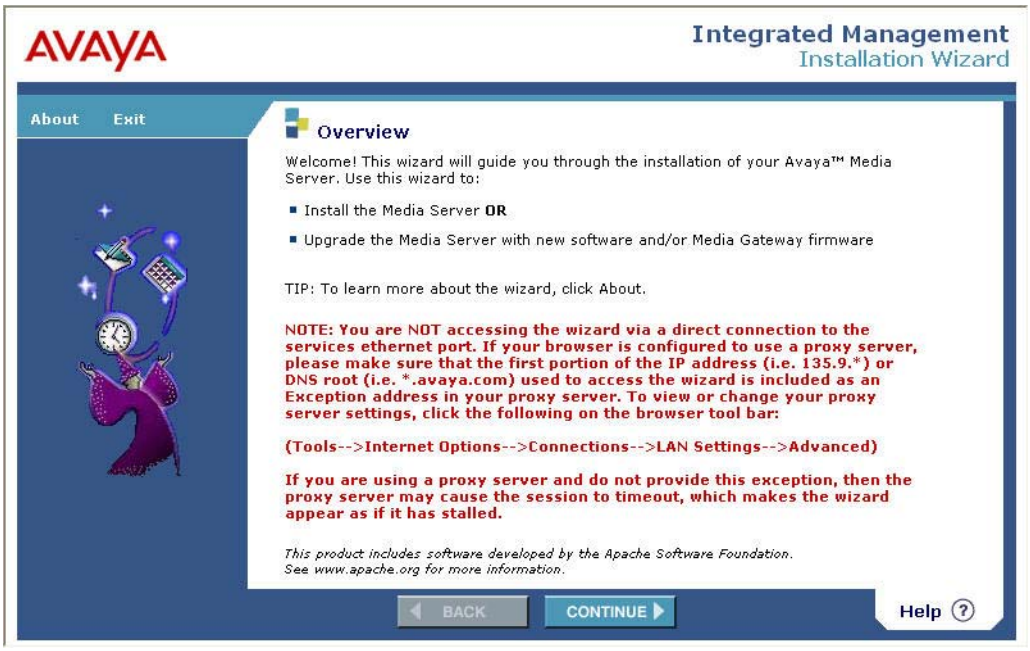
Appendix B: Configuring the G350 using the Avaya IW

This chapter explains how to configure the Avaya G350 Media Gateway using the Avaya Installation Wizard (Avaya IW). The Avaya IW is a web-based installation wizard that is used with the Avaya G350 Media Gateway to perform initial configuration tasks and to upgrade software and firmware. The Avaya IW is designed for use with systems that contain an S8300 Media Server, operating in either ICC or LSP mode. For instructions on accessing the Avaya IW, see Accessing Avaya IW on page 32.

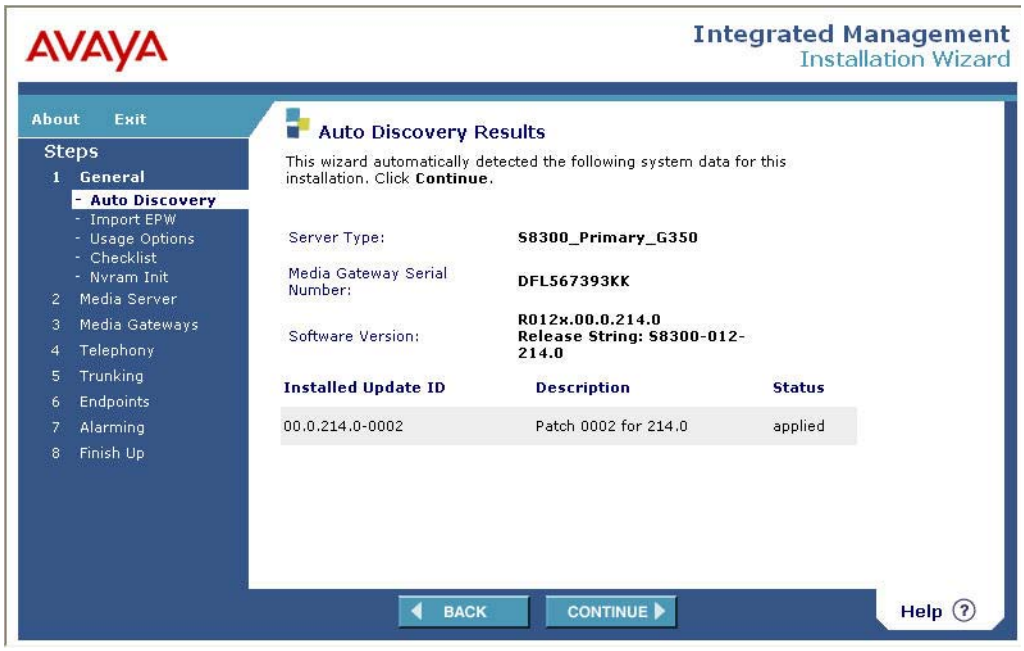
Preliminary screens

View the preliminary screens:

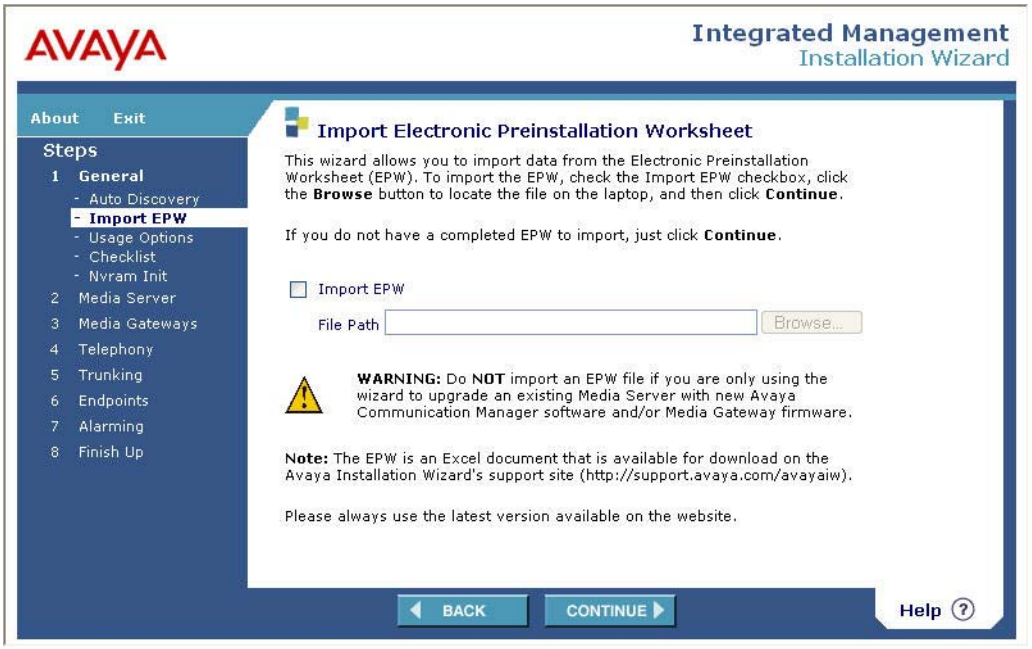
1. When you access the Avaya IW, the first screen that appears is the Overview screen:



2. Click **Continue**. The Avaya IW performs system auto-discovery and displays the results on the following screen:



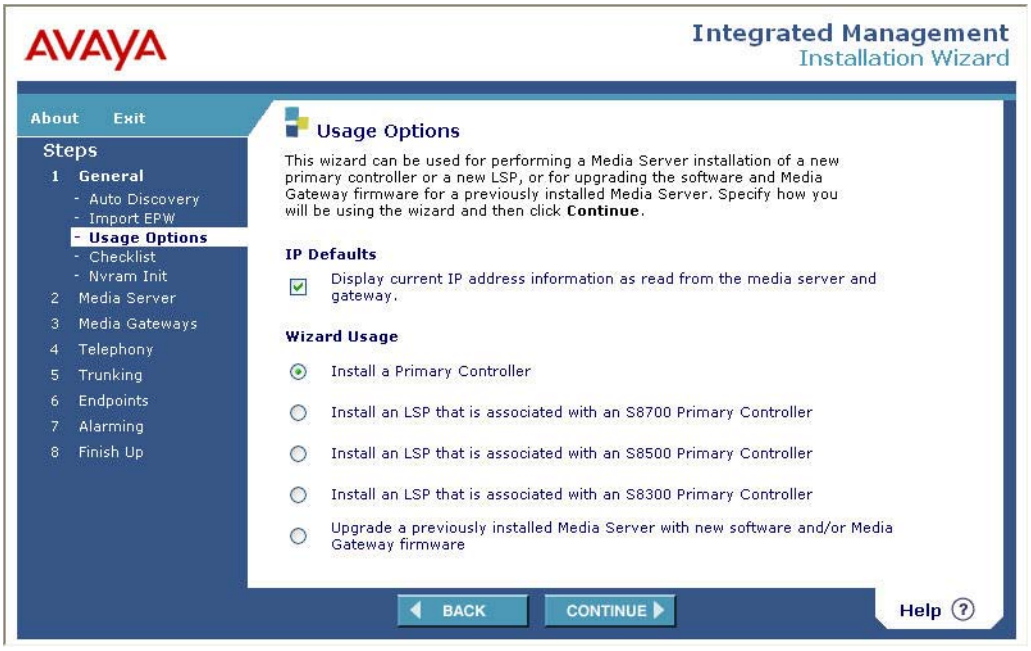
3. Click **Continue**. The Import Electronic PreInstallation Worksheet screen appears. This screen allows you to import system data from the Electronic PreInstallation Worksheet (EPW). The EPW is described in *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.



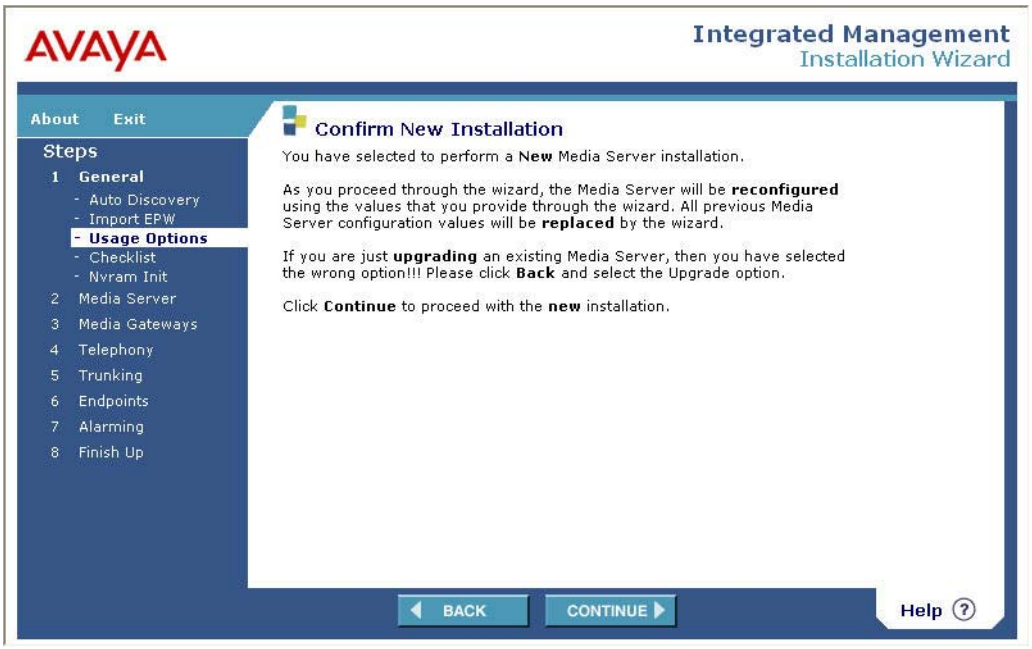
MGC configuration and upgrade

For MGC configuration and upgrade:

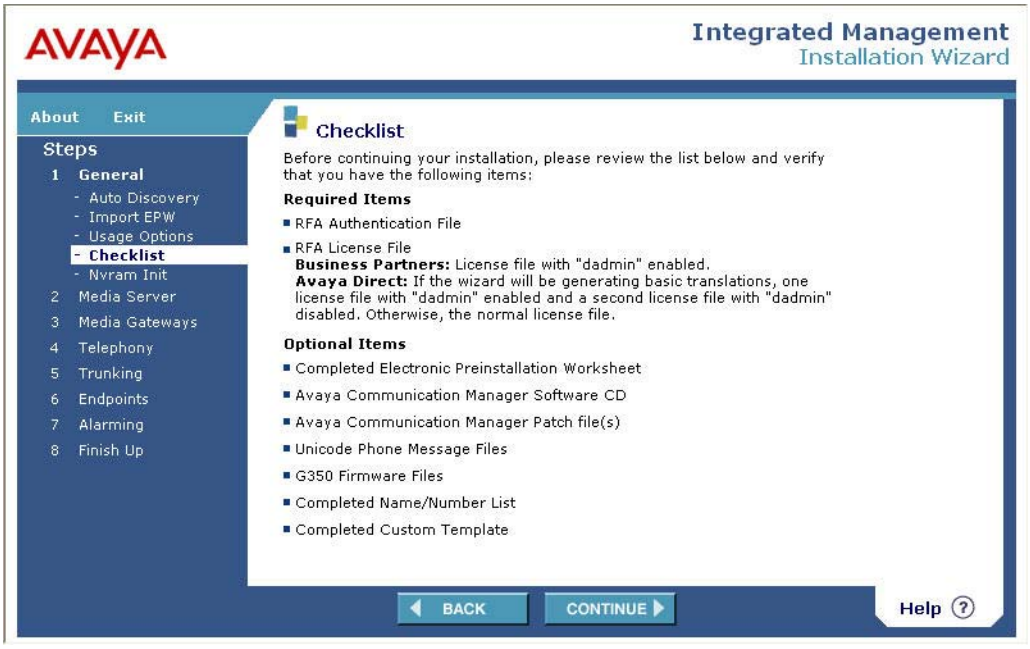
1. Click **`Continue`**. The Usage Options screen appears. This screen allows you to initiate the process of configuring an S8300 media server that is installed on the G350 as a Media Gateway Controller (MGC). You can configure the S8300 as either the primary MGC (ICC configuration) or as a backup MGC (LSP configuration). See Configuring the Media Gateway Controller (MGC) on page 51. You can also initiate a software or firmware upgrade. See Software and firmware upgrades on page 57.



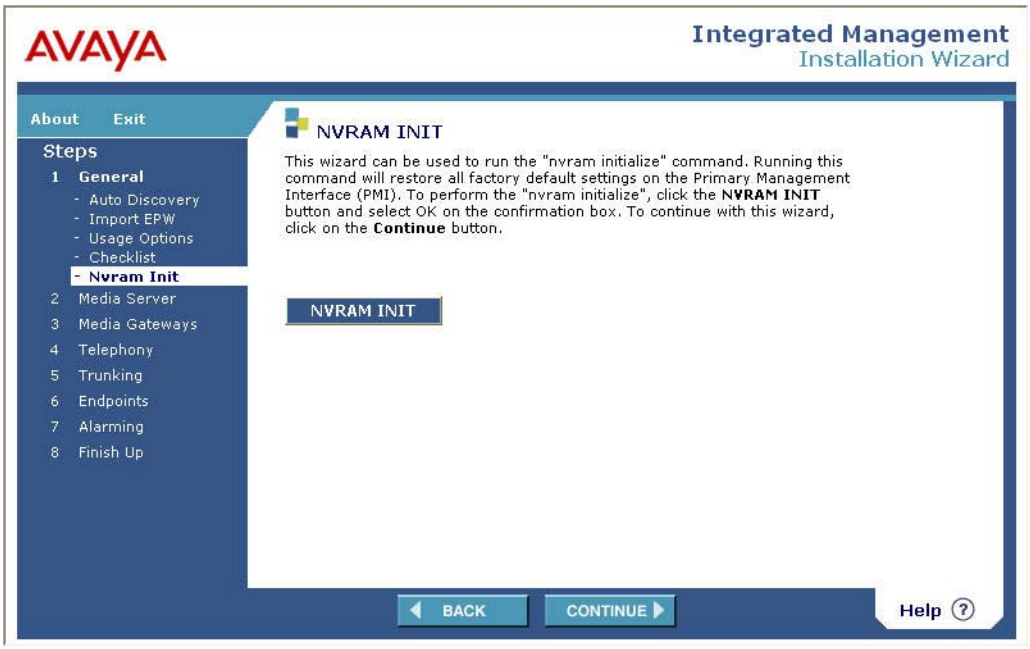
2. Click **Continue**. If you are configuring a new MGC, the Confirm New Installation screen appears as shown below. If you are upgrading an existing MGC, the Avaya Communication Manager Software screen appears. See Upgrading an existing MGC on page 395.



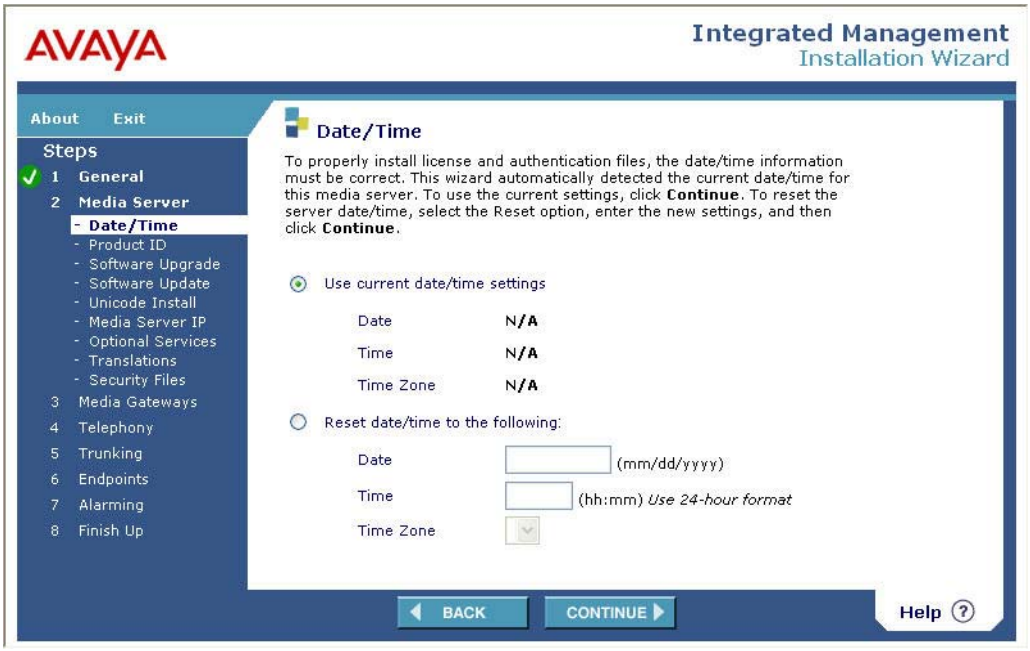
3. Click **Continue**. The Checklist screen appears. The Checklist screen displays a list of required and optional items you need to configure the G350. For details, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.



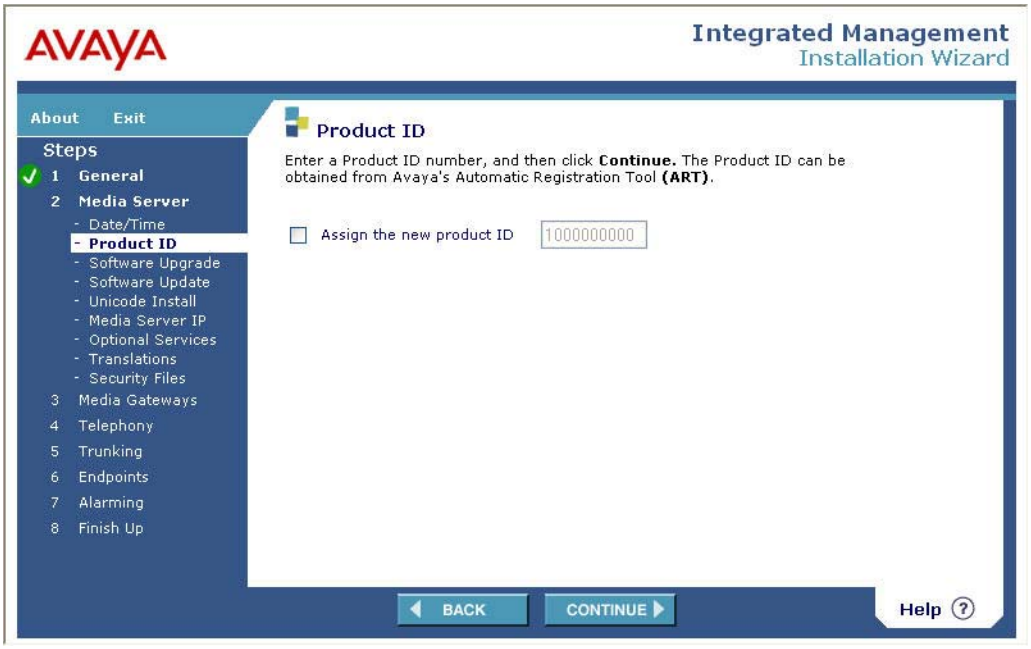
4. Click **Continue**. The NVRAM INIT screen appears. This screen allows you to restore all factory default settings on the Primary Management Interface (PMI). For a description of the PMI, see Configuring the Primary Management Interface (PMI) on page 50.



5. Click **Continue**. The Date/Time screen appears. This screen allows you to reset the G350's date and time.



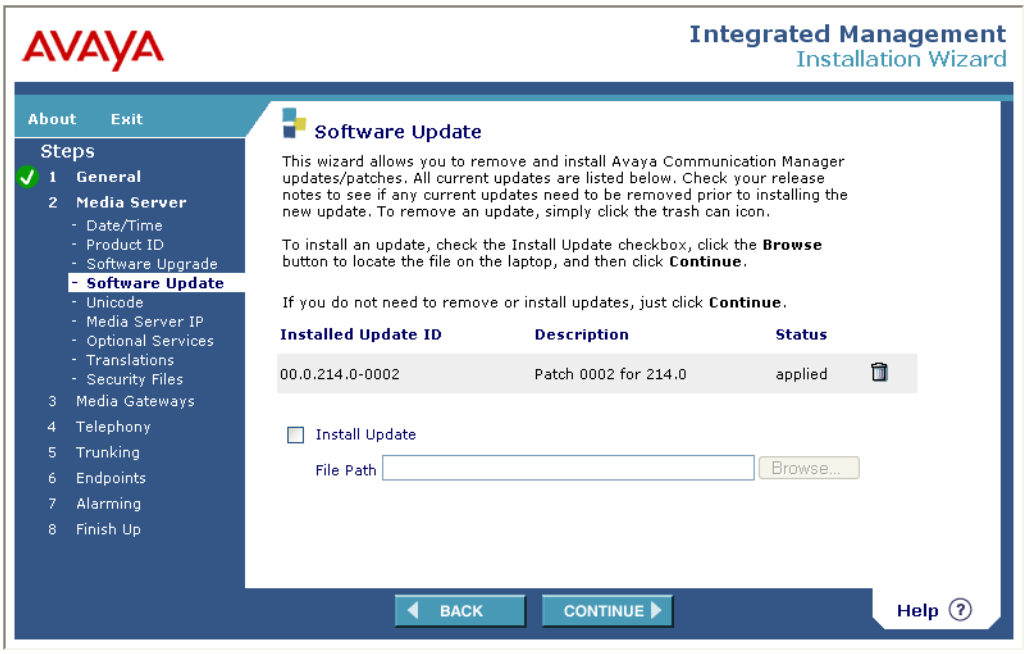
6. Click **Continue**. The Product ID screen appears. If you are configuring a new G350, enter the product ID in the ID field and select **Assign the new product ID**.



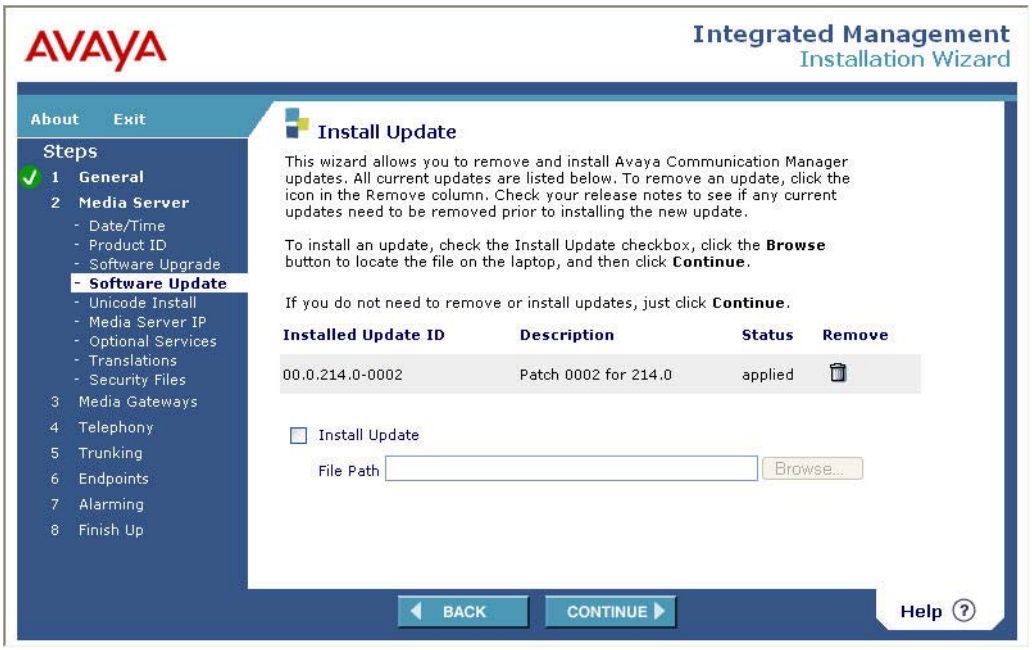
Upgrading an existing MGC

To upgrade an existing MGC:

1. Click **Continue**. The Avaya Communication Manager Software screen appears. This screen allows you to upgrade the Communication Manager software on the S8300 installed in the G350. For instructions on upgrading Communication Manager software, see Software and firmware upgrades on page 57.

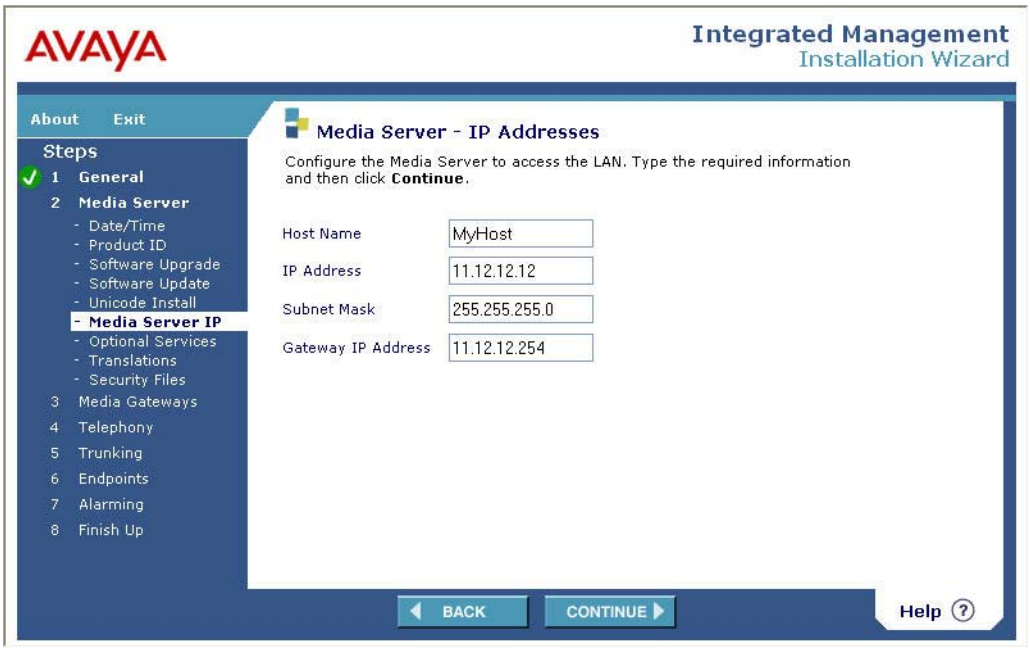


2. Click **Continue**. The Install Update screen appears. This screen allows you to install or remove Avaya Communication Manager updates.

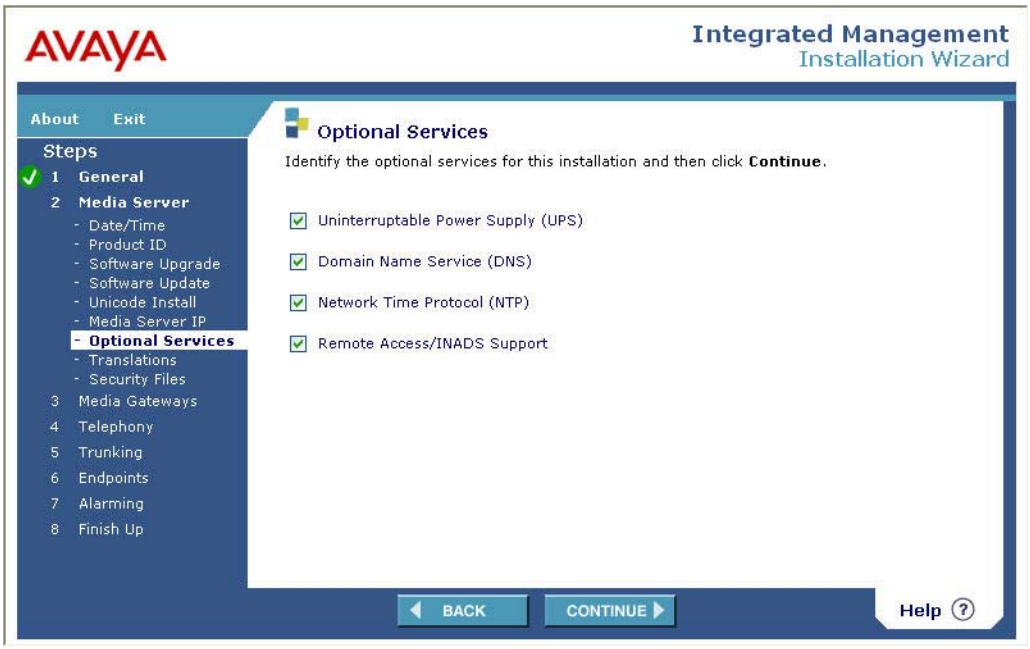


3. Click **Continue**. The Install Unicode Phone Message Files screen appears. This screen allows you to install files that provide unicode messages for display sets that are in the desired unicode language format.

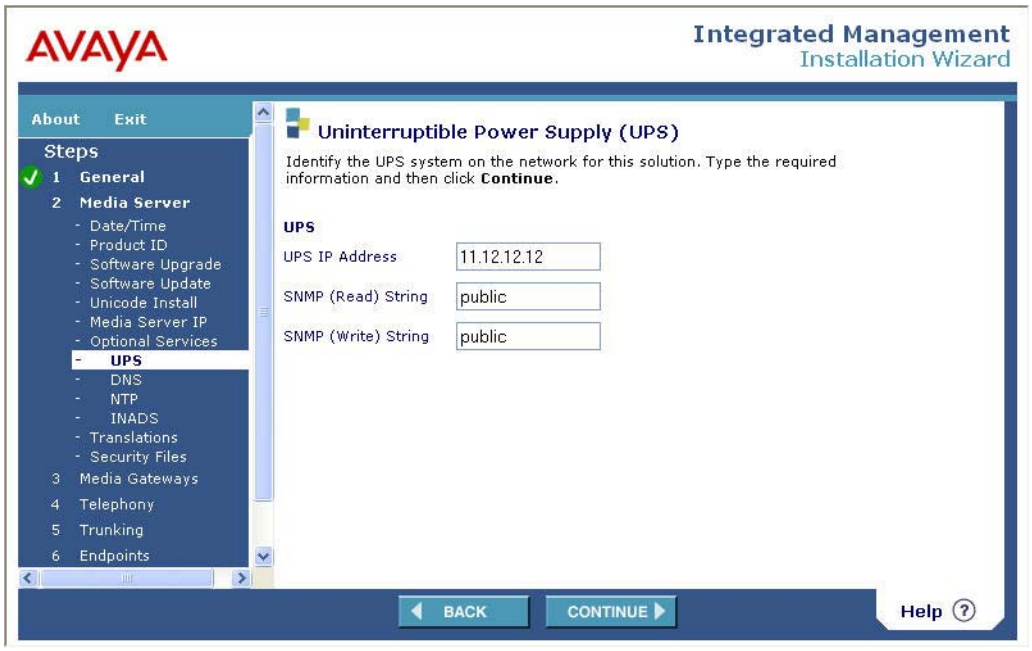
4. Click **Continue**. The Media Server - IP Addresses screen appears. If your S8300 media server is already configured, the Avaya IW should detect and display its address information in this screen. If not, you must enter the required information.



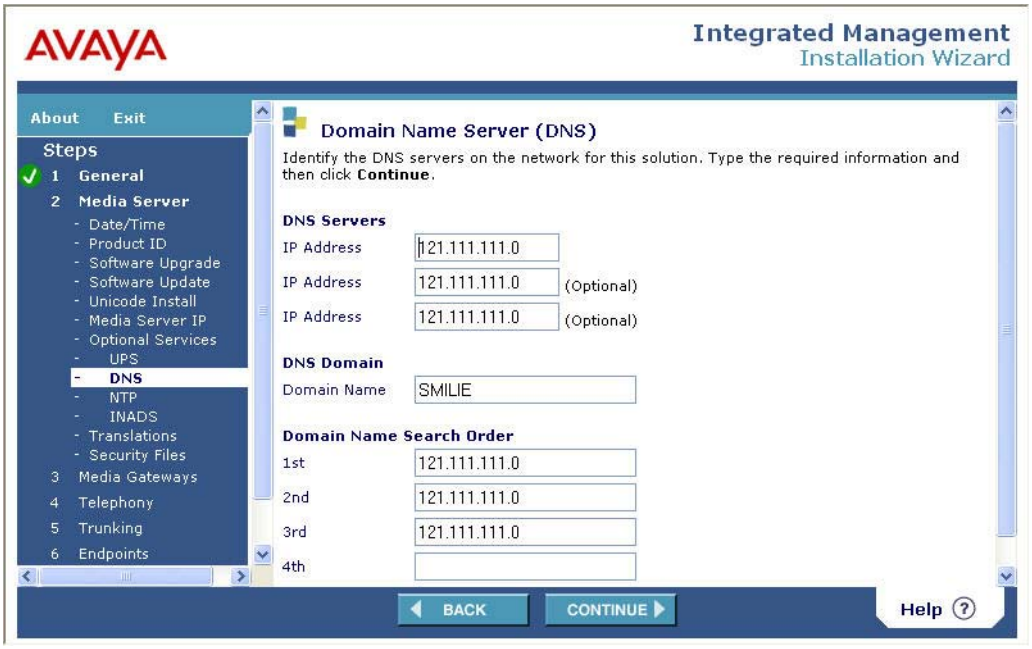
5. Click **Continue**. The Optional Services screen appears. Select the services you want.



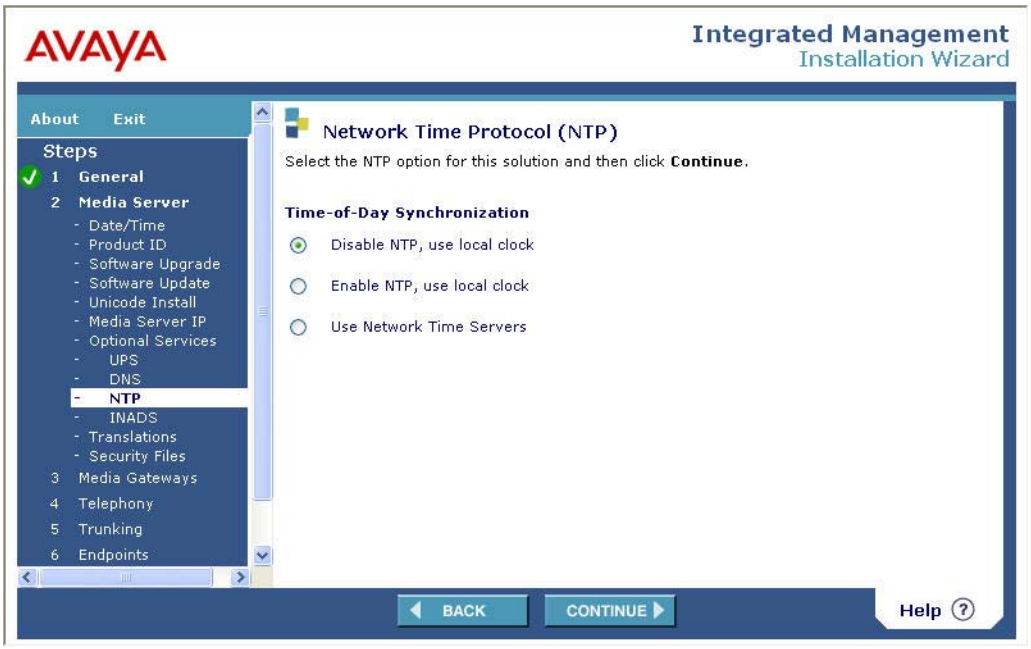
6. Click **Continue**. If you selected Uninteruptable Power Supply (UPS) in the Optional Services screen, the Uninteruptable Power Supply (UPS) screen appears. Enter the required information.



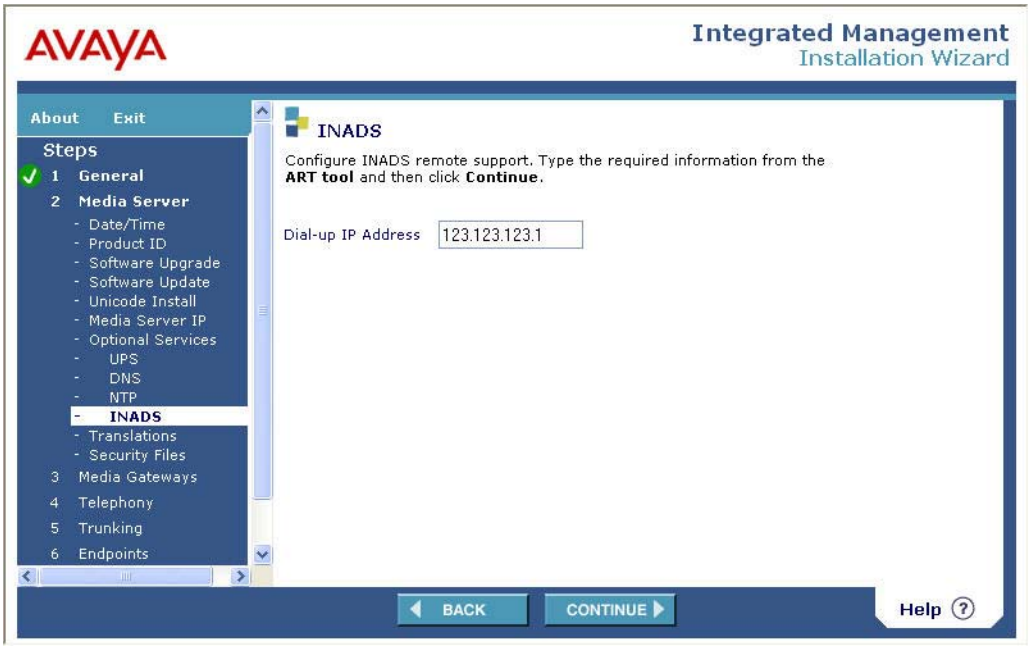
7. Click **Continue**. If you selected Domain Name Service (DNS) in the Optional Services screen, the Domain Name Service (DNS) screen appears. Enter the required information.



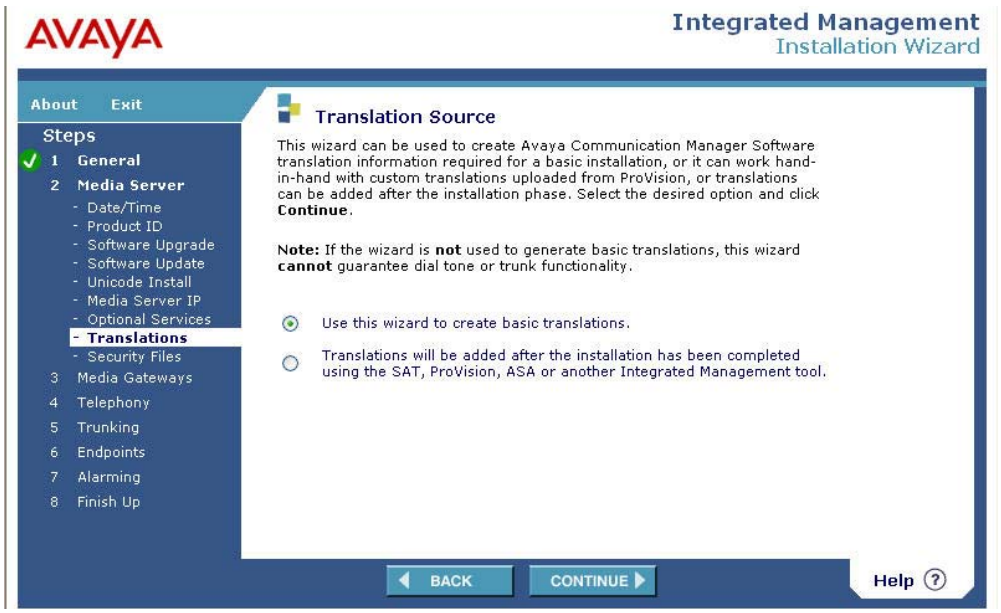
8. Click **Continue**. If you selected Network Time Protocol (NTP) in the Optional Services screen, the Network Time Protocol (NTP) screen appears. Select an NTP option.



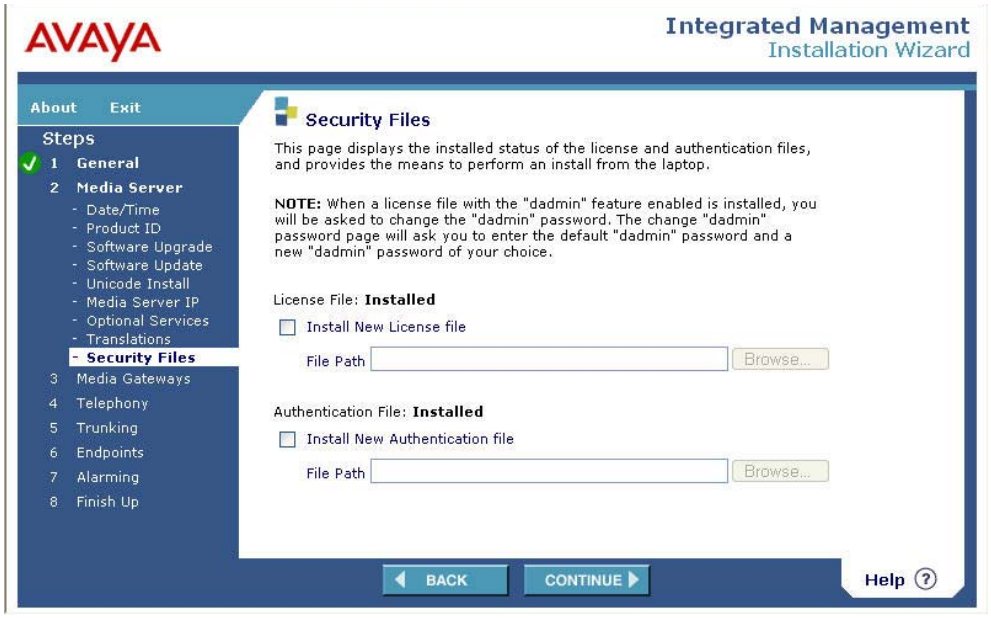
9. Click **Continue**. If you selected Remote Access/INADS Support in the Optional Services screen, the INADS screen appears. Enter a dialup IP address for INADS remote support. For instructions on how to obtain the INADS IP address, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.



10. Click **Continue**. The Translation Source screen appears. This screen allows you to generate Avaya Communication Manager translation information. This feature provides basic translations for administration of extension ranges, trunk types, routes, class of service, feature access codes, trunk access codes, station button assignment, and several other parameters.



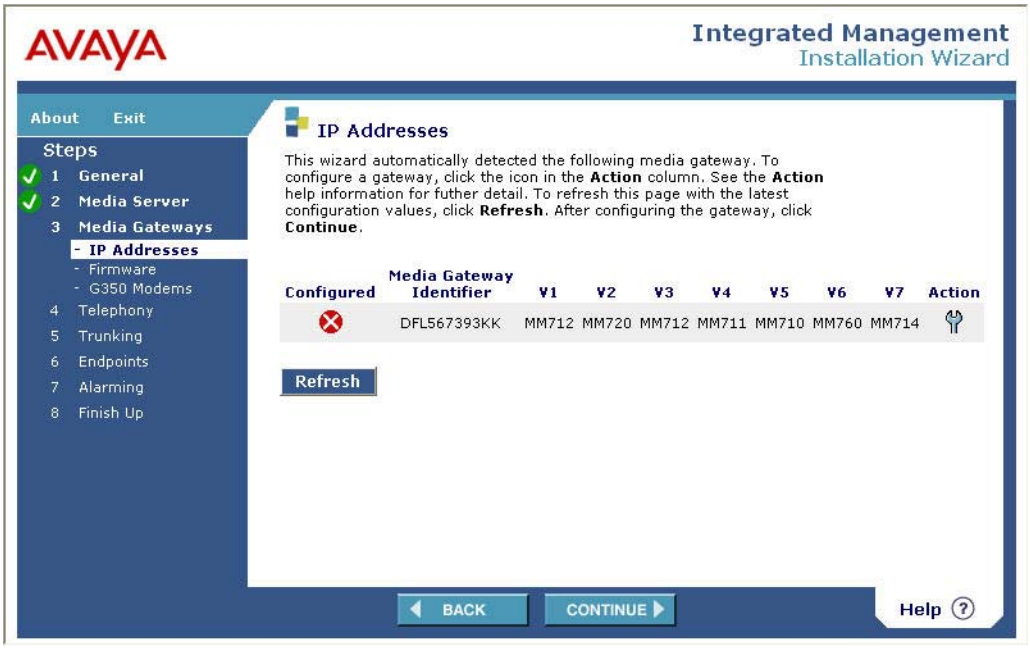
11. Click **Continue**. The Security Files screen appears. This screen displays the status of your license and authentication files, and allows you to install these files from a laptop. For information on these files, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.



Gateway configuration

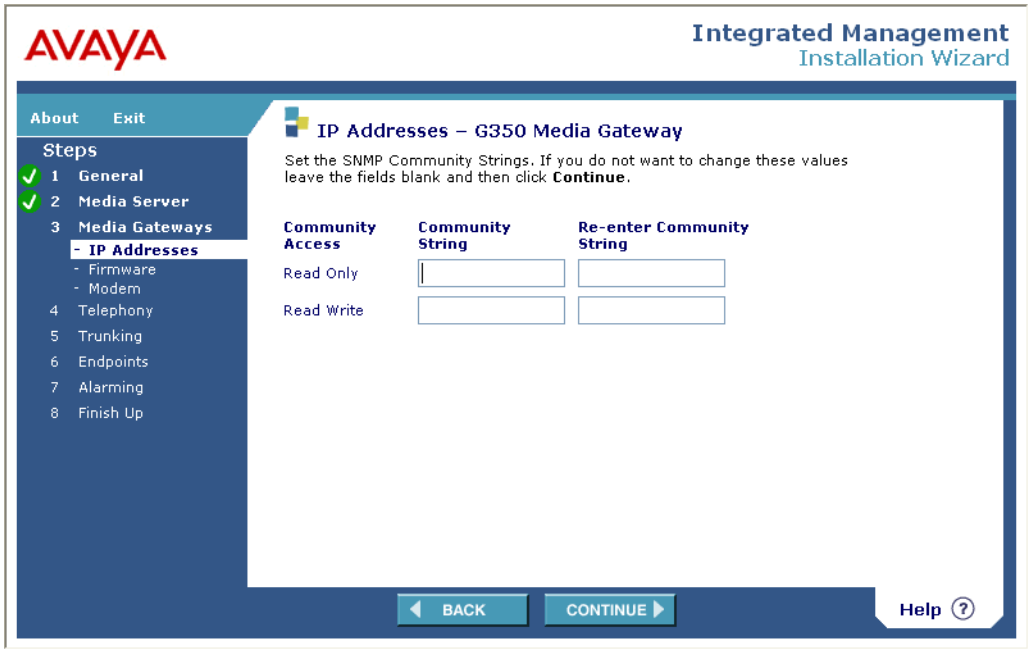
For Gateway configuration:

1. To configure the basic G350 parameters, click **`Media Gateways`**. The IP Addresses screen appears. This screen displays the G350's ID, as well as the type of media module residing in each slot of the G350's chassis. To continue, click the icon corresponding to the G350 in the **Action** column.

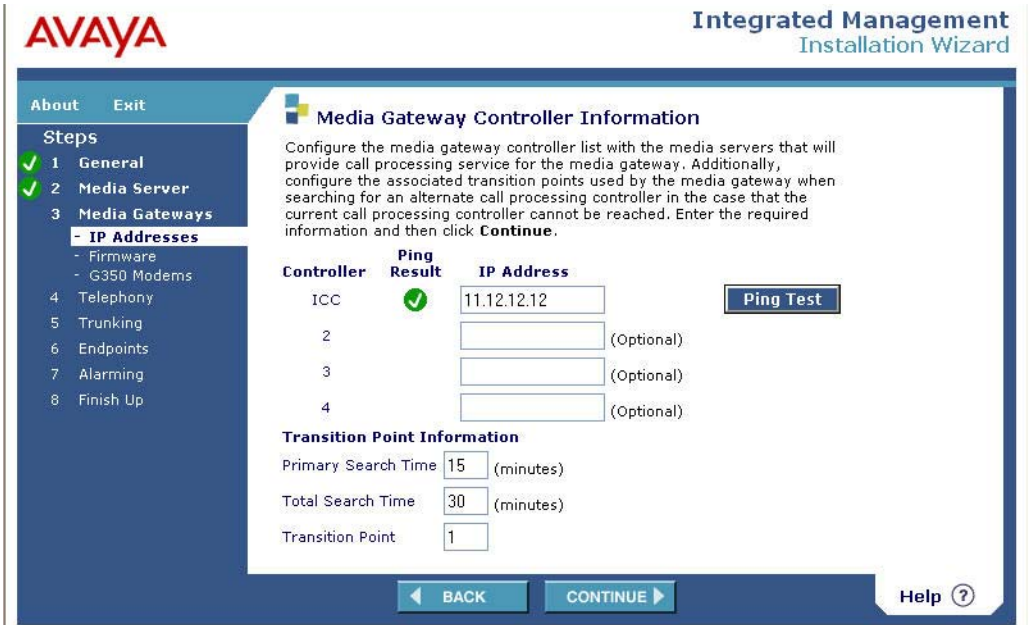


2. Click **Continue**. The PMI configuration screen appears. The IP address and subnet mask of the PMI should appear in this screen. Change this IP address and subnet mask in accordance with your system specifications. For information on the PMI, see Configuring the Primary Management Interface (PMI) on page 50.

3. Click **`Continue`**. The SNMP screen appears. For information on configuring SNMP settings, see Configuring SNMP on page 119.



4. Click **Continue**. The Media Gateway Controller Information screen appears. The IP addresses of the primary MGC appears in the first IP address box. The IP addresses of up to three additional MGCs may appear in the subsequent boxes. For information on configuring MGCs, see Configuring the Media Gateway Controller (MGC) on page 51.



5. Click **Continue**. The IP Addresses screen appears. This screen displays the G350's ID, as well as the type of media module residing in each slot of the G350's chassis. To continue, click the icon corresponding to the G350 in the **Action** column. To update this information, click **Refresh**.

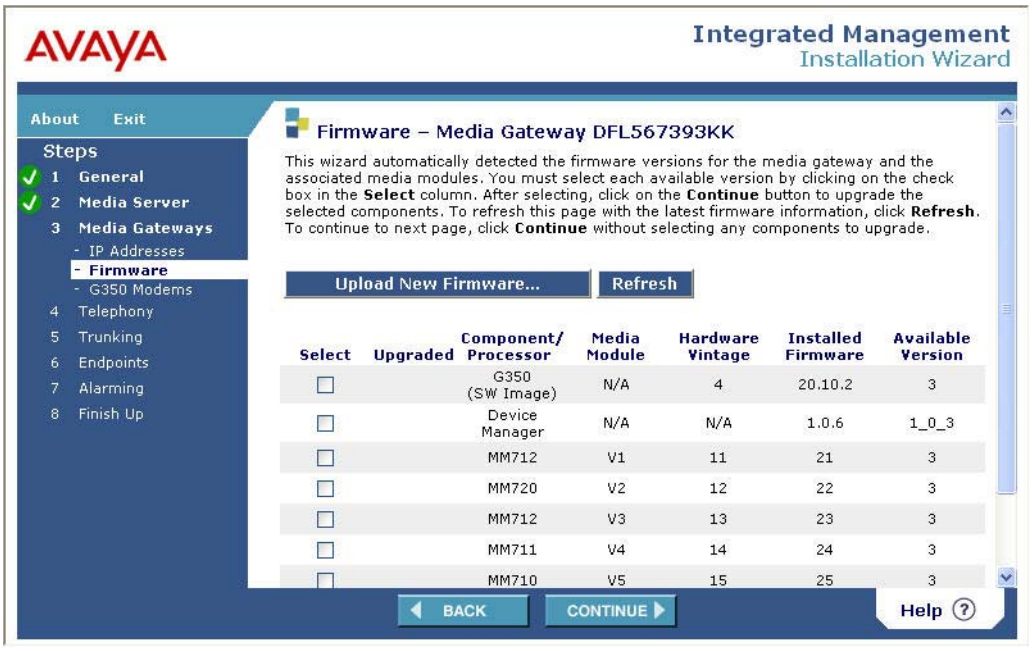
Firmware configuration

For firmware configuration:

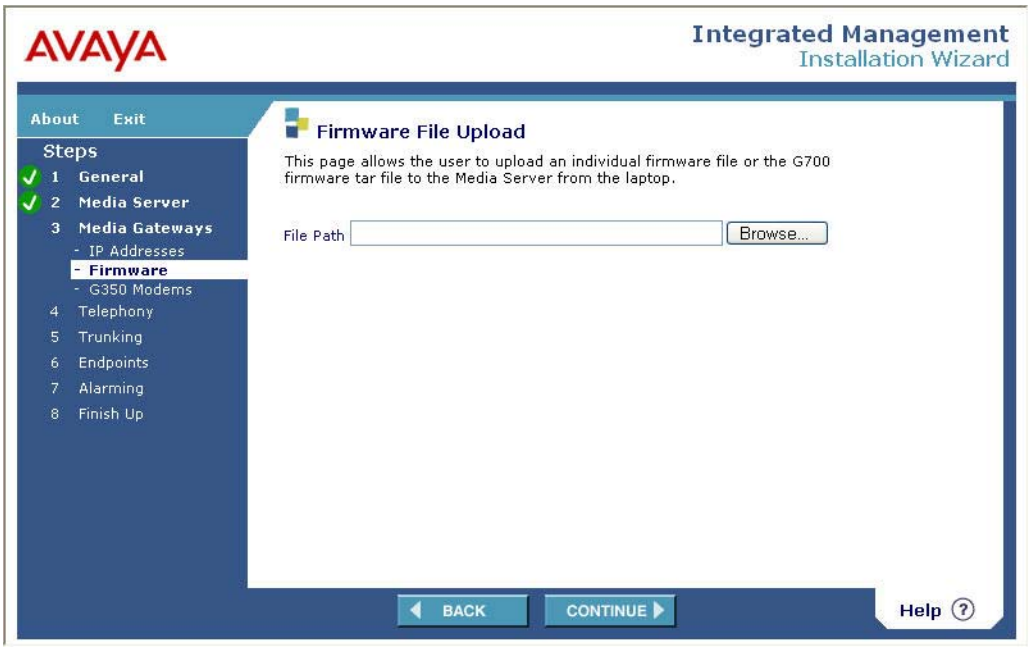
1. To upgrade the G350 firmware, do one of the following:
   - From the IP Addresses screen, click **Continue**, or
   - Click **Media Gateways** from the main menu.

   The Firmware screen appears. This screen displays the currently installed firmware versions on the G350 and its media modules, as well as the most recent available versions.

   - To upgrade firmware, select the modules you want to upgrade and click **Upload New Firmware**.
   - To upload a new firmware version from a laptop, clear all the boxes in the Select column and click **Continue**. The Firmware File Upload screen appears.
   - To proceed without upgrading any firmware, clear all the boxes in the **Select** column and click **Continue** twice.



2. The Firmware File Upload screen allows you to upload a new firmware file from a laptop. Enter the file path of the file you want to upload, or use the **Browse** button to locate the file. Then, click **Continue** to upload the file.

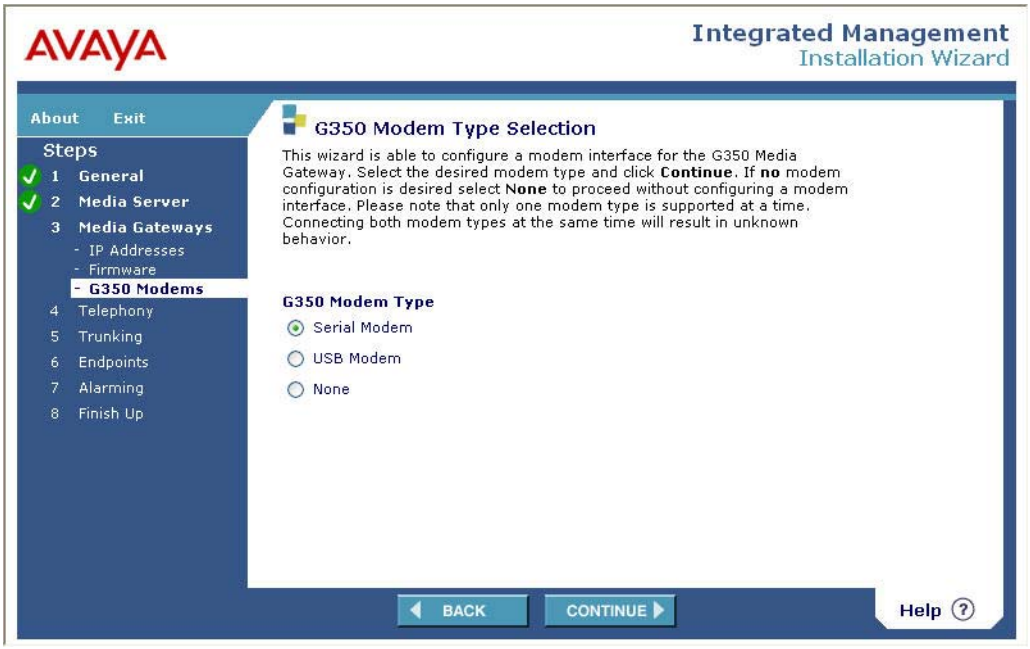


Modem configuration

For modem configuration:

1. To configure the G350 for modem use, do one of the following:
   - From the Firmware File Upload screen, click **Continue**, or
   - Click **Media Gateways>G350 Modems** from the main menu.

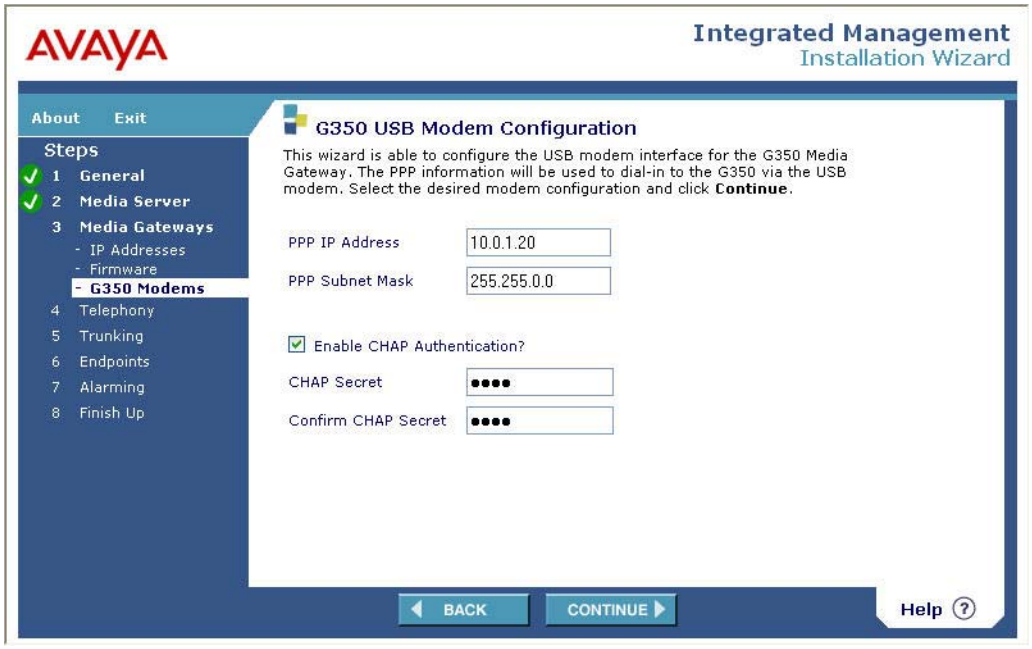
   The G350 Modem Type Selection screen appears. Select the modem type you want to use. For more information on using a modem with the G350, see Configuring the G350 for modem use on page 77.



2. Click **Continue**. If you selected **Serial Modem**, the G350 Serial Modem Configuration screen appears. If you selected **USB Modem**, the G350 USB Modem Configuration screen appears. If you selected **None**, the Country screen appears. See Telephony configuration on page 408.

3. If you selected **Serial Modem**, enter the required information in the G350 Serial Modem Configuration screen, then click **Continue**.

4. If you selected **USB Modem**, enter the required information in the G350 USB Modem Configuration screen, then click **Continue**.

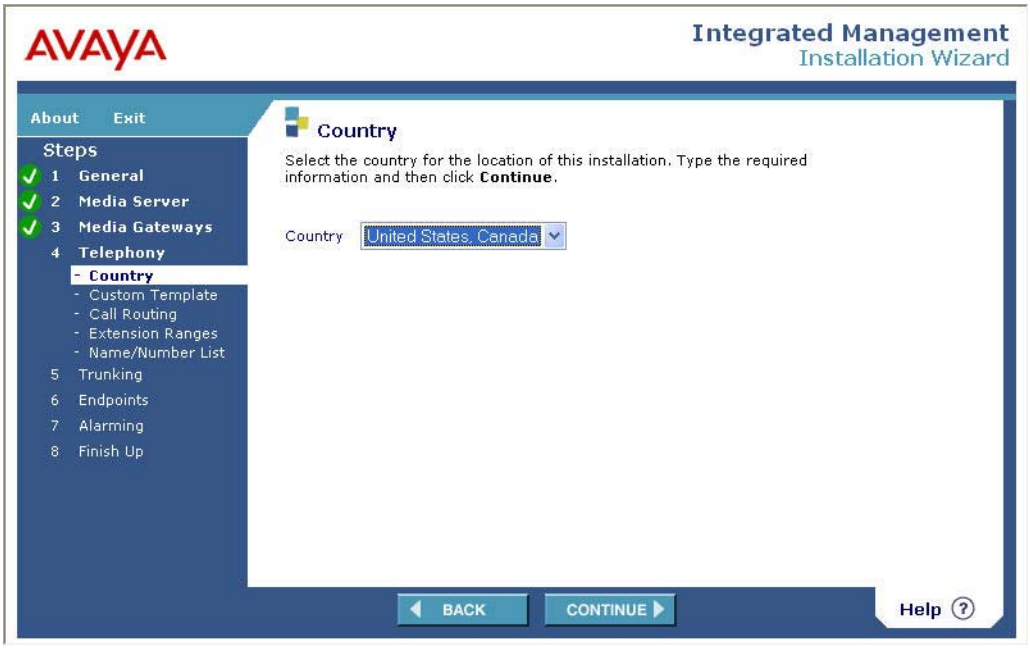


Telephony configuration

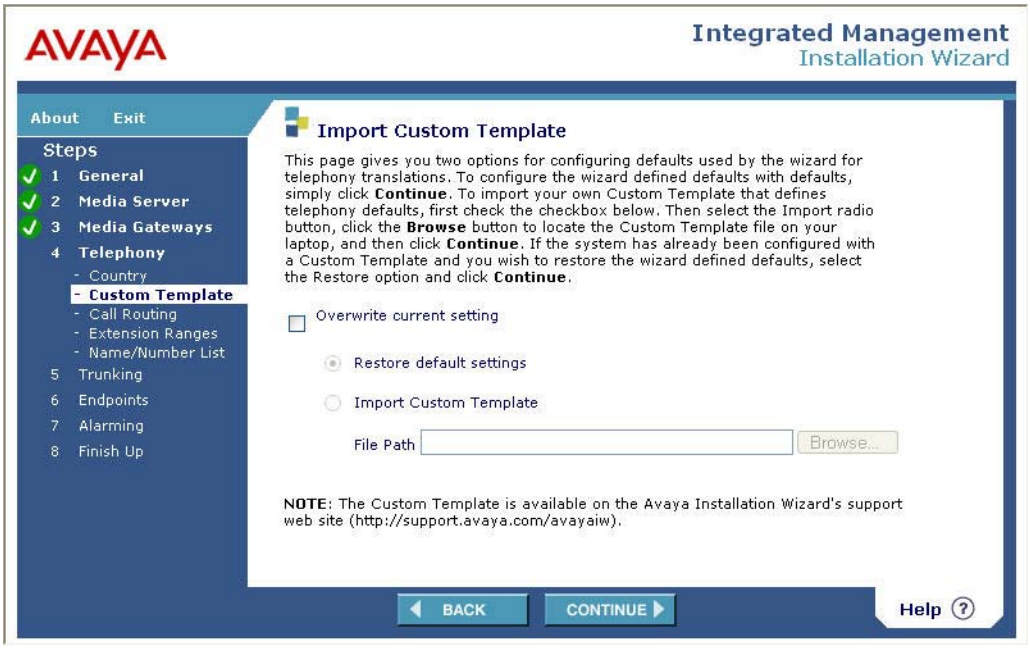
For telephony configuration:

1. To configure the G350's telephony parameters, do one of the following:
   - From the applicable modem configuration screen, click **Continue**, or
   - Click **Telephony** from the main menu.

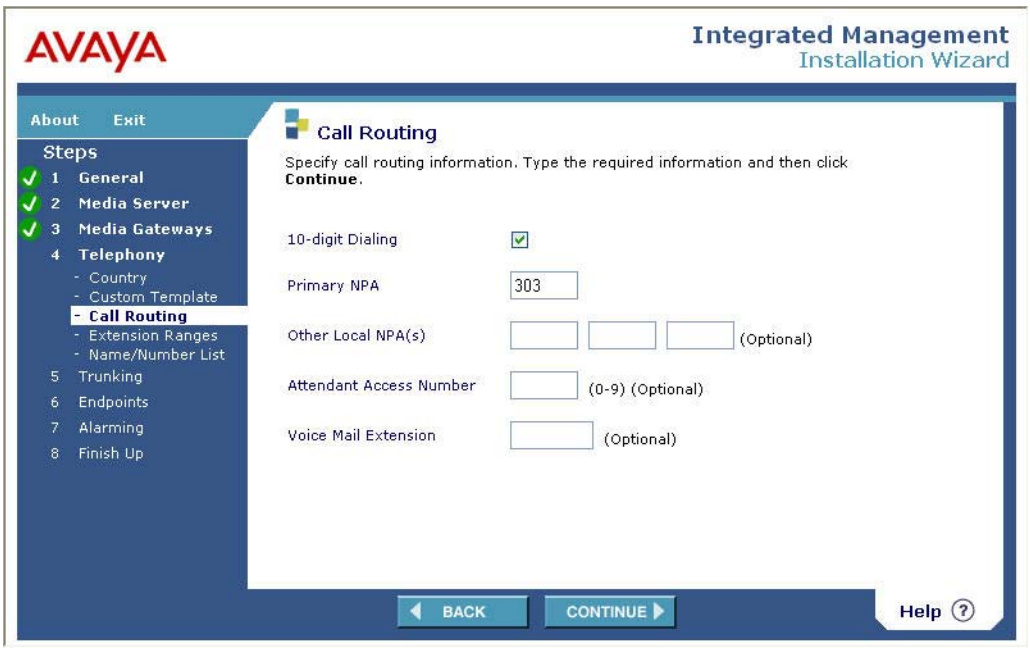
   The Country screen appears. Select the country in which the installation is taking place.



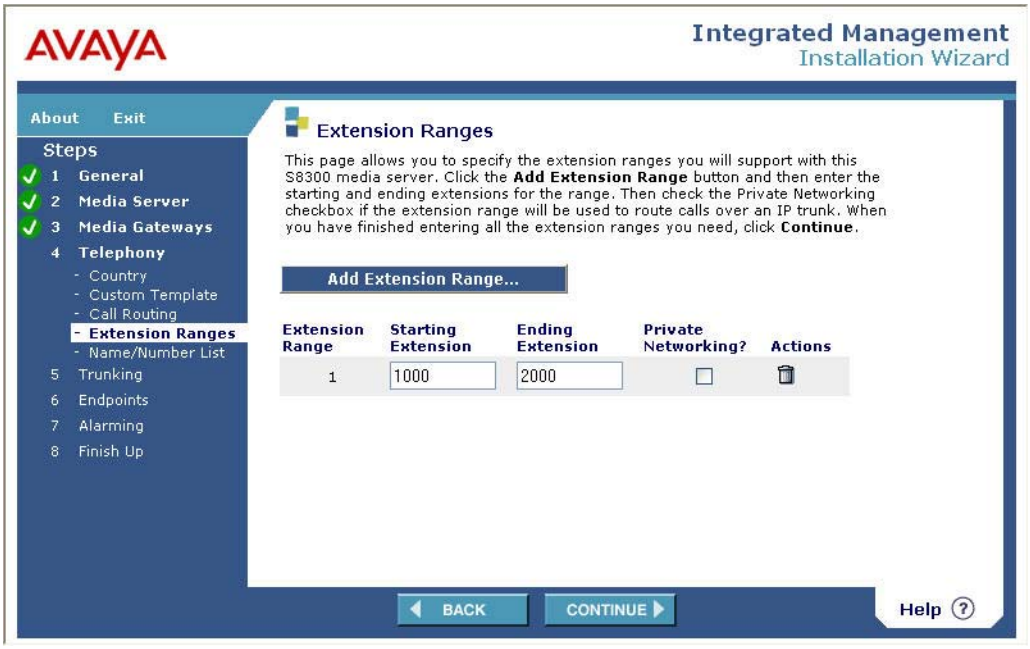
2. Click **Continue**. The Import Custom Template screen appears. This screen allows you to configure telephony translation defaults for the Avaya IW.



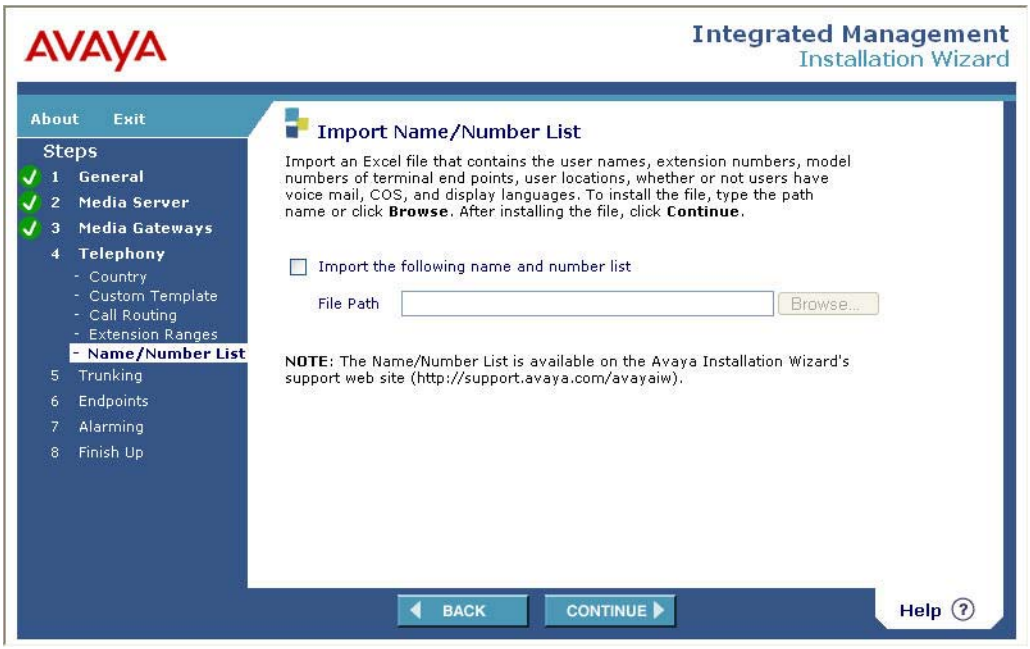
3. Click **Continue**. The Call Routing screen appears. Enter the required call routing information.



4. Click **Continue**. The Extension Ranges screen appears. To add a range, click **Add Extension Range** and enter the starting and ending extensions for the range. If you want this range to be used to route calls over an IP trunk, select **Private Networking**. To add additional extension ranges, repeat these steps. When you are finished, click **Continue**.



5. Click **Continue**. The Import Name/Number List screen appears. This screen allows you to import an Excel file that contains user names, extension numbers, and other information. To import this file:
   a. Select **Import the following name and number list**.
   b. Enter the file path of the file you want to import, or use the **Browse** button to locate the file.
   c. Click **Continue**.

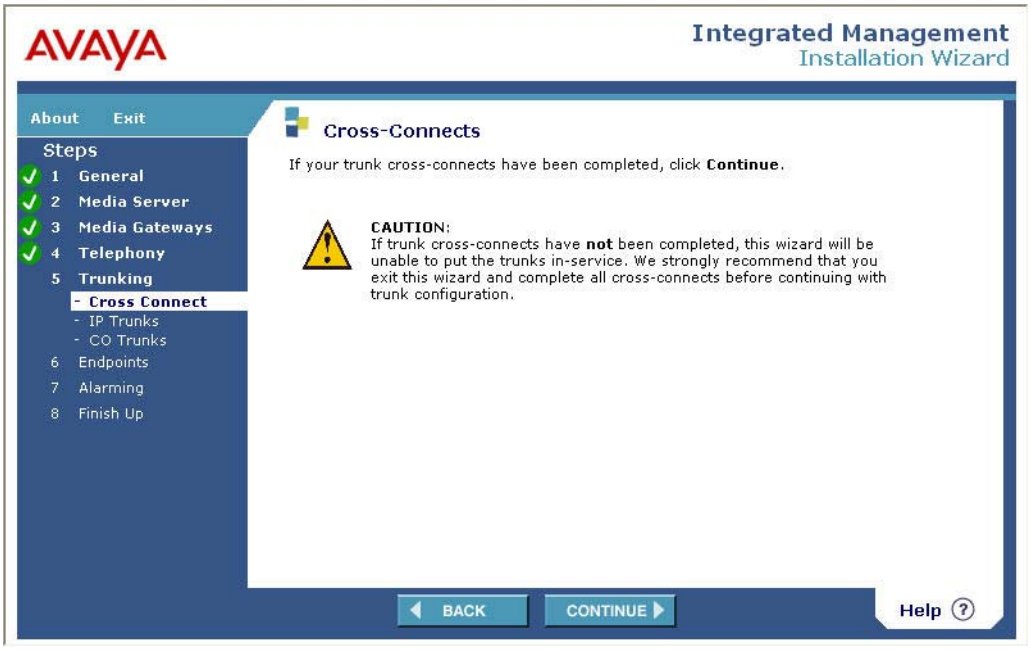


Trunk configuration

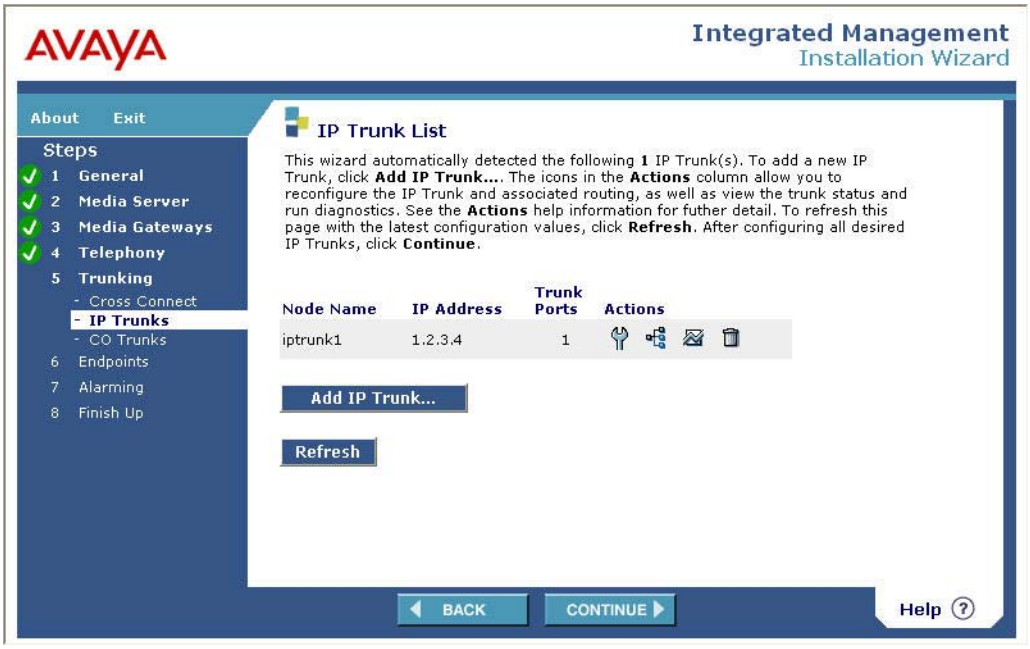
For trunk configuration:

1. To configure the G350's trunk parameters, do one of the following:
   - From the Import Name/Number List screen, click **Continue**, or
   - Click **Trunking** from the main menu.

   The Cross-Connects screen appears. If your trunk cross-connects have been completed, click **Continue** to proceed with trunk configuration. If your trunk cross-connects have not been completed, it is strongly recommended to exit the Avaya IW and complete all cross-connects before proceeding with trunk configuration.



2. Click **Continue**. The IP Trunk List screen appears. This screen displays all IP trunks configured on the G350. To refresh this list, click **Refresh**.



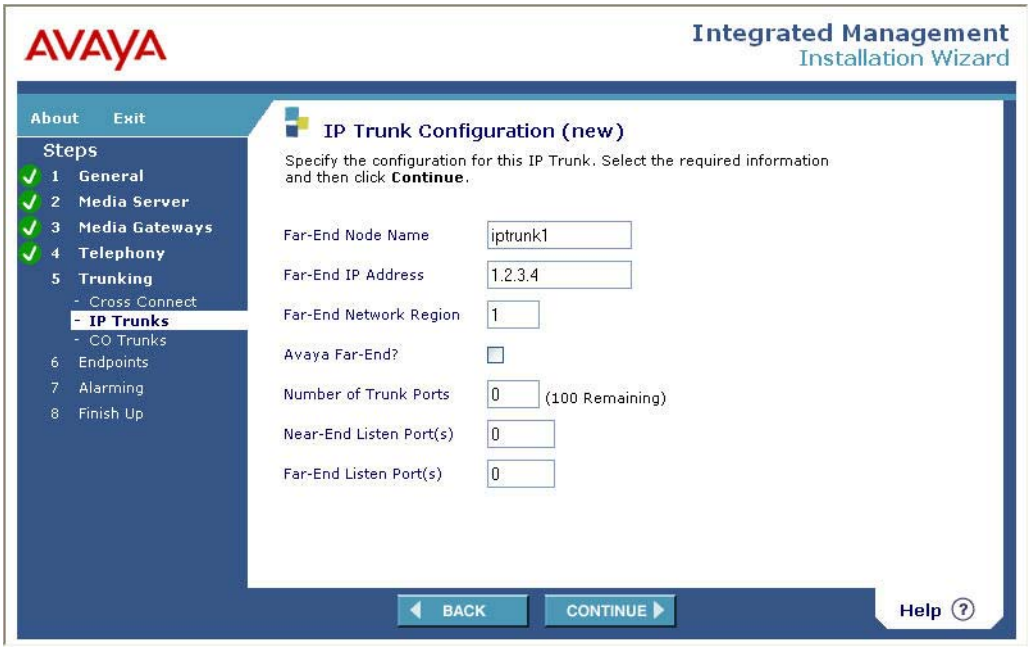
3. You can perform the following actions in the IP Trunk List screen:

   - Adding a trunk
   - Modifying trunk parameters
   - Modifying IP route configuration
   - Displaying trunk status
   - Removing a trunk

   To proceed to the CO Trunk List screen for configuring a trunk media module, click **Continue**. See Configuring a trunk media module on page 419.

Adding a trunk

4. To add a new trunk click **Add IP Trunk**. The IP Trunk Configuration screen appears.

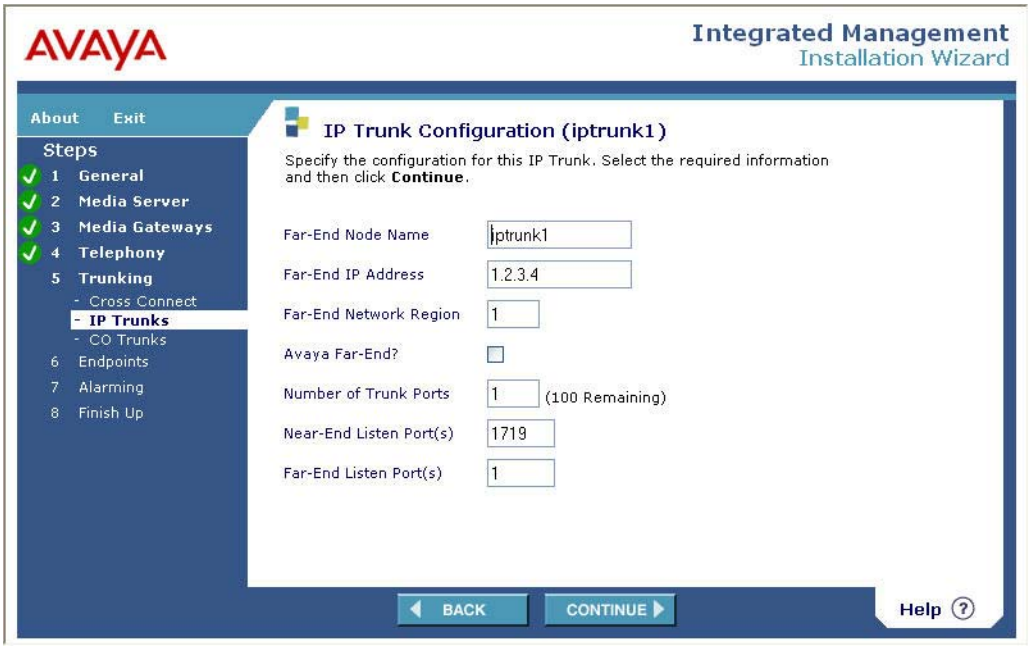


5. Enter the required information in the IP Trunk Configuration screen and click **Continue**. The IP Trunk List appears, with the new trunk included in the list of trunks. To add an additional trunk, click **Add IP Trunk** and repeat this step. When you are finished adding trunks, click **Continue** or select an action from the **Actions** column to modify an existing trunk.

Modifying trunk parameters

6. To modify the trunk's parameters, click the configuration icon in the **Actions** column of the IP Trunk List screen.

The IP Trunk Configuration screen appears, with the trunk's current parameters displayed.

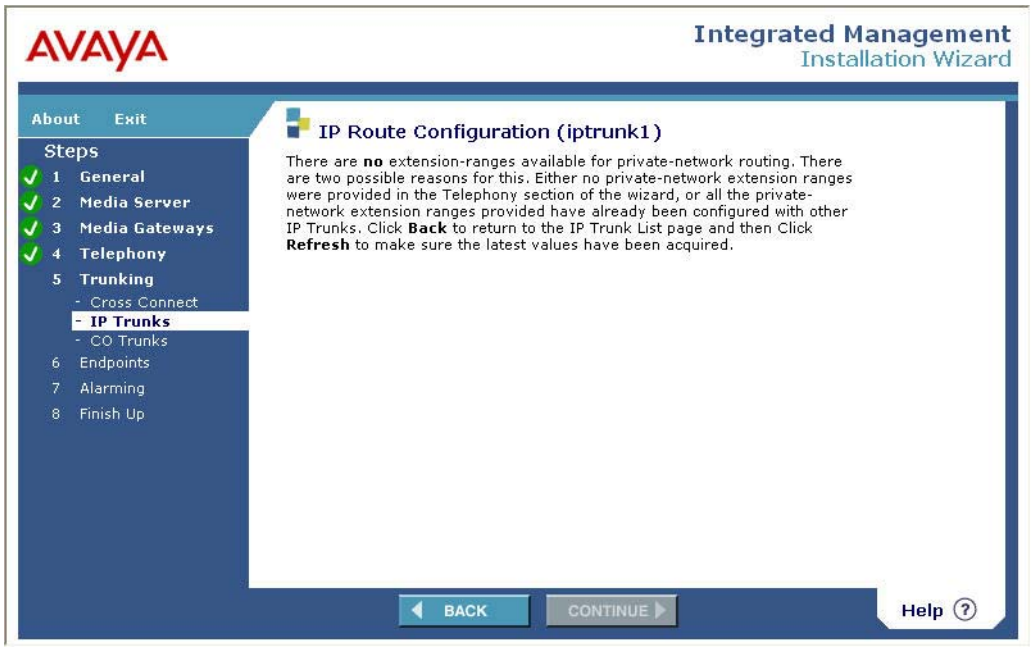


7. Modify the trunk parameters and click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See Configuring a trunk media module on page 419.

Modifying IP route configuration

8. To modify the trunk's IP route configuration, click the IP route icon in the **Actions** column of the IP Trunk List screen.

The IP Route Configuration screen appears.

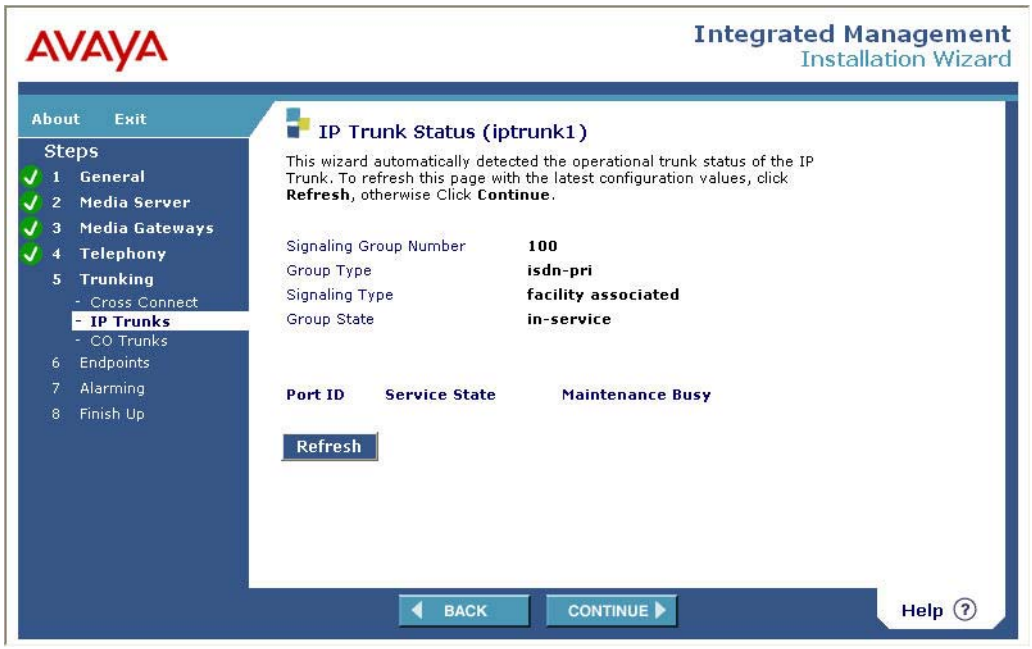


9. The IP Route Configuration screen displays the extension ranges available for private-network routing. Modify these ranges, if any, and click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See Configuring a trunk media module on page 419.

Displaying trunk status

10. To display the trunk's IP route configuration, click the trunk status icon in the **Actions** column of the IP Trunk List screen.

The IP Trunk Status screen appears.

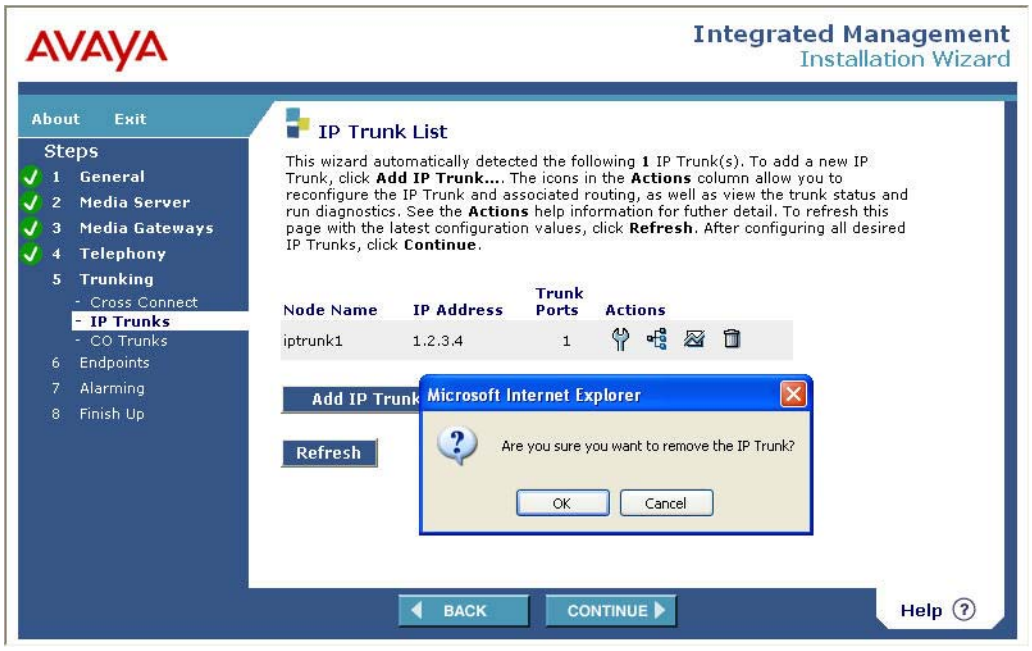


11. The IP Trunk Status screen displays the operational status of the trunk. To refresh the information, click **Refresh**. Otherwise, click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See Configuring a trunk media module on page 419.

Removing a trunk

12. To remove a trunk, click the trunk's remove icon in the **Actions** column of the IP Trunk List screen.

A message appears asking if you want to remove the trunk.

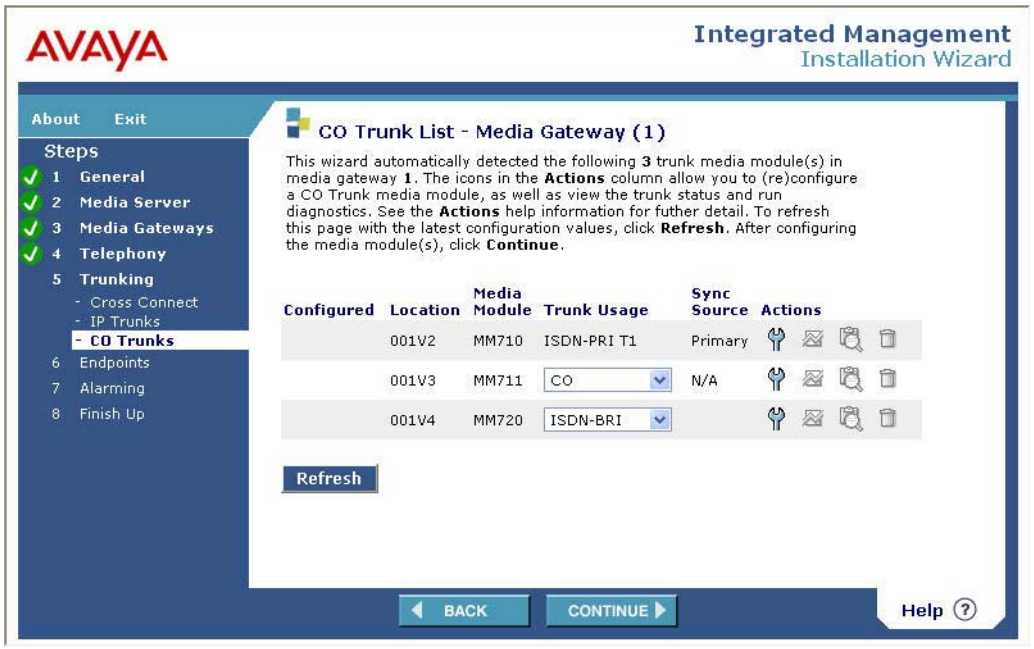


13. Click **OK** to remove the trunk. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen.

Configuring a trunk media module

14. To configure a trunk media module, do one of the following:
    - Click **Continue** from the IP Trunk List screen, or
    - Click **Trunking>CO Trunks** from the main menu.

    The CO Trunk List screen appears. This screen lists trunk media modules detected in the G350 and allows you to configure a media module and run diagnostics. To configure or run diagnostics on a trunk media module, click the Actions icon for the module.

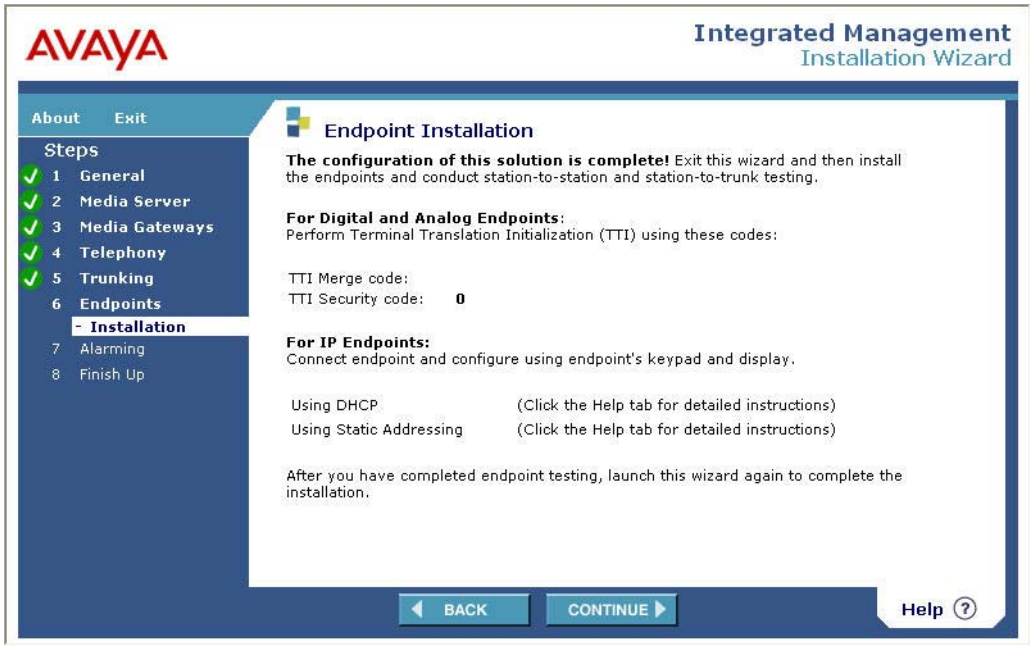


Endpoint installation

For endpoint installation:

1. For instructions on endpoint installation, do one of the following:
   - Click **Continue** from the CO Trunk List screen, or
   - Click **Endpoints** from the main menu.

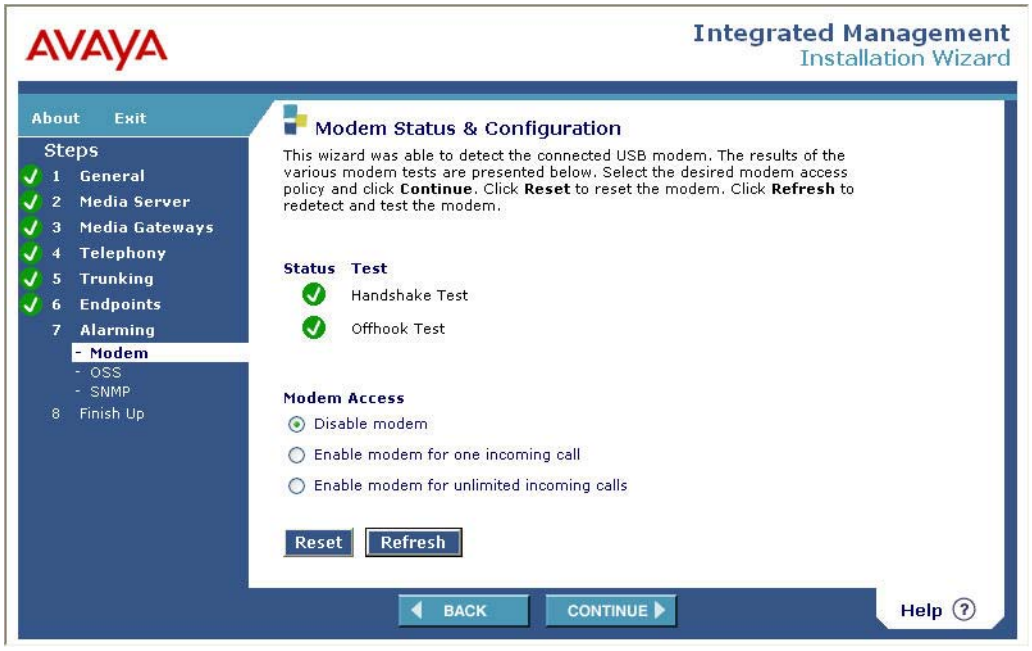
   The Endpoint Installation screen appears. You can access endpoint installation information from this screen.



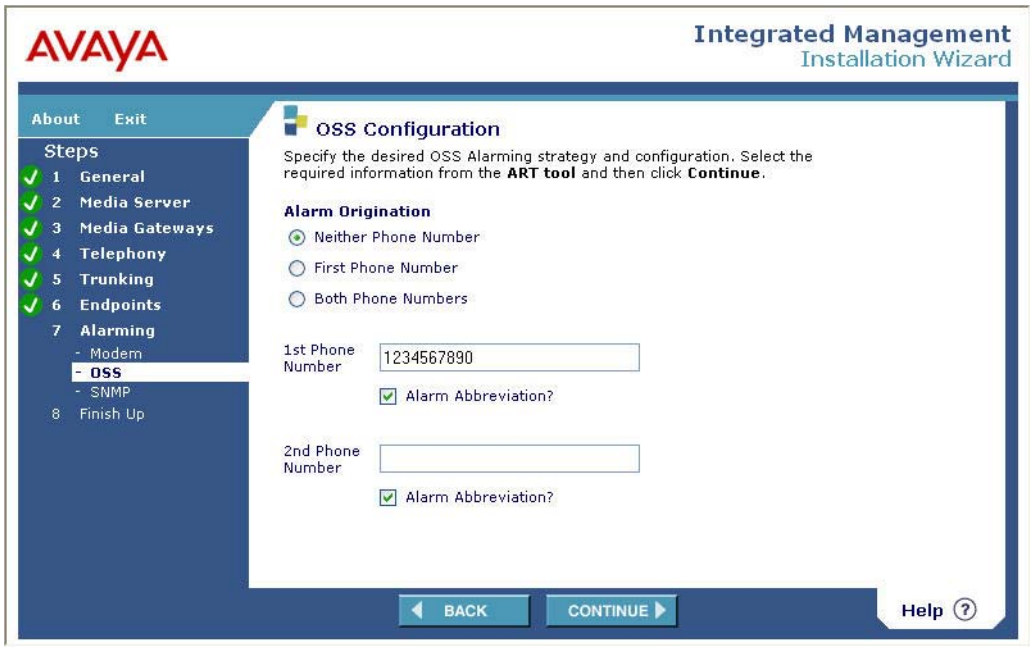
Alarm configuration

For alarm configuration:

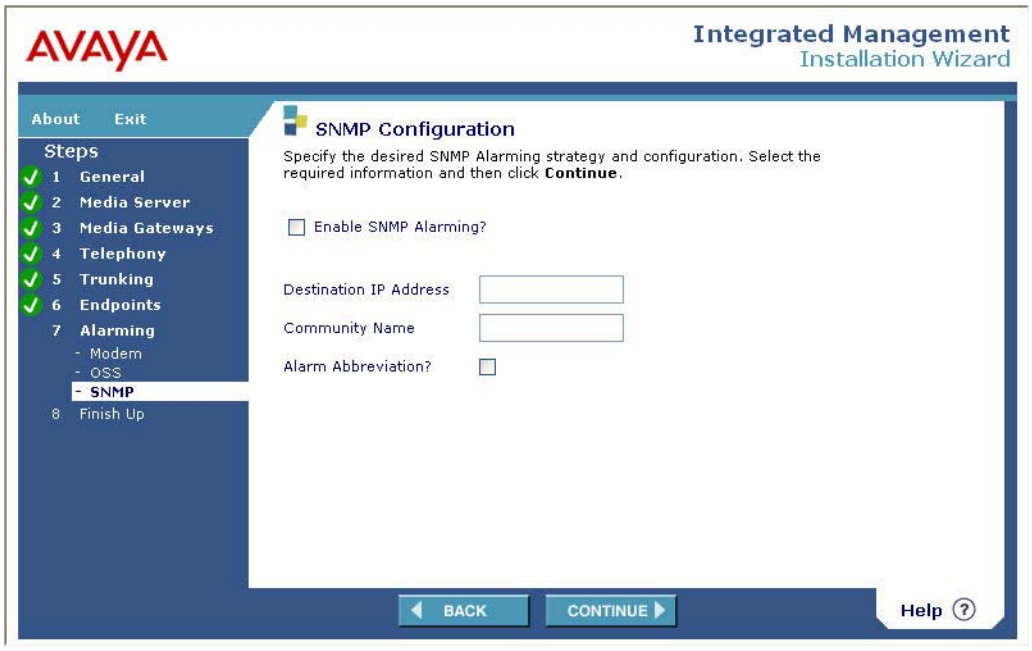
1. To display modem status and configure alarms, click **Alarming** from the main menu. The Modem Status & Configuration screen appears. This screen detects any modem connected to the G350. The screen also displays the results of tests performed on the modem. You can perform the following actions from this screen:
   - Click **Reset** to reset the modem.
   - Click **Refresh** to re-detect and test the modem.
   - Select the appropriate modem access policy in the **Modem Access** area and click **Continue**.



2. Click **Continue**. The OSS Configuration screen appears. Enter the required information from the ART tool. For information on using the ART tool, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.



3. Click **Continue**. The SNMP Configuration screen appears. For information on SNMP configuration, see Configuring SNMP on page 119.

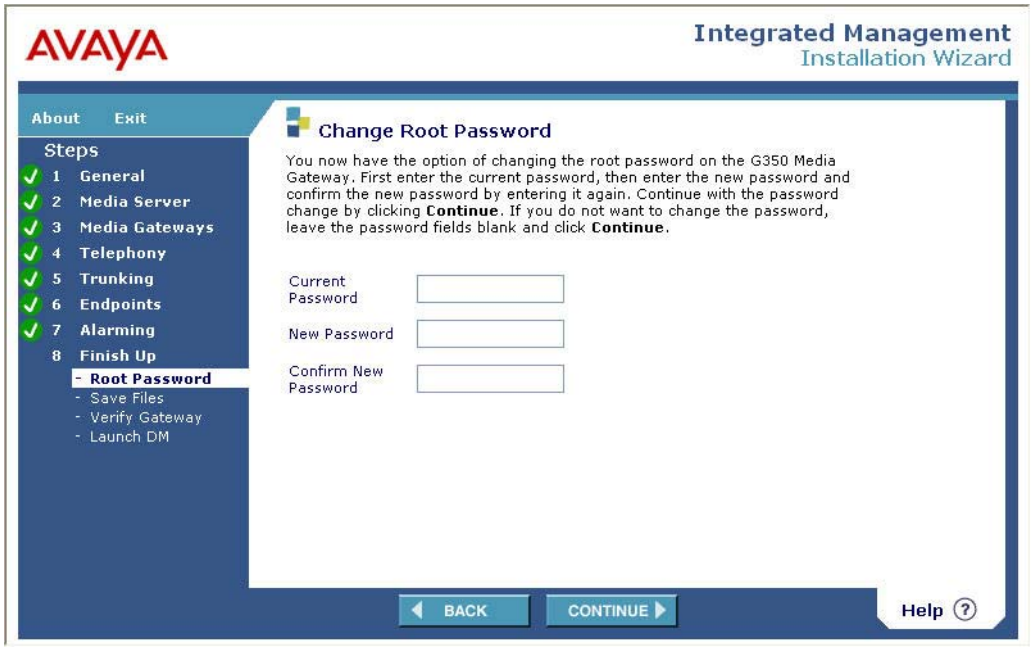


Password and final screens

To view password and final screens:

1. To change your password (optional) and complete the installation, do one of the following:
   - Click **Continue** from the SNMP Configuration screen, or
   - Click **Finish Up** from the main menu.

   The Change Root Password screen appears. This screen allows you to change the root password on the G350.



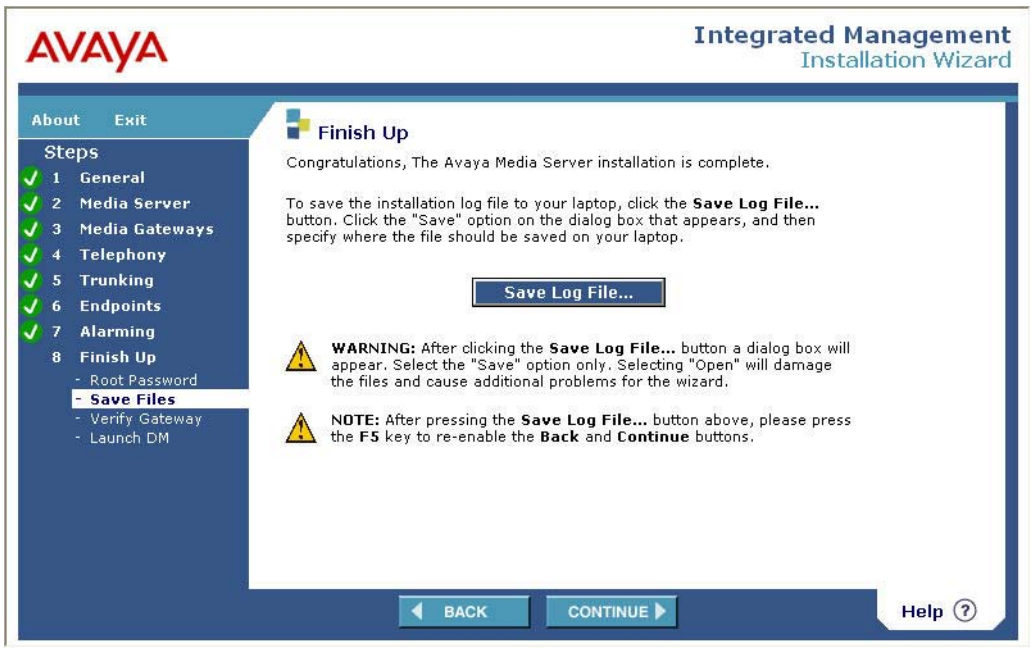
2. Click **Continue**. The Finish Up screen appears. This screen allows you to save the installation log file to your laptop. To save the installation log file:

   a. Click **Save Log File**. A dialog box appears.

   b. Click **Save**.

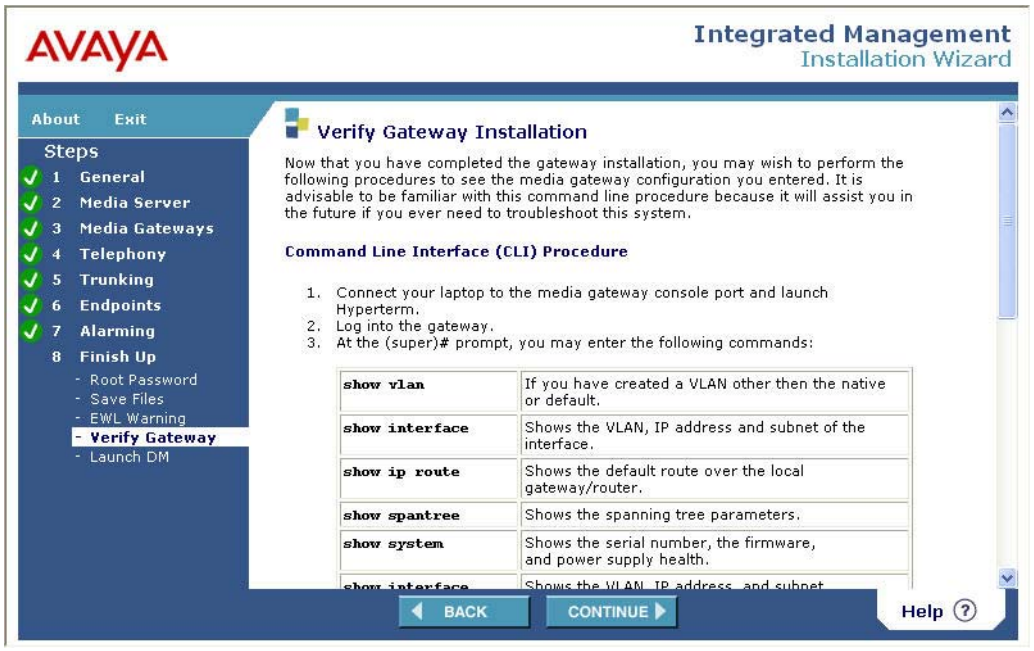
   WARNING:
   Do not click **Open**. Clicking **Open** will damage the log file and may cause other problems to the Avaya IW.

   c. Press **<F5>** to restore the **Back** and **Continue** buttons to the Finish Up screen.

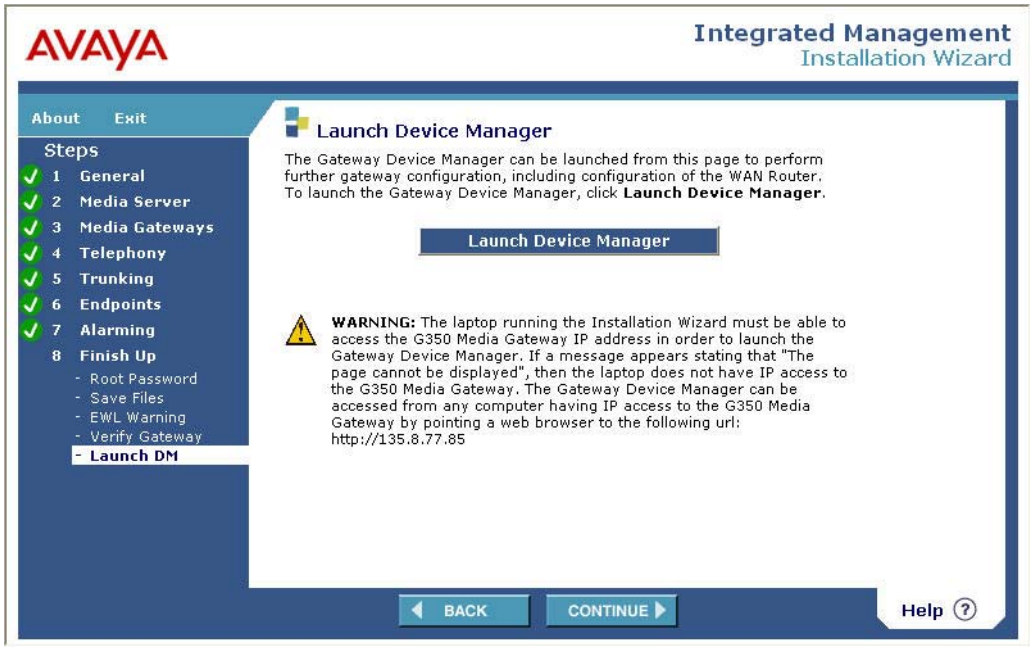


3. Click **Continue**. If you have not installed an allocation license file, a warning appears reminding you to install this file.

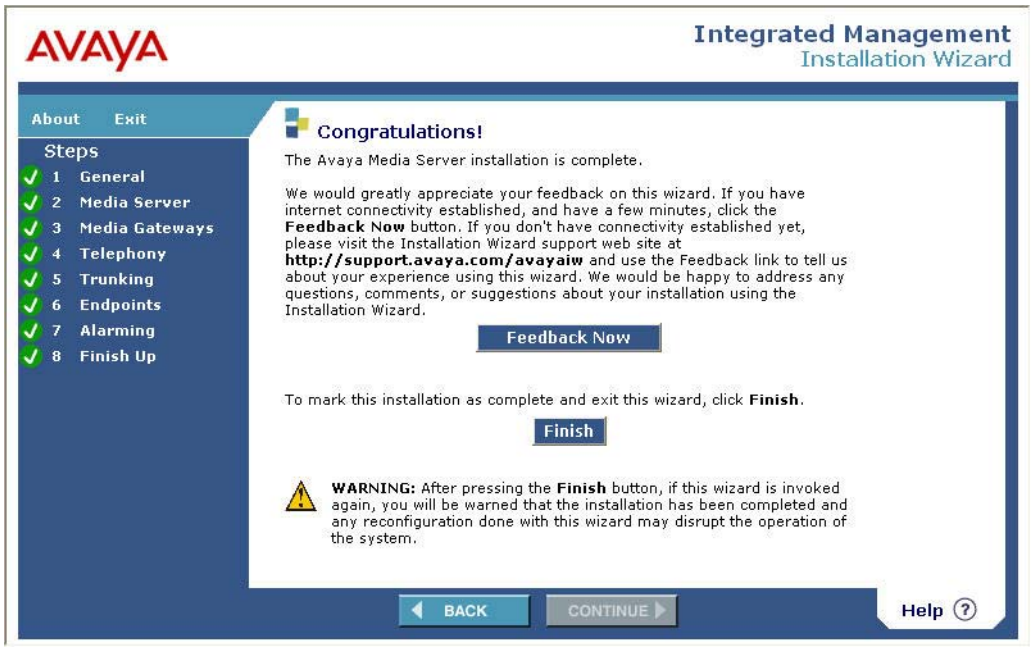
4. Click **Continue**. The Verify Gateway Installation screen appears. This screen displays a list of CLI commands that you can use to verify the G350 configuration. The following figure shows a portion of the Verify Gateway Installation screen.



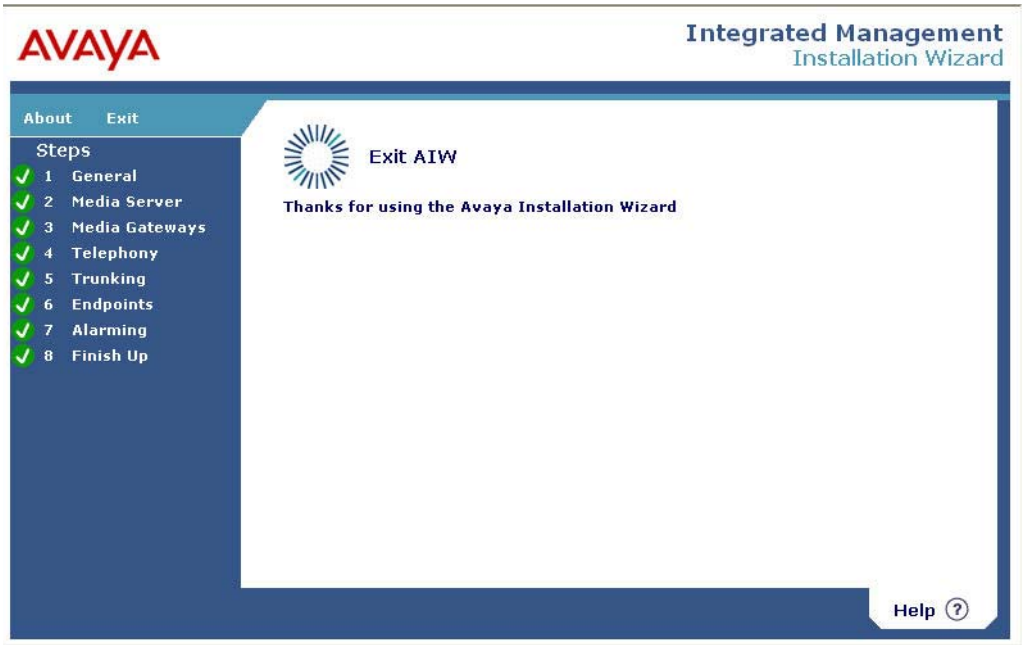
5. Click **Continue**. The Launch Device Manager screen appears. This screen allows you to launch the Gateway Device Manager, an application that allows you to configure the WAN Router and perform other advanced configuration tasks.



6. Click **Continue**. The Congratulations! screen appears to inform you that the installation is complete. To exit the Avaya IW, click **Finish**.



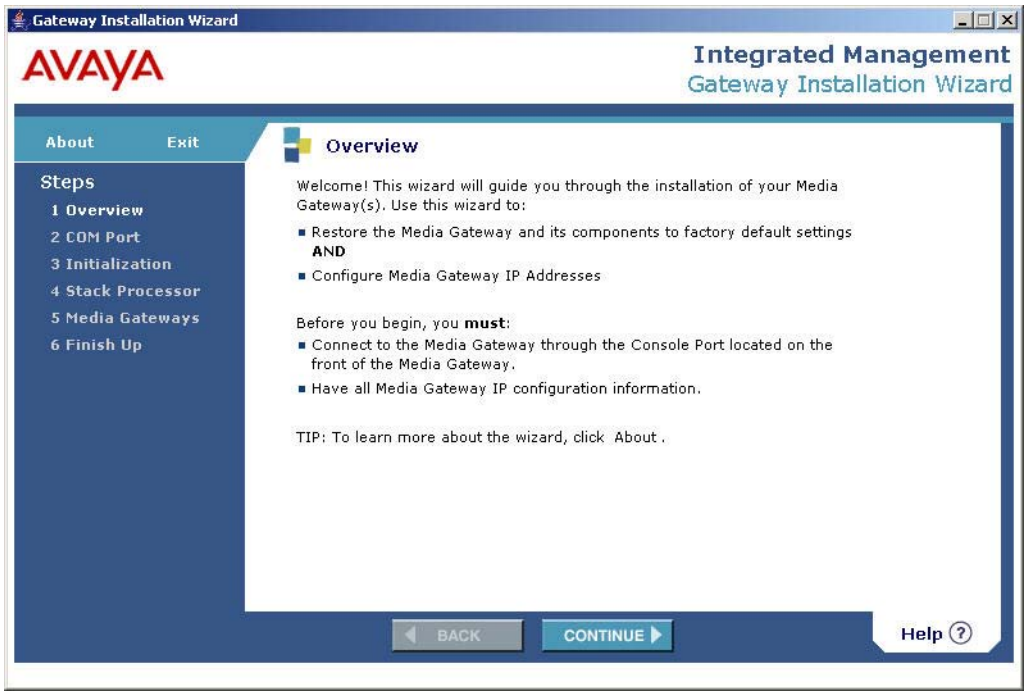
7. The Exit AIW screen appears.



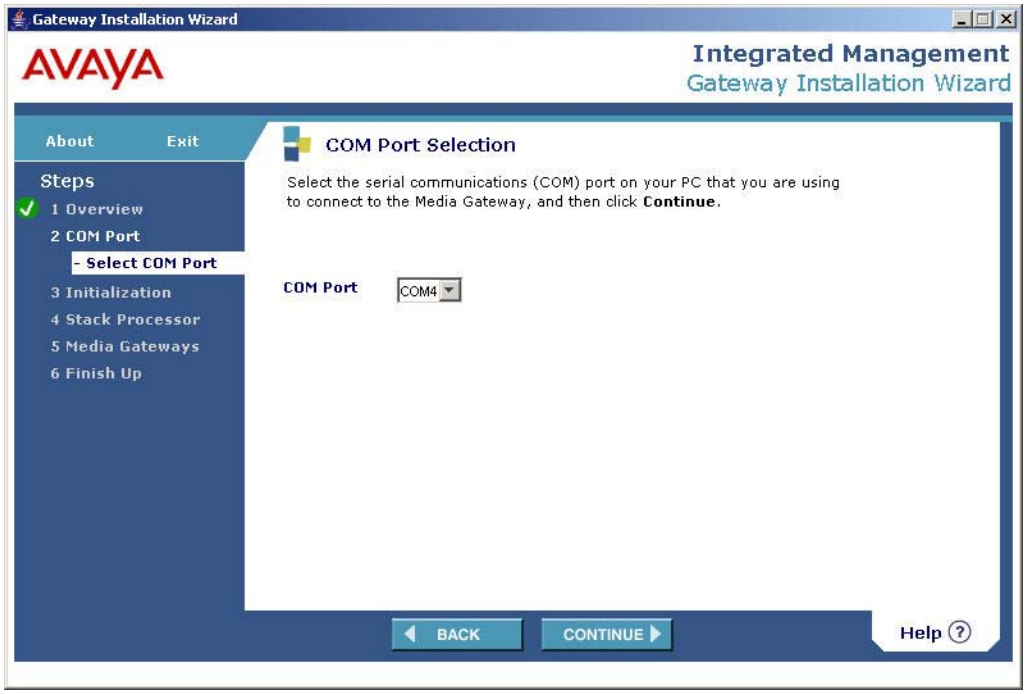
Appendix C: Configuring the G350 using the GIW

This chapter explains how to configure the Avaya G350 Media Gateway using the Gateway Installation Wizard (GIW). The GIW is an automated tool that allows you to perform a streamlined installation and configuration of a standalone G350. You can use the GIW to perform initial configuration of the G350 and to upgrade software and firmware. For instructions on accessing the GIW, see Accessing GIW on page 34.

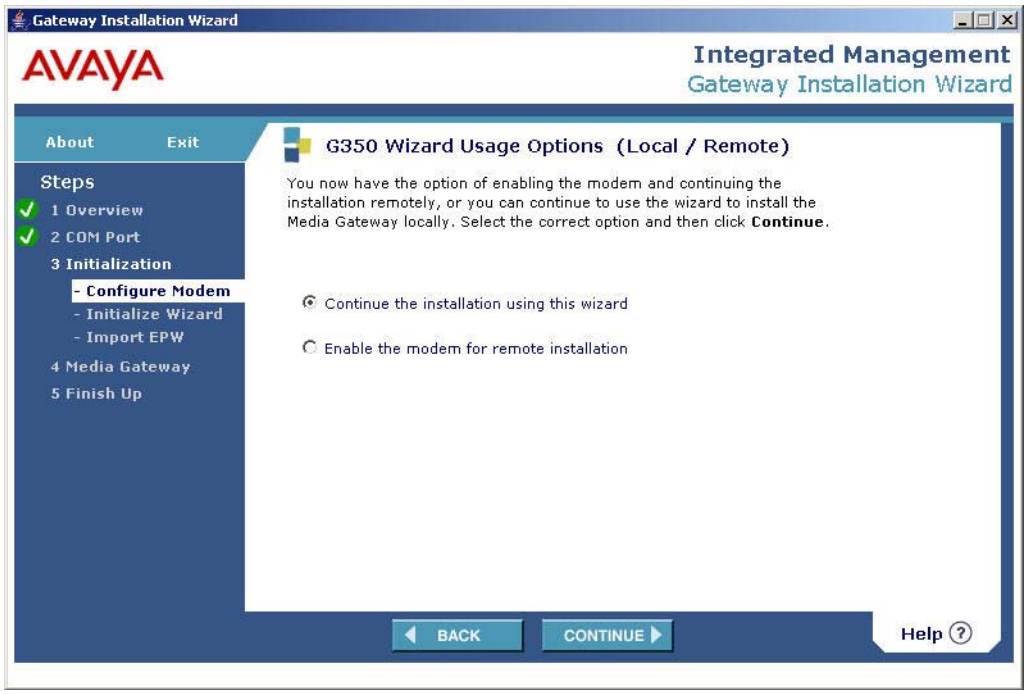
1. When you access the GIW, the first screen that appears is the Overview screen.



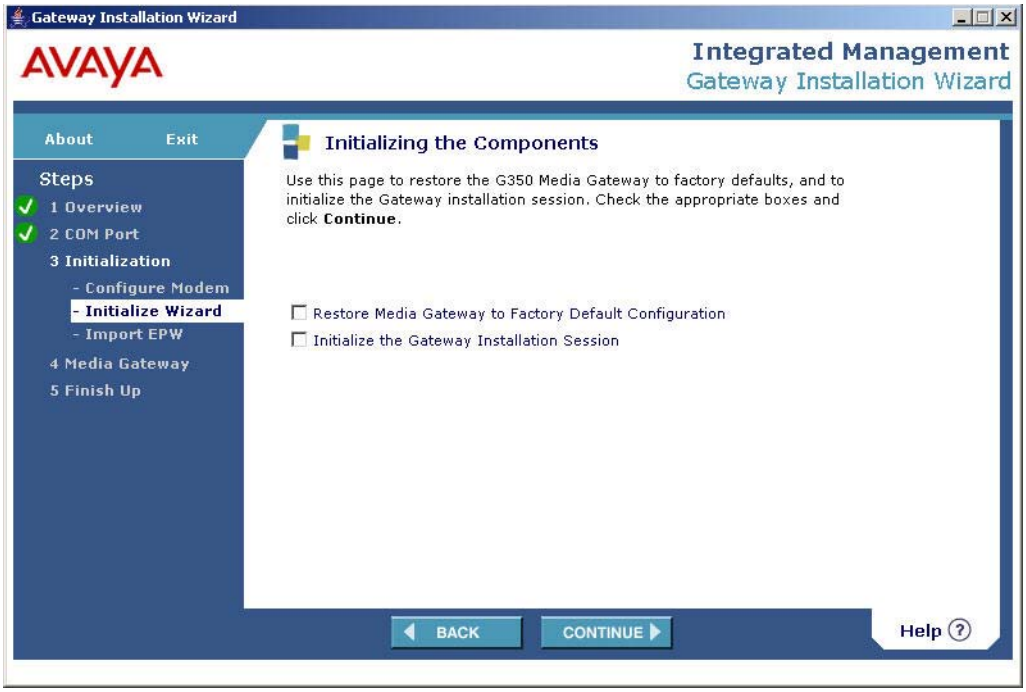
2. Click **Continue**. The COM Port Selection screen appears.



3. Select the COM port on the laptop that you are using the connect to the G350.
4. Click **`Continue`**. The G350 Wizard Usage Options screen appears.

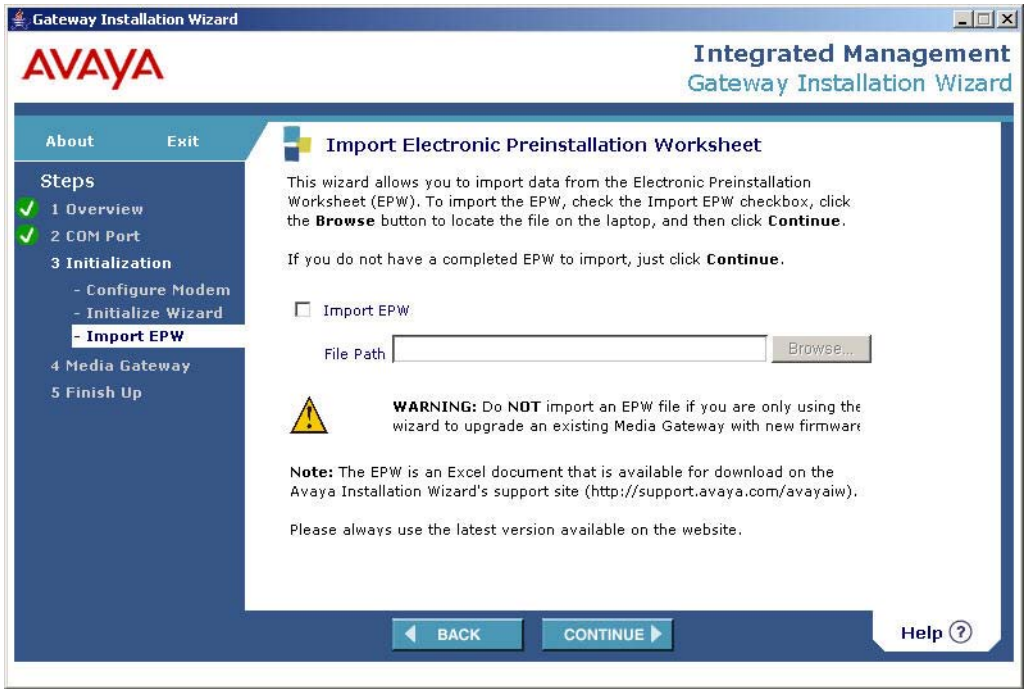


5. Select one of the following options:
   - To configure the G350 via remote configuration, select **`Enable the modem for remote installation`**, then click **Continue**. The Connect Modem screen appears.
   - If you wish to continue the configuration using GIW, select **`Continue the installation using this wizard`**, then click **Continue**. The Initializing the Components screen appears.



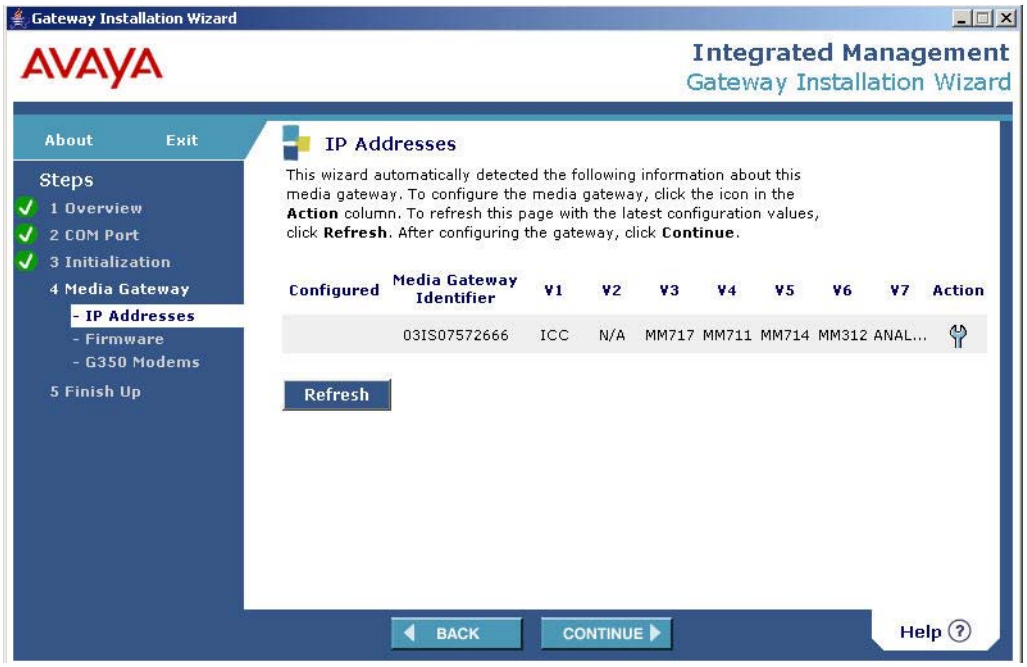
6. Select **Initialize the Gateway Installation Session**.

7. Click **Continue**. The Import Electronic Preinstallation Worksheet screen appears:

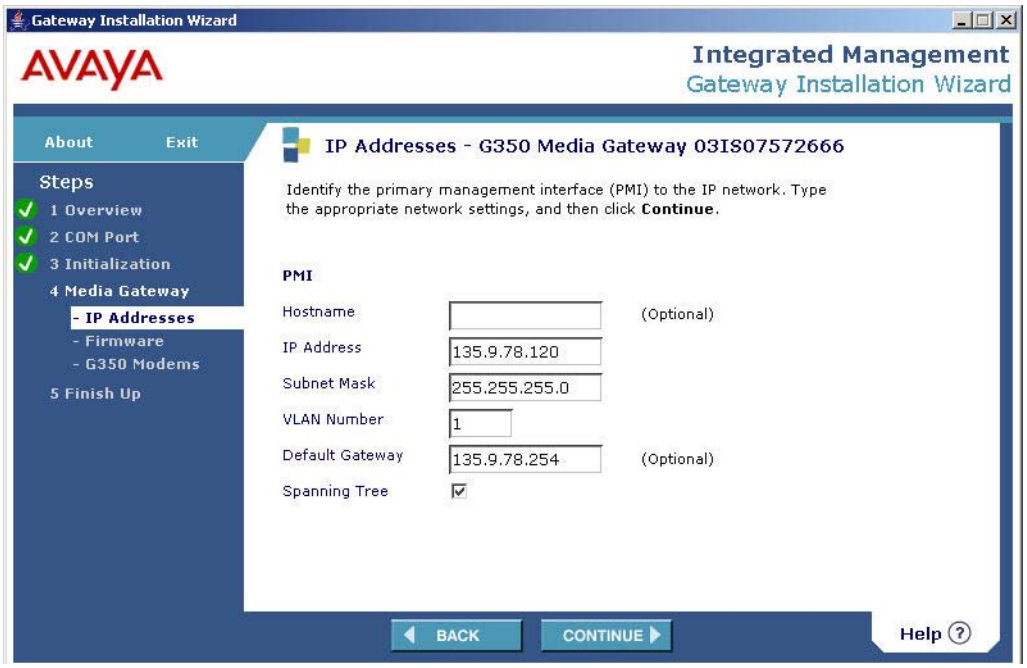


8. If you have an EPW on your laptop, select **Import EPW**. For information on the EPW, see *Installation and Upgrades for the Avaya G350 Media Gateway*, 03-300394.
9. Browse to the EPW file on your laptop. Any values that are included in the EPW will appear as default values from now on as you move through this wizard.

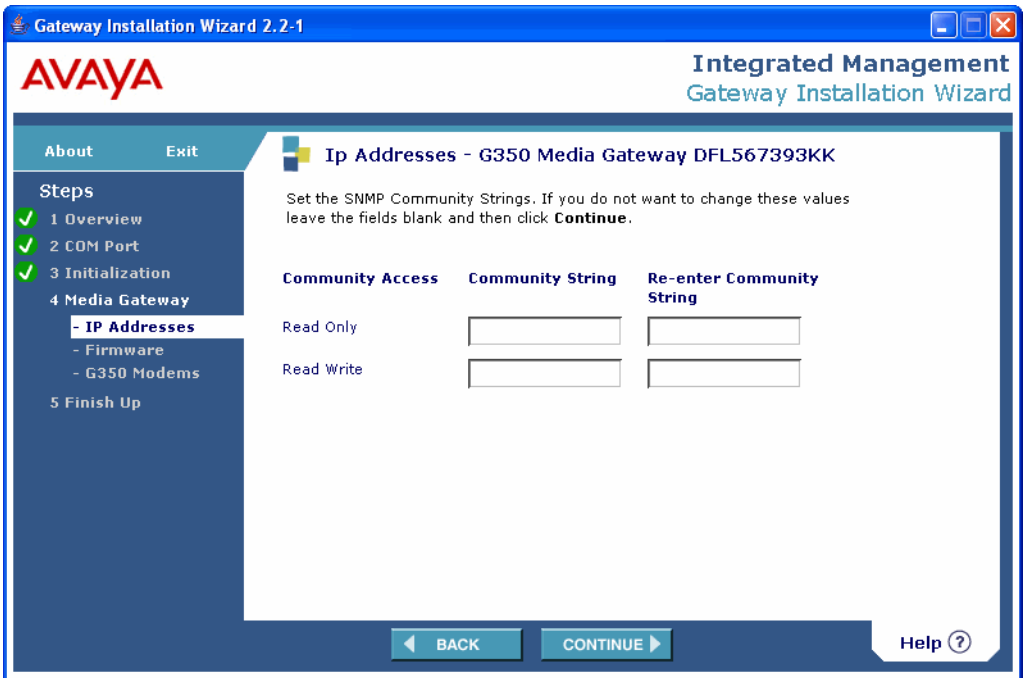
10. Click **Continue**. The IP Addresses screen appears. The IP Addresses screen displays automatically detected information about the G350, such as what media modules are installed in the media modules slots.



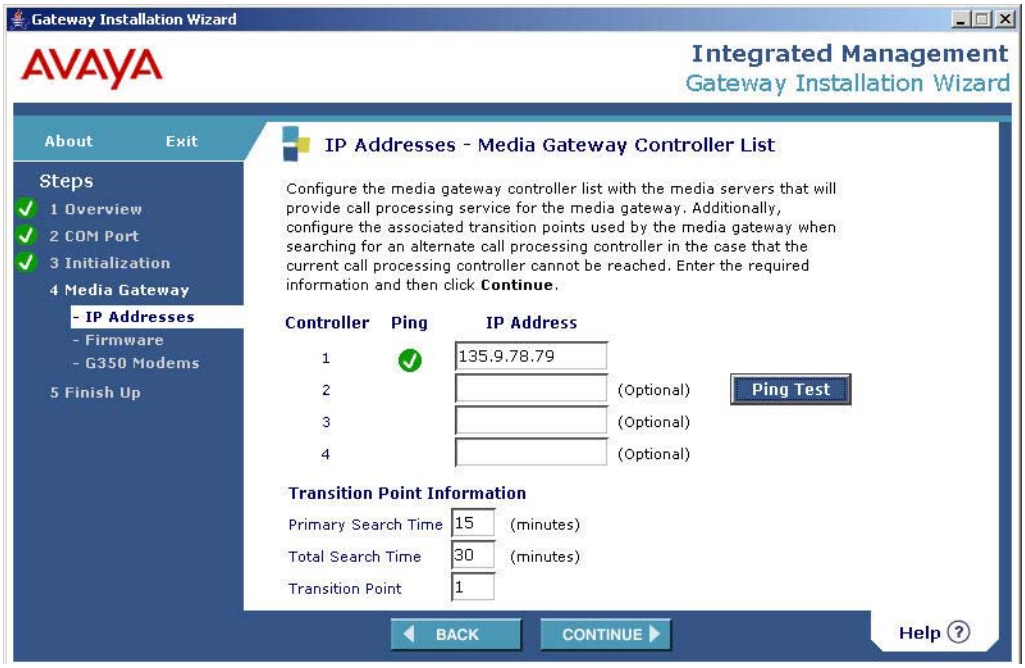
11. Click in the Action column. The PMI screen appears. In the PMI screen, specify the details of the Primary Management Interface (PMI) for the G350. See Configuring the Primary Management Interface (PMI) on page 50.



12. Click **Continue**. The SNMP screen appears. In the SNMP screen, specify SNMP community strings and trap destinations. SNMP traps will be sent to all IP addresses entered in the destination fields. For instructions on configuring SNMP, see Configuring SNMP on page 119.

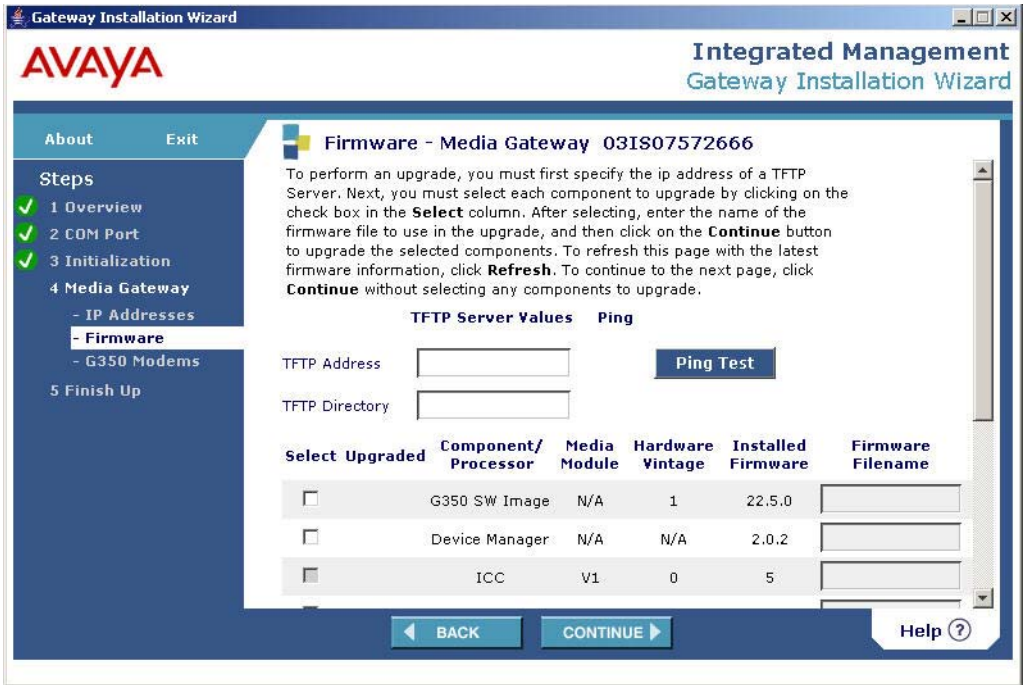


13. Click **Continue**. The Media Gateway Controller List screen appears. In the Media Gateway Controller List screen, specify the IP address of the primary Media Gateway Controller (MGC). You can also specify the IP addresses of up to three additional MGCs (optional). For instructions on MGC configuration, see Configuring the Media Gateway Controller (MGC) on page 51.



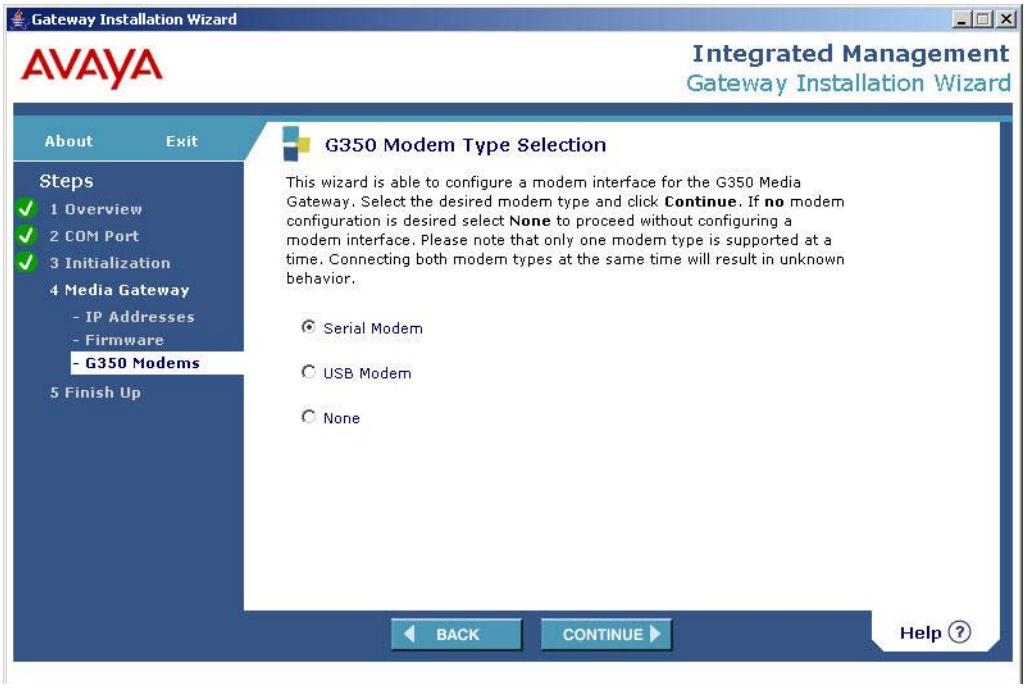
14. Click **Ping Test** to test the accessibility of each MGC.

15. Click **Continue**. The Firmware screen appears:



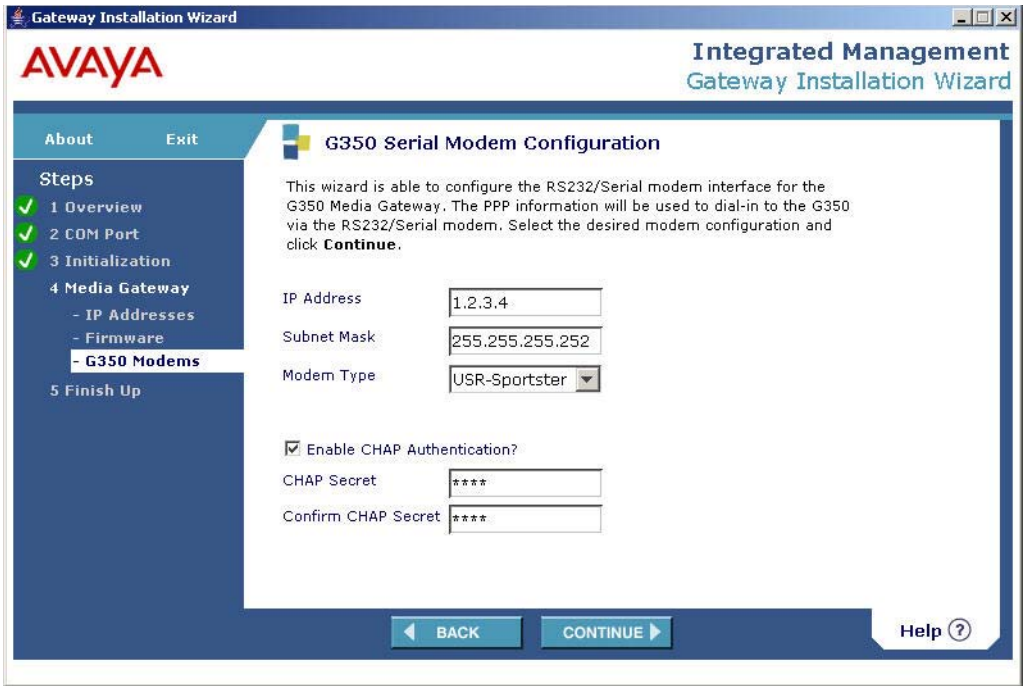
16. In the **TFTP Directory** field, enter the name of the directory on the TFTP server in which the upgrade files are located.
17. In the table, select the **Select** box for all firmware components you want to upgrade. The current version of each component is listed to help you confirm the need for upgrade.
18. Enter the filename of each firmware upgrade file you want to install in each line of the table where you selected the **Select** box.

19. Click **Continue**. The firmware is upgraded and the G350 Modem Type Selection screen appears. Select the modem type you want to use. For more information on using a modem with the G350, see Configuring the G350 for modem use on page 77.

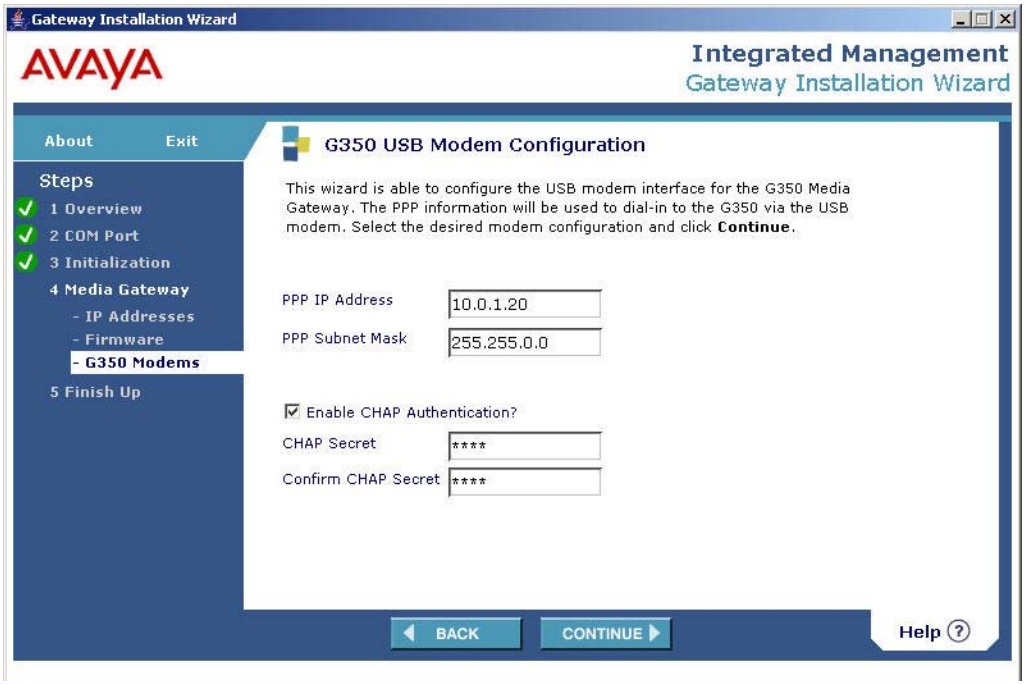


20. Click **Continue**. If you selected **Serial Modem**, the G350 Serial Modem Configuration screen appears. If you selected **USB Modem**, the G350 USB Modem Configuration screen appears. If you selected **None**, the Change Root Password screen appears.

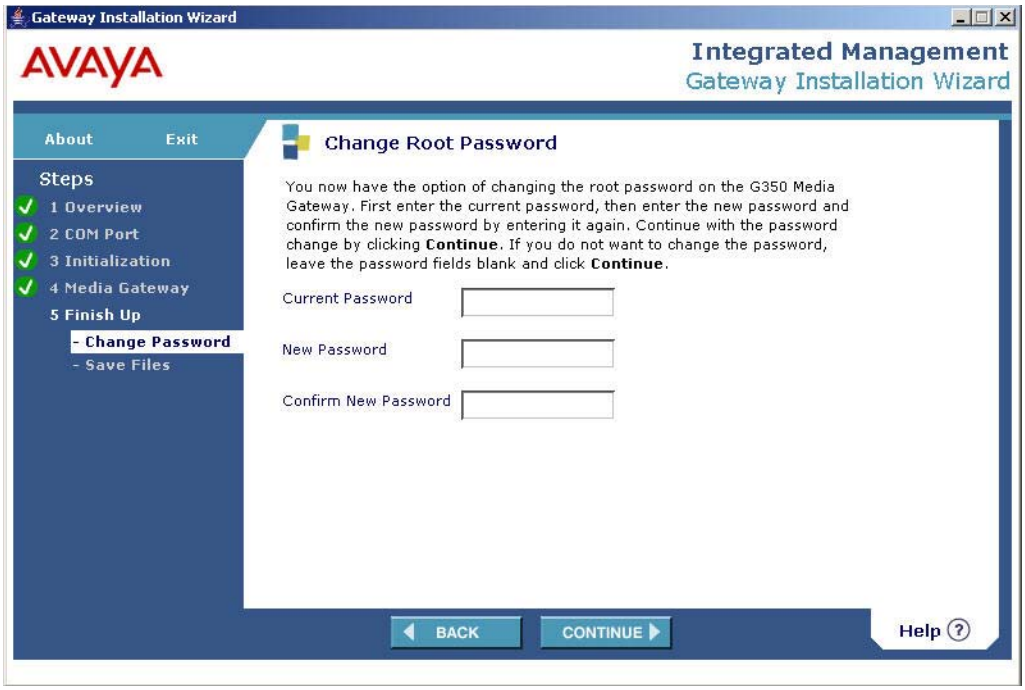
21. If you selected **Serial Modem**, enter the required information in the G350 Serial Modem Configuration screen, then click **Continue**.



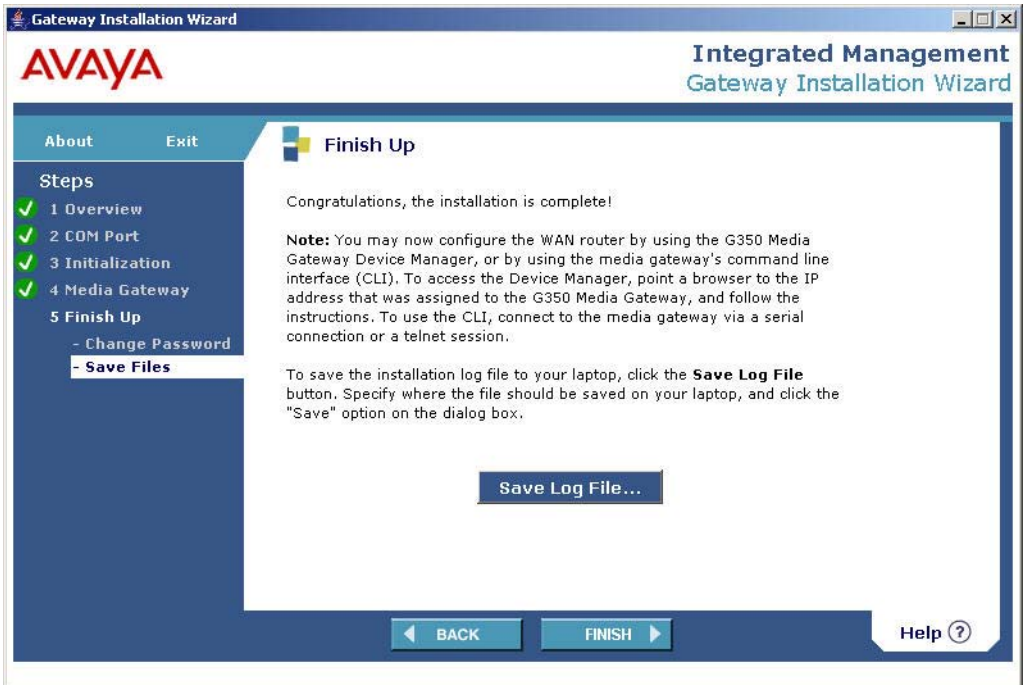
22. If you selected **USB Modem**, enter the required information in the G350 USB Modem Configuration screen, then click **Continue**.



23. Click **Continue**. The Change Root Password screen appears. This screen allows you to change the root password on the G350.



24. Click **Continue**. The Finish Up screen appears:



25. Click **Continue**. The Finish Up screen appears. This screen allows you to save the installation log file to your laptop. To save the installation log file:
    a. Click **Save Log File**. A dialog box appears.
    b. Specify the location on your laptop in which in want to save the log file.
    c. Click **Save**.
26. You have completed the GIW configuration process. Further configuration tasks, as described in this screen, can now be performed either remotely, via a modem that you enabled with GIW, or locally.

Index

Numerical

802.1x protocol 41

A

ARP table
adding entries 189
configuration 189
deleting dynamic entries 189
description 187
dynamic entries. 187
removing entries 189
static entries 187
ASB button 291
Auto-negotiation
FastEthernet port 64
flowcontrol advertisement 62
port speed 63
Autonomous System Boundary Router 195
Avaya Communication Manager
accessing 35
Avaya G350 Media Gateway
system backup 117
Avaya IW
accessing 32
configuration using 32
description 32
laptop configuration for 32
Avaya Site Administration 35

B

Backup interfaces
configuring 97
defining through policy-based routing 275
dynamic bandwidth reporting 101
GRE tunnels as. 167
limitations 98
overview 64
Backup service 117
Bandwidth
displaying 102
dynamic reporting. 101
manual adjustment 195
reducing via RTP header compression 72
setting maximum 102
used to calculate Cost 195
BOOTP
configuration 178
description 177
BOOTstrap Protocol
see BOOTP
BPDU 144
Bridge Protocol Data Units
see BPDU
Bridges
direct handshaking 144
loops 143
Broadcast address 162
Broadcast relay
description 185
directed broadcast forwarding 186
NetBIOS rebroadcast 186
Buttons
ASB 291
RST 291

C

Call admission control, *see* Dynamic CAC
CAM table 136
CCA port. 290
Challenge Handshake Authentication Protocol . . 77, 79
Channel Groups
creating. 87
illustration. 83
mapping 86
CHAP 77, 79
CIR 104
CLI
accessing. 27
accessing from local network. 29
accessing from remote location. 30
accessing with console device 29
accessing with modem. 30
contexts 28
online help 28
remote access with S8300 Media Server 31
Codec 74
Commands
area 196
arp 187, 189
arp timeout 189
async mode interactive 78
async mode terminal 78
async modem-type 78
async reset-modem 77, 78

Commands, (continued)
autoneg 64
backup delay 99
backup interface 99
bandwidth 89, 195
cablelength. 86
channel-group 86
clear arp-cache 189
clear dot1x config 44
clear fragment 202
clear ip route 166
clear ip rtp header-compression 72
clear port mirror 142
clear port static-vlan 135
clear vlan 134, 135
clock source 86
controller slot/port. 85
copy running-config startup-config85, 87, 89, 169, 170, 173
crypto key generate dsa. 39
default-metric. 193, 196
disconnect ssh 39
distribution list 192
distribution-list 193
dscp 280
ds-mode 85
duplex 64
dynamic-cac bbl 101
encapsulation frame relay 95
encapsulation ppp 90
encapsulation pppoe 92
extended-keepalive 99
extended-keepalive failure-retries 100
extended-keepalive interval 101
extended-keepalive source-address 101
extended-keepalive success-retries 100
extended-keepalive timeout 100
fair-queue-limit 76
fair-voip-queue 76
fragment chain 202
fragment size. 202
fragment timeout 202
fragments 202
frame-relay interface-dlci 95
frame-relay lmi 95
frame-relay priority-dlci-group 96, 103
frame-relay traffic-shaping. 95, 104
framing. 86
help 28
icc-vlan 135
idle characters 89
ignore dcd 89
interface 162
interface console 79
interface FastEthernet 63
interface Serial 86, 88, 90, 95

Commands, (continued)
Interface tunnel 172
interface usb-modem 77
interface vlan 135
invert txclock 89
ip address 77, 79, 89, 90, 93, 96, 162
ip admin-state 162
ip bootp-dhcp network 178
ip bootp-dhcp relay 178
ip bootp-dhcp server. 178
ip broadcast-address 162
ip default-gateway 166
ip directed-broadcast 186
ip distribution access-default-action. 192
ip distribution access-list 192
ip icmp-errors 190
ip max-arp-entries 189
ip netbios-rebroadcast 186
ip next-hop-list 281
ip ospf cost 195
ip ospf network point-to-multipoint 84
ip pbr-group. 278
ip pbr-list 276
ip proxy-arp 189
ip rip 193
ip rip poison-reverse 191
ip rip split-horizon 191
ip route 164, 165, 166, 168
ip routing 160
ip rtp compression-connections. 72
ip rtp max-period 72
ip rtp max-time 73
ip rtp non-tcp-mode 73
ip rtp port-range 73
ip tcp decompression-connections 73
ip telnet. 48
ip telnet client 48
ip-rule 280
keepalive 90, 94, 171, 173
linecode 86
name 183, 184, 185, 276
network. 193, 196
next-hop list. 280
next-hop-interface 281
next-hop-ip 281
nrzi-encoding 89
operation 280
owner 276
passive-interface 196
ping 97
ppp authentication. 77, 79
ppp chap hostname 93, 94
ppp chap-secret 77, 79
ppp pap sent-username 92
ppp timeout ncp 90

Commands, (continued)
ppp timeout retry 90
pppoe-client persistent delay 93
pppoe-client persistent max-attempts 93
pppoe-client service name. 93
pppoe-client wait-for-ipcp 93
priority-queue. 76
redistribute 194, 196, 198
router ospf 196
router rip 194
router vrrp 200
set dot1x max-req 44
set dot1x quiet-period 44
set dot1x re-authperiod 43
set dot1x supp-timeout 44
set dot1x system-auth-control 42
set dot1x tx-period 44
set etr 117
set port. 62
set port auto-negotiation-flowcontrol-advertisement 62
set port classification 149
set port disable 62
set port dot1x initialize 44
set port dot1x max-req 44
set port dot1x port control 42
set port dot1x port-control 42
set port dot1x quiet-period. 44
set port dot1x re-authentication 43
set port dot1x server-timeout 45
set port dot1x supp-timeout 44
set port dot1x tx-period 44
set port duplex 62
set port edge admin state 62
set port enable 62
set port level 62
set port mirror 142
set port name. 62
set port negotiation 62
set port point-to-point admin status. 63
set port redundancy. 140
set port redundancy-intervals 139, 140
set port spantree 146
set port speed 63
set port static-vlan 135
set port vlan 135, 136
set port vlan-binding-mode 136
set prt dot1x re-authenticate 44
set qos bearer 74
set qos control 74
set qos rsvp 75
set qos signal. 74
set radius authentication disable 40
set radius authentication enable 40
set radius authentication retry-number 40
set radius authentication retry-time. 40

Commands, (continued)
set radius authentication secret. 40
set radius authentication server 40
set radius authentication udp-port 40
set spantree 146
set terminal recovery password. 48
set trunk 136
set vlan 136
shortest-path-first algorithm 194
show cam vlan 136
show controllers 85, 96
show dot1x 45
show dynamic-cac. 102
show extended-keepalive 101
show fragment 202
show frame-relay 96
show icc-vlan 135
show interface tunnel 174
show interface usb-modem 78
show interfaces 90, 95
show interfaces vlan 136
show ip active-lists 282
show ip arp 189
show ip icmp 190
show ip interface 97
show ip next-hop-list all 282
show ip pbr-list 282
show ip pbr-list all detailed 282
show ip reverse-arp 189
show ip route 166
show ip route best-match 166
show ip route static 166
show ip route summary 166
show ip rtp header-compression 73
show ip ssh 39
show ip vrrp. 201
show ip-rule. 283
show list 282
show next-hop 281, 283
show port classification 149
show port dot1x 45
show port dot1x statistics 46
show port mirror. 142
show port redundnacy 140
show port-vlan-binding. 136
show ppp authentication 94
show qos 74
show qos-rtcp 75
show radius authentication. 41
show running-config 97
show spantree 147
show startup-config 97
show trunk 136
show vlan. 136
show-ds 85

Commands, (continued)
show-rule 280
shutdown 64, 78, 79
speed 64, 77, 78
ssh enable 39
ssh-client known-hosts 39
telnet 31
timeout absolute 78, 79
timers basic 194
traceroute 166
traffic-shape rate 64
transmitter-delay 89
tunnel checksum 174
tunnel destination 172
tunnel DSCP 174
tunnel key 174
tunnel path-mtu-discovery 172
tunnel source 172
tunnel TTL 174
voip-queue 74, 76
voip-queue-delay 74, 76
Committed Burst size 104
Committed Information Rate
see CIR
Computer, connecting to fixed router port 61
CON port
see Console port
Configuration
startup 97
using Avaya IW 32
using GIW 34
Console device
configuring console port for use with 78
configuring console port to detect 78
CONSOLE port 291
Console port
assigning IP address 79
configuring for modem use 31
configuring for telnet access 79
configuring for use with console device 78
configuring for use with modem 79
configuring to detect console device 78
configuring to detect modem 78
connecting console device 29
connecting modem 31
default settings 79
description 78
entering interface context 79
GIW configuration via 34
setting authentication method 79
setting PPP baud rate 78
Contexts 28
Controller
configuring mode 85
displaying configuration 85
entering context 85
Cost 195
Crypto lists 214
Crypto maps 213

D

Data Link Connection Identifier
see DLCI
DE pre-mark 104
Default gateway
defining 166
removing 166
DeMilitarized Zone
see DMZ
DHCP
configuration 178
description 177
DHCP/BOOTP relay 178
Directed broadcast forwarding 186
Discard Eligible
see DE pre-mark
Discard routes 165
Distribution access lists 192
DLCI
configuring for frame relay sub-interface 95
OSPF mapping 103
Priority
see Priority DLCI
DMZ 161
DSA 38
DSCP
as policy-based routing rule criteria 280
in GRE header 174
routing based on 274
Duplex, configuring duplex type 62
Dynamic CAC 101
Dynamic Host Configuration Protocol
see DHCP
Dynamic routes
deleting 166
redestributing 197

E

E1/T1 lines
connecting to WAN media module 81
default settings 88
E1/T1 ports 85
EAP 41
EAP over RADIUS 41
EAPOL 41

ECMP . . . 195
Emergency Transfer Relay
  see ETR
ETH LAN port . . . 291
ETH WAN port . . . 290
Ethernet ports
  configuring duplex type . . . 62
  configuring link negotiation protocol . . . 62
  configuring switch port . . . 62
  connecting devices to . . . 61
  list of . . . 61
  port redundancy . . . 139
  WAN Ethernet port
    see WAN Ethernet port
ETR
  deactivating . . . 117
  description . . . 117
  displaying status . . . 118
  LED . . . 117
  manual activation . . . 117
  setting state . . . 117
Excess Burst size . . . 104
Extended keepalive . . . 99, 273
Extensible Authentication Protocol . . . 41

F

Fair VoIP queue . . . 76
FastEthernet interface . . . 161
  checking status . . . 99
  configuring PPPoE . . . 91
  dynamic bandwidth reporting . . . 101
  extended keepalive . . . 99
FastEthernet port . . . 100
  auto-negotiation . . . 64
  configuring duplex type . . . 64
  configuring interface . . . 63
  configuring port speed . . . 64
  firewall connected . . . 161
  VPN connected . . . 161
Federal Information Processing Standard, *see* FIPS
FIPS
  overview . . . 289
Firewall . . . 161
Fixed analog trunk port . . . 117
Fixed ports
  CCA . . . 290
  CONSOLE . . . 291
  ETH LAN . . . 291
  ETH WAN . . . 290
  LINE 2 . . . 290
  LINE1 . . . 290
  TRUNK . . . 290
  USB . . . 291
Flowcontrol advertisement . . . 62
Fragmentation
  as map class parameter . . . 104
  configuration . . . 202
  description . . . 201
  GRE tunneling . . . 172
  reassembly . . . 202
Frame relay . . . 81
  configuring sub-interfaces . . . 95
  displaying configuration . . . 96
  egress queuing mechanism . . . 105
  enabling traffic shaping . . . 104
  ingress queuing mechanism . . . 105
Frame relay encapsulation
  configuring on WAN port . . . 95
  down status . . . 98
  establishing Layer 3 interface . . . 165
  illustration . . . 83
  supported features . . . 103
  supported on Serial interfaces . . . 162
  supported on serial interfaces . . . 83
Front panel
  buttons, description . . . 291

G

General context . . . 28
Generic Routing Encapsulation, *see* GRE tunneling
Gigabit Ethernet port
  location . . . 61
  port redunancy . . . 139
GIW
  accessing . . . 34
  configuration using . . . 34
  description . . . 34
  installation on laptop . . . 34
GRE tunneling
  adding checksum . . . 174
  adding ID keys . . . 174
  applications . . . 167
  assigning DSCP . . . 174
  assigning TTL . . . 174
  checking tunnel status . . . 171, 173
  compared to VPN . . . 167
  configuring tunnel . . . 172
  displaying tunnel information . . . 174
  dynamic MTU discovery . . . 172
  optional features . . . 171
  overview . . . 161, 167
  preventing loops . . . 168
  routing packets to tunnel . . . 168
GRE tunnels
  as next hop . . . 281
  dynamic bandwidth reporting . . . 101

H

Hello packets 196
High Preference static routes 164

I

ICC-VLAN 135
ICMP
  errors 190
Ingress Access Control List 273
Ingress QoS List 273
Interfaces
  adjusting bandwidth 195
  administrative status 64
  applying PBR lists 278
  assigning Cost 195
  authentication 193
  backup 64
  configuration 160, 162
  configuration examples 162
  disabling 163
  displaying information 97
  duplex type 64
  dynamic bandwidth reporting 101
  FastEthernet 161
  frame relay 95
  GRE tunnel, *see* GRE tunneling
  IP
    see IP interfaces
  Layer 2 . . . . . 161, 163
  Layer 3 165
  logical 162
  Loopback 161, 273, 278
  metrics 196
  network type 196
  physical 161
  priority 196
  Serial 162
  serial
    see Serial interfaces
  speed 64
  switching 161, 162
  testing configuration 96
  USP WAN 161
  virtual 83, 161
  WAN 161
IP address
  defining 162
  storing in ARP table 187
IP interfaces 162
  configuration 162
  configuration examples 162
  disabling 163
  setting administrative state 162
  types 162
  updating broadcast address 162
IP Security, *see* IPSec
IPSec 203
ISAKMP
  peer information 211
  policies 209

K

keepalive
  configuring on PPP WAN line 90
  configuring on PPPoE interface 94
Keepalive, extended 99, 273
Keepalive, GRE tunnel 171

L

LAN 161
Layer 2 interfaces 163
Layer 2 logical interfaces 162
Layer 2 virtual interfaces 161
Layer 3 interfaces 165
LEDs
  ETR 117
LINE 1 port 290
LINE 2 port 290
Link Fragmentation and Interleaving 104
Link-state algorithm 194
LMI parameters 95
Load balancing
  ECMP 195
  VRRP 198
Local Management Interface
  see LMI parameters
Logging
  VPN 219
Logical interfaces 162
Loopback interface 161, 273, 278
Loops
  defined 143
  preventing in GRE tunneling 168
  preventing in RIP 191
Low Preference static routes 164

M

MAC addresses
- storing in ARP table . . . 187

Map classes
- applying to all configured Permanent Virtual Channels . . . 104
- default . . . 104
- number that can be configured . . . 104
- parameters . . . 104

Media modules
- MM314 . . . 41, 61
- MM340 . . . 85, 161
- MM342 . . . 85, 88, 161
- USP WAN
  - *see* MM342 media module
- WAN . . . 85

Metrics . . . 198

MGC
- accessing . . . 35
- reporting bandwidth to . . . 101
- running Avaya Communication Manager . . . 35

MM314 media module
- 802.1x protocol . . . 41
- Ethernet ports . . . 61

MM340 media module
- configuring . . . 85
- E1/T1 WAN interface . . . 161

MM342 media module
- configuring . . . 88
- USP WAN interface . . . 161

Modem
- configuring console port for use with . . . 79
- configuring console port to detect . . . 78
- configuring type on console port . . . 78
- connecting to console port . . . 31
- connecting to S8300 Media Server . . . 31
- connecting to USB port . . . 30
- connecting via USB modem . . . 31
- displaying USB modem status . . . 78
- serial . . . 78
- USB . . . 77

Multipoint topology support . . . 84

N

Nested tunneling . . . 168

NetBIOS . . . 186

Next hop lists
- applying to policy-based routing rules . . . 280
- backup routes . . . 275
- editing . . . 281
- entries . . . 281
- overview . . . 280

Next-hops
- adding . . . 164
- configuring . . . 164
- static routes . . . 163

O

Open Shortest Path First protocol
- *see* OSPF

OSPF
- advertising static routes . . . 164
- compared to RIP . . . 190, 194
- configuration . . . 196
- default metric . . . 198
- description . . . 194
- displaying information . . . 197
- DLCI mapping . . . 103
- dynamic Cost . . . 195
- enabling on network . . . 196
- enabling on system . . . 196
- interface authentication password . . . 196
- limitations . . . 195
- metrics . . . 196
- priority . . . 196
- redistributing routing information . . . 196
- suppressing updates . . . 196
- using with RIP . . . 197

OSPF Autonomous System Boundary Router . . . 195

P

Password Authentication Protocol . . . 77, 79

Passwords
- changing . . . 37
- overview . . . 36
- recovery password . . . 48

PBR lists
- attaching to interface . . . 278
- attaching to Loopback interface . . . 273, 278
- creating . . . 276
- deleting . . . 282
- editing . . . 276
- editing rules . . . 280
- modifying . . . 282
- name . . . 183, 184, 185, 276
- rule criteria . . . 279
- rules . . . 279

Permanent routes . . . 165

Ping . . . 97

Point to Multi-Point topology . . . 84

Point-to-Point frame relay . . . 81, 84

Poison-reverse . . . 191, 193

Policy-based routing
applications 274
attaching list to interface 278
based on DSCP 274
distinguishing between voice and data 274
overview 273
routing to GRE tunnel 168
rules 279
used to define backup routes 275
VoIP 274
Policy-based routing lists, *see* PBR lists
Port mirroring
configuration 142
configuration examples 142
description 142
Port redundancy
configuration 140
configuration examples 141
description 139
displaying information 140
enabling 140
secondary port activation 139
switchback 140
Ports
alternate 144
analog line 117
assigning static VLANs 135
auto-negotiation mode 63
backup 144
CCA 290
classification 149
configuring administrative state 62
configuring E1 port 85
configuring name 62
configuring speed 63
configuring T1 port 85
configuring VLAN tagging mode 136
CONSOLE 291
disabling 62
displaying VLAN binding mode information 136
enabling 62
ETH LAN 291
ETH WAN 290
Fast Ethernet
see Fast Ethernet port
FastEthernet
see FastEthernet port
LINE 1 290
LINE 2 290
managing connection type 63
mirroring
see Port mirroring
opening traffic 144
Ports, (continued)
redundancy
see Port redundancy
roles in RSTP 145
setting priority level 62
TRUNK 290
USB 291
USP
see USP ports
PPP
as default WAN protocol 85
configuring on WAN line 90
connection 30, 31
establishing Layer 3 interface 165
over channeled and fractional E1/T1 81
over USP 81
supported on serial interfaces 83, 162
PPP over Ethernet, *see* PPPoE
PPPoE 81
description 91
shutting down client 94
Priority DLCI
applying map classes 104
configuring 96, 103
description 103
Priority queuing
description 105
general 103
Priority VoIP queuing 76
Privilege levels
changing 37
description 37
Proxy ARP 189
PTMP
see Point to Multi-Point topology

Q

QoS
*see also*ee alsoPolicy
configuration 74
displaying parameters 74
fair packet scheduling 76
frame relay queuing mechanisms 105
Priority DLCI
see Priority DLCI
queue sizes for VoIP traffic 74
Weighted Fair VoIP Queuing 76, 82
Queues
fair packet scheduling 76
Weighted Fair VoIP Queuing 76, 82

R

RADIUS authentication 36, 40
Rapid Spanning Tree protocol
  see RSTP
Recovery password 48
RIP
  advertising static routes 164
  authentication type 193
  compared to OSPF 194
  configuration 193
  default metric 198
  description 190
  distribution access lists 192
  enabling 194
  learning default route 193
  limitations 193
  poison-reverse 191
  preventing loops 191
  redistributing routing information 194
  setting timers 194
  specifying networks 193
  specifying version 193
  split-horizon 191
  using with OSPF 197
  versions supported 190
RIPv1 191
RIPv2 191
Route redistribution 190
  configuration 198
  description 197
  metric translation 197
  metrics 198
Router
  backup 198
  computing path 194
  configuring BOOTP 177
  configuring broadcast relay 185
  configuring DHCP 177
  connecting to fixed router port 61
  defining default gateway 166
  description 160
  determining shortest path 195
  disabling 160
  enabling 160
  enabling RIP 194
  Ethernet port 61
  features 160
  fragmentation
    see Fragmentation
  hello packets 196
  ID 196
  interfaces 161
  load balancing 198
Router, (continued)
  OSPF Automomous System Boundary 195
  redundancy 198
  RIP
    see RIP
  virtual 198, 200
Router port, connecting to 61
. 166
Routes
  *see also*ee alsoStatic routes, Dynamic routes . . 166
  displaying 166
  distribution policy rules 193
  metrics 193
  setting route preference 168
  tracing 166
Routing Information Protocol
  see RIP
Routing table
  configuration 166
  deleting dynamic entries 166
  deleting static routes 163
  description 163
  dispaying for destination address 166
  displaying information 166
RSA authentication 38
RST button 291
RSTP
  description 143
  fast network convergence 145
  features 144
  role of ports 145
RSVP 75
RTCP 72
RTP
  configuring 72
  configuring UDP port range for 73
  decompression 72
  header compression 72

S

S8300 Media Server
  accessing G350 via 31
  connecting modem 31
  remote connection to 31
SCP 39
Security
  overview 36
  special features 48
  VLANs 135
Serial interfaces 162
  configuring encapsulation 87
  default encapsulation 87
  dynamic bandwidth reporting 101
  entering context 86, 88

set vlan . . . 133
show ip ospf commands . . . 197
Spanning tree
configuration . . . 146
configuration examples . . . 147
description . . . 143
disabling . . . 144
Split-horizon . . . 191, 193
SSH
configuration . . . 39
overview . . . 38
Static routes
advertising . . . 164
configuring next-hops . . . 163, 164
deleting . . . 163, 164
description . . . 163
discard route . . . 165
displaying . . . 166
dropping packets to . . . 165
establishing . . . 166
High Preference . . . 164
inactive . . . 163
IP addressed next-hops . . . 165
load-balancing . . . 164
Low Preference . . . 164
permanent . . . 165
redistributing to RIP and OSPF . . . 197
removing . . . 166
types . . . 164
via interface . . . 165
Switch
connecting to fixed router port . . . 61
displaying configuration . . . 97
displaying VLAN tagging information . . . 136
displaying VLANs . . . 136
interface . . . 161, 162
Switch ports
configuring . . . 62
location . . . 61
Switchback . . . 140
Switching
configuring . . . 131
interface . . . 161
Switching interface . . . 162

T

TCP
compression . . . 73
TCP/IP connection . . . 30, 31
Telnet
accessing console port . . . 79
accessing G350 via . . . 30, 31
accessing S8300 via . . . 31
enabling and disabling access . . . 48
Time slots, mapping . . . 86
Traffic marking . . . 104
Traffic shaping
activating on frame relay interface . . . 95
configuring within map classes . . . 104
description . . . 104
DLCI . . . 96
enabling on frame relay interface . . . 104
parameters . . . 104
per Virtual Channel . . . 103
WAN Ethernet port . . . 64
TRK port
see Fixed analog trunk port
TRUNK port . . . 290
TTL . . . 174

U

UDP
probe packets . . . 166
treating packets like RTP packets . . . 72
Unframed E1 . . . 81
USB port . . . 291
configuring for modem use . . . 30
connecting modem . . . 30
description . . . 77
enabling . . . 77
parameters . . . 77
resetting . . . 77
setting authentication method . . . 77
setting ip address . . . 77
setting PPP baud rate . . . 77
User authentication . . . 36
SSH . . . 38
Usernames
configuring . . . 37
overview . . . 36
removing . . . 37
USP ports
configuring . . . 88
illustration . . . 84
USP WAN lines . . . 81
default settings . . . 90
USP WAN media module
see MM342 media module . . . 88

V

via interface static routes . . . 165
Virtual Channels
applying map classes . . . 104
assigning by QoS level . . . 103
described . . . 103
Virtual interface . . . 161

Virtual Private Network
see VPN
Virtual Private Network, *see* VPN
Virtual router 198, 200
Virtual Router Redundancy Protocol
see VRRP
Virtual topological networks 132
Vlan 1 161
VLANs
assigning to ports 135
configuration 135
configuration examples 136
deleting 135
description 132, 162
DHCP/BOOTP requests 178
displaying configuration and statistics 136
entering configuration mode 135
ICC-VLAN 135
ingress security 135
multi VLAN binding 134
multiple interfaces 178
switching interface 161, 162
table 134
tagging 133
VLMS 191
VoIP
assigning to unique Virtual Channel 103
enabling queuing 74
fair packet scheduling 76
overivew 71
PPP configuration example 106
queue delay 74
queue priority 105
queue size 74
routing based on 274
RSVP protocol 75
Weighted Fair VoIP Queuing 76, 82
VPN 161, 167
configuration 204
crypto maps 213
crypto-lists 214
intervention 219
ISAKMP peer information 211
ISAKMP policies 209
license file 208
loggin 219
maintenance 218
overview 203
prerequisites 208
status 218
transform-sets 210
VRRP
configuration 200
configuration example 199
description 198

W

WAN
backup interfaces 99
checking interface status 99
configuration example 105
default encapsulation 90
default protocol 85
dynamic bandwidth reporting 101
extended keepalive 99, 273
features 81
initial configuration 85
interfaces 161
overview 81
PPP 85
PPP configuration 90
testing configuration 96
WAN endpoint device
connecting to fixed router port 61
WAN Ethernet port
backup interfaces 64
configuring 63
traffic shaping 64
Weighted Fair VoIP Queuing 76, 82
WFVQ
see Weighted Fair VoIP Queuing