Avaya G350 Media Gateway

CLI Reference

555-245-202
Issue 3
January 2005

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

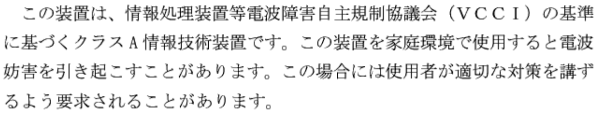
European Union Declarations of Conformity

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

Overview

The *Avaya G350 Media Gateway CLI Reference* describes the commands used to configure and manage the Avaya G350 Media Gateway after it is already installed. For instructions on using these commands to configure and manage the G350, refer to *Administration of the Avaya G350 Media Gateway*, 555-245-501.

Audience

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

Using this book

This book describes how to use the G350 Command Line Interface (CLI) and provides a reference to the CLI commands. Each command description contains:

- The command name
- A short description of the purpose of the command
- The following sections:
  - **Syntax** - This section describes the correct syntax for the command.
  - **Parameters -** This section lists and describes elements of the command syntax, such as parameters, their definitions, and allowed values.
  - **User Level** - This section shows the lowest access level for which the command is accessible. There are three access levels: User (read-only), Configure (read-write), and Supervisor (admin).
  - **Context** - This section shows the contexts from which the command can be executed.
  - **Example** - This section provides an example of the use of a command, and, where applicable, the output display. This section does not appear if the syntax and output are simple.
  - **Output Fields** - This section describes the fields in the command output, if applicable.

Conventions

The following are the conventions used in this book to represent syntax and examples:

Display Type	Description
Screen Display text	Text represented in this format is displayed by the CLI.
`User entered text`	Text represented in this format is entered by the user.
`Variable`	This format indicates a variable argument as it is entered by the user.
`Variable in text`	This format indicates a variable argument discussed in the Parameters section.
`[]`	Syntax elements grouped by square brackets are optional.
`|`	Syntax elements separated by a pipe are mutually exclusive. Choose one of the elements separated by the pipe.
`{}`	These braces are used to group syntax elements, where necessary, to eliminate ambiguity in the syntax. For example, if a keyword and an argument together constitute one of a set of mutually exclusive elements, the keyword and argument are grouped with braces and separated from the other options with a pipe.

Downloading this book and updates from the Web

You can download the latest version of the *Avaya G350 Media Gateway CLI Reference 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 also 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 **555-245-202**, 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
Installation and Upgrades for the Avaya G350 Media Gateway	03-300394
Administration of the Avaya G350 Media Gateway	555-245-501
Avaya G350 Media Gateway Glossary	555-245-301
Quick Start for Hardware Installation for the Avaya G350 Media Gateway	03-300148
Maintenance of the Avaya G350 Media Gateway	555-245-105

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

Ensure that you mention the name and number of this book, *Avaya G350 Media Gateway CLI Reference*, 555-245-202.

Chapter 1: User Levels and Contexts

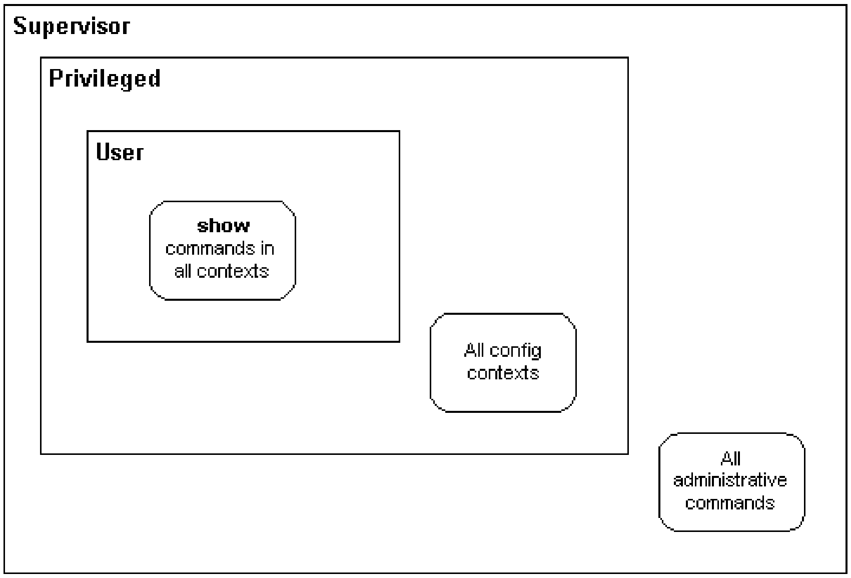
The G350 Command Line Interface (CLI) consists of commands that are divided into logical contexts. These contexts enable you to view and configure the G350 Media Gateway more efficiently. A context can be a particular interface of the media gateway, or it can be a specific function with all its related commands.

The contexts you can enter and the commands you can access, depend on the user level from which you log in to the CLI.

For example, you can use all **show** commands in User mode. To configure the Avaya G350 Media Gateway, you must be in Supervisor or Privileged mode.

The following figure illustrates the relationship between the user levels and the contexts.

Figure 1: Relationship between User Levels and Contexts



After logging in, type **tree** to see a list of all the commands that are accessible at your user level. Type **help** to see the list of commands available in the current context.

User Levels

The following are the user levels that control access to the various parts of the CLI:

Level	Access	Description
User	read-only	User level is a general access level used to display system parameter values. This level complies with the Read Only restrictions level.
Privileged	read-write	Privileged level is used to access configuration options. This level complies with the Read and Write restrictions level.
Supervisor	admin	Supervisor level is used for highly secured operations, such as adding a new user account, showing the PPP chap secret, and setting the device policy manager source.

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 root context. Commands that can be executed from any context in the system are listed as having the *general* context.

Interface contexts

Each interface has its own context in the CLI, which you use to manage the interface. The set of commands related to an interface are only accessible from its interface context. For example, in order to configure a Loopback interface, you must first enter the Loopback context. You enter the Loopback context using the interface command with an interface identifier such as **`interface loopback 1.`**

When an interface has only one sub-interface, the commands for the sub-interface are available from the context of the parent interface. This is called unified configuration. When there are multiple sub-interfaces, you must enter the context of a particular sub-interface in order to configure the sub-interface.

For example, when you create a new VLAN interface 1, the sub-interface VLAN 1.0 is also created. In this case, you can execute sub-interface context commands such as **`ip admin-state`** from the parent context. If you add a second sub-interface VLAN 1.1, then you can only execute sub-interface commands from the context of the sub-interface.

If you are in Supervisor or Privileged mode, you can enter any of the following interface contexts:

- Interface Console
- Interface USB
- Interface Fast Ethernet
- Interface VLAN
- Interface Serial
- Interface Loopback
- Interface Tunnel

Entering an Interface

You enter an interface context using the **`interface`** command, followed by the type of interface, and the interface specification. For the Console interface there is no interface specification.

Interface types include:

- FastEthernet
- Serial
- VLAN
- Loopback
- Console
- USB
- Tunnel

An interface is specified with the following syntax:

```
interface_num[.ip_interface] [if_link_type]
```

For a complete discussion of the **`interface`** command syntax, see the **`interface`** command description.

Command line prompts

The command line prompt is always prefixed with the hostname of the media gateway. If the media gateway is registered, then the prompt is **hostname-media_gateway_number**. Otherwise, the prompt is **hostname-???**.

The root context prompt reflects the logged-in user level.

- The Supervisor level prompt always ends with **(super)#**
- The Privileged level prompt ends with **#**
- The User level prompt ends with **>**

As you change contexts, the command line prompt changes to reflect the context path. For example, when you enter the **access-control-list** configuration context as a Privileged user, the prompt reads **(ACL 330)#**.

To enter a context from another context:

- Enter the name of the context. The prompt changes to indicate the context entered.

To leave a context:

- Enter `exit`. The user returns to the parent context.

Available contexts

The following table describes all the contexts in the CLI. The Context column provides the command to type in order to enter the context. The CLI prompt column is the prompt that you see once you have entered the context.

Table 1: List of CLI Contexts *1 of 3*

Context	Description	CLI prompt
(Log in as User)	Root Read Only context	**>**
(Log in as Privileged User)	Root Read Write context	**#**
(Log in as Supervisor)	Root Admin context	(super)#
Interface Console	Configuring the Console interface	**(if:Console)#**
Interface USB	Configuring the USB interface	**(if:USB-Modem)#**
		1 of 3

Table 1: List of CLI Contexts *2 of 3*

Context	Description	CLI prompt
Interface Serial	USP, E1/T1	**(if:serial 2/1)#**
Interface loopback	The loopback virtual interface	**(if:loopback 1.0)#**
Interface VLAN	G350 interfaces to VLANs	**(if:vlan 1)#**
Interface FastEthernet	An Ethernet port connected directly to the router	**(if:fastEthernet 20/1)#**
Interface Tunnel	A GRE tunnel interface. A GRE tunnel is a virtual point-to-point link between two routers at two ends of an Internet cloud.	**(if:Tunnel 1)#**
Banner login	For editing a text message that appears before users login	**(super/login)#**
Banner post login	For editing a text message that appears after users login	**(super/post-login)#**
Router OSPF	OSPF routing protocol configuration	**(router:ospf)#**
Router RIP	RIP routing protocol configuration	**(router:rip)#**
ip QoS-list <list#>	QoS policy list	**(QoS 401)#**
rule <rule#>	QoS policy list entry	**(QoS 401/rule 4)#**
composite-operation <cot#>	QoS policy list match action	**(QoS 401/CompOp 2)#**
dscp-table <table#>	QoS policy list DSCP to CoS map	**(QoS 401/dscp 63)#**
ip Access-Control-List <list#>	Security Access list	**(ACL 301)#**
ip-rule <rule#>	Security ACL entry	**(ACL 301/ip rule 4)#**
composite-operation <cot#>	Security ACL match action	**(ACL 301/CompOp 2)#**
ip capture-list	Configure a capture list	**(Cap 501)#**
ip capture-list/ip-rule	Configure a capture list rule	**(Cap 501/ip rule 22)#**
ip dhcp pool	Configure a DHCP pool	**(DHCP 5)#**
		2 of 3

Table 1: List of CLI Contexts ***3 of 3***

Context	Description	CLI prompt
ip dhcp pool/option	Configure a DHCP option	**(DHCP 5/option 19)#**
ip dhcp pool/ vendor-specific-option	Configure a vendor specific DHCP option	**(DHCP 5/vendor specific 1)#**
ip next-hop-list	Configure a next hop list	**(next hop list 1)#**
ip pbr-list	Configure a PBR list	**(PBR 801)#**
ip pbr-list/ip-rule	Configure a PBR list rule	**(PBR 801/ip rule 22)#**
map-class frame-relay <name>	Create a QoS template	**(map-class)#**
crypto isakmp policy	Create an ISAKMP policy	**(config-isakmp:1)#**
		3 of 3

Chapter 2: CLI Commands

About the CLI

The Avaya G350 Media Gateway CLI Reference CLI is accessible directly via the serial console port, remotely via Telnet, or via the modem PPP interface. The CLI is command-line driven and does not have any menus. The CLI commands available, and the functions of those commands, depend on the context you are in when you issue the command. For a complete discussion of contexts, refer to Contexts on page 28.

This chapter lists all the CLI commands for the G350 Media Gateway.

Logging in to the CLI

To login to the CLI, you need a username and a password. Initially, there is only one user, named **root** (with password **root**), on the system. It is recommended to change the root user password to prevent unauthorized entry into the system. The root user has Administrative privileges. You can add more users with the **`username`** command.

When you open the CLI interface, you are prompted for a username. Enter the username and press **Enter**. Enter your password at the password prompt, and press **Enter**. Once you have logged in, you can execute all the CLI commands that are permitted at your user level. For a full discussion of user levels, refer to User Levels on page 28.

Using the CLI

To use a command, type the desired command at the prompt and press **Enter**.

Using Help

You can use the built-in Help feature to display the list of commands that are available to you. Type **`help`** to see the list of available commands in the present context. Type **`help`** followed by a word or part of a word to see a list of all commands starting with that word. For example, type **`help show`** to see a list of all commands using **`show`**. Type **`tree`** to see the full list of commands available at the current permission level.

Using auto-complete

If you are unsure of the spelling of a command, use the auto-complete feature. Type the first few letters of the command and then press the **tab** key. The system completes the command automatically. If more than one command begins with those letters, the system displays a list of commands matching those letters.

Abbreviating commands

You can abbreviate commands or parts of commands in the CLI. As long as the abbreviation uniquely identifies a command, the system executes that command. If the abbreviation is ambiguous, the system displays a list of possible matches.

For example, typing **`sh ban login`** is the same as typing **`show banner login`**. However, typing **`show m`** matches more than one command and is not executed. Instead the system displays a list such as:

```
Ambiguous Command.  Possible commands are:
map-class    mediaserver  mg          mgc         mm          module
```

Alphabetical listing of CLI commands

area

Use the **area** command to configure the area ID of a router. Use the **no** form of the command to delete the area ID.

Syntax

```
[no] area area_id [stub]
```

Parameters

Parameter	Description	Possible Values	Default Value
area_id	The IP address		
stub	Configure a stub area		

User level

read-write

Context

Router OSPF

Example

To configure an area for this OSPF interface with IP address 192.168.49.1:

```
G350-001(router:ospf)# area 192.168.49.1
```

To configure a stub area for this OSPF interface with IP address 176.1.13.12:

```
G350-001(router:ospf)# area 176.1.13.12 stub
```

To remove the area with IP address 192.168.49.1:

```
G350-001(router:ospf)# no area 192.168.49.1
```

arp

Use the **arp** command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove either a static entry or a dynamically learned entry from the ARP cache.

Syntax

arp *ip_address mac_address*

no arp *ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	IP address of the station		
mac_address	Corresponding MAC address for this station		

User level

read-write

Context

general

Example

To add a permanent entry for station 192.168.7.8 to the ARP cache:

```
G350-001# arp 192.168.7.8 00:40:0d:8c:2a:01
```

To remove an entry from the ARP cache for the station 192.168.13.76:

```
G350-001# no arp 192.168.13.76
```

arp timeout

Use the **`arp timeout`** command to configure the amount of time, in seconds, that an entry remains in the ARP cache. Entering the **`arp timeout`** command without a ***`seconds`*** parameter will display the current timeout value. Use the **`no`** form of this command to restore the default value (four hours).

Syntax

```
arp timeout [seconds]
```

```
no arp timeout
```

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds that an entry remains in the ARP cache	60 – 604800	14400

User level

read-write

Context

general

Example

To set the ARP timeout to one hour:

```
G350-001# arp timeout 3600
```

To restore the default value for ARP timeout:

```
G350-001# no arp timeout
```

async mode interactive

Use the **`async mode interactive`** command to enter modem mode every time the proprietary modem cable is plugged into the Console port.

Syntax

```
async mode interactive
```

User level

read-write

Context

Interface: Console

async mode terminal

Use the **`async mode terminal`** command to disable interactive mode on the Console.

Syntax

```
async mode terminal
```

User level

read-write

Context

Interface: Console

async modem-init-string

Use the **`async modem-init-string`** command to change the default modem initialization string. Use the **no** form of the command to return the modem initialization string to its default value.

Syntax

```
async modem-init-string modem_string
no async modem-init-string
```

Parameters

Parameter	Description	Possible Values	Default Value
modem_ string	The modem initialization string		

User level

admin

Context

Interface: Console, USB-modem

Example

To set the modem initialization string to ‘AT&FE0Q0V0X0&D2N0S37=6’:

```
G350-001(super-if:Console)# async modem-init-string
AT&FE0Q0V0X0&D2N0S37=6
```

async modem-type

Use the **async modem-type** command to set the type of modem being used. This command also sets the default modem parameter values such as default initialization string and escape sequence for the specified type of modem. Use the **no** form of the command to return modem type to its default value of **MultiTech-ZBA**.

Note:

If modem-type is specified as **none**, the system connects the PPP stack to the console port.

Syntax

async modem-type *modem_type*

no async *modem_type*

Parameters

Parameter	Description	Possible Values	Default Value
modem_type	The type of modem being used	**MultiTech-ZBA, USR-Sportster, null**	

User level

admin

Context

Interface: Console

Example

To set the modem type to USR-Sportster:

```
G350-001(super-if:Console)# async modem-type USR-Sportster
```

async reset-modem

Use the **`async reset-modem`** command to reset the connected modem.

Syntax

`async reset-modem`

User level

read-write

Context

Interface: Console

async reset-modem

Use the **`async reset-modem`** command to reset the USB modem. This command resets the PPP stack, deactivates the DTR signal, issues an ATZ (reset) command to the USB modem, and reissues the Init string sequence.
You can perform this command from within an active PPP session to close the session and allow the USB modem to accept a new call.

Syntax

`async reset-modem`

User level

read-write

Context

Interface: USB-modem

authentication

Use the **authentication** command to set the authentication of ISAKMP policy pre-shared secret.

Syntax

authentication *pre-share*

Parameters

Parameter	Description	Possible Values	Default Value
pre-share	The authentication of the ISAKMP policy pre-shared secret	**pre-share**	**pre-share**

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmp:1)# authentication pre-share
Done!
```

autoneg

Use the **autoneg** command to set the port speed and duplex to auto-negotiation mode for the external Fast Ethernet port. Use the **no** form of this command to disable auto-negotiation mode.

Syntax

[no] autoneg

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3)

backup delay

Use the **`backup delay`** command to set the time to wait before switching to the backup interface, in case of failure.

Syntax

`backup delay` ***`failure_delay secondary_disable_delay`***

Parameters

Parameter	Description	Possible Values	Default Value
`failure_delay`	The delay before switching to the backup interface, in seconds	0 - 3600	0
`secondary_disable_delay`	The delay before reverting to the primary interface, in seconds	0 - 3600	0

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP FR L2, USP PPP L2, USP PPP L2-L3), Tunnel (L2, L2-L3)

Example

To switch over immediately to the backup interface, in case of failure, and pause 60 seconds before reverting to the primary interface:

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

backup interface

Use the **`backup interface`** command to set a backup interface for the current interface.

Syntax

`backup interface` ***`interface_type interface_number`***

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**Serial, FastEthernet**	
interface_number	The interface number		

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3), Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP FR L2, USP PPP L2, USP PPP L2-L3), Tunnel (L2, L2-L3)

Example

To specify that Serial interface 2/1:1 is a backup interface for the current interface:

```
G350-001(if:Serial 2/1:2)# backup interface Serial 2/1:1
```

bandwidth

Use the **bandwidth** command to set the bandwidth parameter manually for this interface. Use the **no** form of this command to restore the bandwidth parameter to its default value. The manually specified bandwidth value overrides the dynamically calculated bandwidth during route cost calculations.

Syntax

bandwidth *kilobits*

no bandwidth

Parameters

Parameter	Description	Possible Values	Default Value
kilobits	The bandwidth for the interface in kilobits per second	**1 – 10000000**	**2048** (for Frame Relay)

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3, USP FR L2), Fast Ethernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To manually set the bandwidth for the VLAN interface to 100 KB/s:

```
G350-001(if:Vlan 1)# bandwidth 100
```

banner login

Use the **`banner login`** command to enter the login banner configuration mode. Use the **no** form of this command to set the login banner to its default value. The login banner displays before the user is prompted for the login name. To enter text for the login banner, refer to the command line on page 235.

Note:

Before creating a new banner, delete the current banner using the **`no banner login`** command.

Syntax

`[no] banner login`

User level

admin

Context

general

Example

To enter login banner configuration mode:

```
G350-001(super)# banner login
G350-001(super/login)#
```

banner post-login

Use the **`banner post-login`** command to enter the post-login banner configuration mode. The post-login banner displays after the user has logged in successfully. Use the **no** form of this command to set the post-login banner to its default value. To enter text for the post-login banner, refer to the command line on page 235.

Note:

> Before creating a new banner, delete the current banner using the **`no banner post-login`** command.

Syntax

```
[no] banner post-login
```

User level

admin

Context

general

Example

To enter the post-login banner configuration mode:

```
G350-001(super)# banner post-login
G350-001(super/post-login)#
```

bc out

Use the **`bc out`** command to configure the committed burst size in bits, for the outbound direction. Use the **no** form of this command to return the committed burst size to its default value.

Note:

> The time interval used in the frame relay meter is: (BC/CIR)*1000, where BC is the committed burst size, and CIR is the committed information rate. The minimum time interval is 10ms, and the device will prevent setting the BC and CIR in a way that violates this minimum.

Syntax

```
bc out bits
no bc out
```

Parameters

Parameter	Description	Possible Values	Default Value
bits	The committed burst size in bits	**8 – 39999999**	**7000**

User level

read-write

Context

map-class frame-relay

Example

To configure outbound BC to be 64 Kbit:

```
G350-001(map-class)# bc out 64000
```

be out

Use the **be out** command to configure the excess burst size in bits, for the outbound direction. Use the **no** form of this command to return the excess burst size to its default value.

> **Note:**
> The Excess Information Rate (EIR) is equal to: (BC+BE)/Tc/1000, where Tc is the Frame Relay meter time interval in mSec, BC is the committed burst rate and BE is the excess burst size.

Syntax

be out *bits*

no be out

Parameters

Parameter	Description	Possible Values	Default Value
bits	The excess burst size in bits	**0 – 39999999**	**7000**

User level

read-write

Context

map-class frame-relay

Example

To configure outbound BE to be 64 Kbit:

```
G350-001(map-class)# be out 64000
```

bootfile

The bootfile provides startup parameters for the DHCP client device. Use the **`bootfile`** command to specify the file name to be used as boot file. Use the **no** form of this command to clear the boot file name.

Syntax

`[no] bootfile` ***`file-name`***

Parameters

Parameter	Description	Possible Values	Default Value
`file-name`	The name of the file to be used as boot file.	string, **1-128** bytes	null string

User level

read-write

Context

dhcp pool

Example

To set the file “booter” as the bootfile:

```
G350-001(DHCP 5)# bootfile "booter"
```

To clear the bootfile definition:

```
G350-001(DHCP 5)# no bootfile
```

busyout voip-dsp

Use the **busyout voip-dsp** command to put the VoIP engine in busyout (not available) state for a Bit Transfer Rate test. For related VoIP testing commands, refer to the commands test voip-dsp on page 549, and release voip-dsp on page 268.

Note:

Status changes made during the test create SNMP traps.

Syntax

```
busyout voip-dsp
```

User level

read-write

Context

general

cablelength long

Use the **cablelength long** command to configure transmit and receive levels for a cable longer than 655 feet. Use the no form of the command to restore the transmit and receive levels to their default values.

Syntax

```
cablelength long rx_level tx_level
no cablelength long
```

Parameters

Parameter	Description	Possible Values	Default Value
rx_level	The receive sensitivity	**gain26**, **gain36**	**gain26**
tx_level	The transmit attenuation	**-15db, -22.5db, -7.5db, 0db**	**0db**

User level

read-write

Context

Interface: Controller (T1)

Example

To set the receive and transmit values for the cable to gain36 and -7.5db:

```
G350-001(controller:5/1)# cablelength long gain36 -7.5db
```

cablelength short

Use the **cablelength short** command to configure transmit levels for a cable of length 655 feet or shorter. Use the **no** form of the command to restore the transmit level to its default value.

Note:

The transmit attenuation is configured using the loop length.

Syntax

cablelength short *tx_value*

Parameters

Parameter	Description	Possible Values	Default Value
tx_value	The transmit level	**133ft, 266ft, 399ft, 533ft, 655ft**	**133ft**

User level

read-write

Context

Interface: Controller (T1)

Example

To set the transmit value for the cable to 399ft:

```
G350-001(controller:5/1)# cablelength short 399ft
```

capture buffer-mode

Use the **`capture buffer-mode`** command to specify the type of buffer used by the packet sniffer.

Syntax

```
capture buffer-mode {non_cyclic | cyclic}
```

Parameters

Parameter	Description	Possible Values	Default Value
`non_cyclic`	Linear buffer that is used until it is filled up		
`cyclic`	Circular buffer that overwrites the oldest records when it is filled up. Use a cyclic buffer to store the most recent history of packet activity.		

User level

read-write

Context

general

Example

```
G350-001# capture buffer-mode cyclic
```

capture buffer-size

Use the **`capture buffer-size`** command to specify the maximum size of the packet sniffing buffer.

Note:

> To activate the change in buffer size, you must run copy running-config startup-config, and reboot the device.

Syntax

```
capture buffer-size buffer_size
```

Parameters

Parameter	Description	Possible Values	Default Value
buffer_size	The maximum size of the packet sniffing buffer.	**256-10000 (Kbytes)**	**1000**

User level

read-write

Context

general

Example

```
G350-001# capture buffer-size 2000
```

capture filter-group

Use the **capture filter-group** command to apply the specified filter to the packet sniffer. When a capture filter is applied, packets must match the criteria for a rule whose action is ’capture’ in order to be saved to the buffer.

Syntax

capture filter-group *capture_list_id*

Parameters

Parameter	Description	Possible Values	Default Value
capture_list_id	The capture list number to apply	**500-599**	

User level

read-write

Context

general

Example

```
G350-001# capture filter-group 501
```

capture interface

Use the capture interface command to specify the interface on which to run the packet sniffing service. Use the **no** form of the command to run packet sniffing on all routing interfaces.

Syntax

`capture interface` ***`interface_name`***

no capture interface

Parameters

Parameter	Description	Possible Values	Default Value
`interface_name`	The name of the interface on which to run packet sniffing. If the interface name contains spaces, it must be enclosed in quotes.		

User level

read-write

Context

general

Example

```
G350-001> capture interface ’’FastEthernet 10/2’’
```

capture max-frame-size

Use the **`capture max-frame-size`** command to specify the maximum number of bytes captured for each packet by the packet sniffer.

Syntax

`capture max-frame-size` ***`max_frame_size`***

`no capture max-frame-size`

Parameters

Parameter	Description	Possible Values	Default Value
max_frame_size	The maximum number of bytes captured for each packet by the packet sniffer.	**14 - 4096**	**128**

User level

read-write

Context

general

Example

```
G350-001# capture max-frame-size 68
```

capture start

Use the **capture start** command to start the packet sniffing service.

Note:
The capture start command resets the buffer before starting the sniffer.

Note:
In order to upload a capture file, you must first stop the packet sniffing service.

Syntax

capture start

User level

read-write

Context

general

Examples

If the packet sniffing service has been enabled by the administrator:

```
G350-001> capture start
Starting the packet sniffing process
```

If the packet sniffing service has not been enabled by the administrator:

```
G350-001> capture start
The sniffing service is not available.
To re-enable, use the ‘capture-service’ command in supervisor mode.
```

capture stop

Use the **capture stop** command to stop the packet sniffing service.

Note:

This command is not saved in the startup configuration file.

Note:

In order to upload a capture file, you must first stop the packet sniffing service.

Syntax

capture stop

User level

read-write

Context

general

Examples

If the packet sniffing service has been enabled by the administrator:

```
G350-001> capture stop
110 packets captured.
```

If the packet sniffing service has not been enabled by the administrator:

```
G350-001> capture stop
The Packet sniffing process is not running.
```

capture-service

Use the **`capture-service`** command to enable the packet sniffing service. Use the **no** form of the command to disable the packet sniffing service. By disabling the service, the administrator can prevent users with read-write access from starting packet sniffing.

Note:

This command can only be executed by an admin user connected via the console port.

Syntax

`[no] capture-service`

User level

admin

Context

general

Example

To enable packet sniffing:

```
G350-001> capture-service
Packet sniffing service enabled
```

To disable packet sniffing:

```
G350-001> no capture-service
Packet sniffing service disabled
```

channel-group

Use the **`channel-group`** command to create a channel group logical interface for a PPP or Frame Relay session. Use the **no** form of the command to delete a channel group.

Note:

If you issue this command with an existing channel number, the timeslots you specify will replace any that already exist.

Syntax

`channel-group` ***`channel_number`*** **`timeslots`** ***`ts_list`*** **`speed`** ***`speed_value`***

`no channel-group` ***`channel_number`***

Parameters

Parameter	Description	Possible Values	Default Value
channel_ number	The ID number to identify the channel group	For T1: **0 – 23** For E1: **0 – 30**	
ts_list	The time slots to include in this channel group. Values can be separated either by a "–" for a range, or by commas for a list.	For T1: **1 – 24** For E1: **1 – 31**	
speed_value	The acceptable speed values	**56, 64**	**56**

User level

read-write

Context

Interface: Controller

Example

To create a new channel group number 2, with time slots 5, 6, and 8 and speed of 56:

```
G350-001(controller:5/1)# channel-group 2 timeslots 5-6,8 speed 56
```

cir out

Use the **`cir out`** command to configure the Committed Information Rate in bits per second, for the outbound direction. Use the **no** form of this command to return the CIR to its default value.

Note:

This command fails if the map class is currently associated with a DLCI.

Syntax

`cir out` ***`cir`***

`no cir out`

Parameters

Parameter	Description	Possible Values	Default Value
cir	The CIR in bits per second	**0 – 39999999**	**56000**

User level

read-only

Context

map-class frame-relay

Example

To configure outbound CIR to be 64 Kbps:

```
G350-001(map-class)# cir out 64000
```

class-identifier

Use the **`class-identifier`** command to set a vendor specific identifier string.

Syntax

`[no] class-identifier` ***`string`***

Parameters

Parameter	Description	Possible Values	Default Value
`string`	Identifier string for vendor specific option	string, **1-255** bytes	null string

User level

read-write

Context

dhcp pool vendor specific

Example

To set an identifier string for vendor-specific option 1:

```
G350-001(DHCP 5/vendor specific 1)# class-identifier "ccp.avaya.com"
```

clear arp-cache

Use the **`clear arp-cache`** command to delete all dynamic entries from the ARP cache.

Syntax

`clear arp-cache [`*`interface`*`|`*`vlan_id`*`|`*`ip_address`*`[`*`mask`*`]]`

Parameters

Parameter	Description	Possible Values	Default Value
interface	The interface name for which to delete entries		
vlan_id	The VLAN ID for which to delete entries	**1 – 3071**	
ip_address	The host IP address to clear		
mask	The IP mask of the subnet to clear		

User level

read-write

Context

general

Example

To flush all ARP entries:

```
G350-001# clear arp-cache
```

```
Flushing all arp entries
Flushed 22 ARP entries.
```

To flush ARP entries for an interface named “FastEthernet 10/2”:

```
G350-001# clear arp-cache "fastethernet 10/2"
```

```
Flushing ARP cache entries on ifName fastethernet 10/2
Flushed 1 ARP entries.
```

To flush ARP entries for one host address:

```
G350-001# clear arp-cache 156.16.11.32
```

```
Flushing ARP cache entry of host 156.16.11.32
Flushed 0 ARP entries.
```

To flush a range of ARP entries belonging to one subnet:

```
G350-001# clear arp-cache 156.3.2.33 255.255.255.0
```

```
Flushing ARP cache entries in the range [156.3.2.33, 255.255.255.0]
Flushed 0 ARP entries.
```

clear cam

Use the **`clear cam`** command to delete all entries from the Contents Address Memory (CAM) table.

Syntax

`clear cam`

User level

read-write

Context

general

Example

To clear the CAM table:

```
G350-001# clear cam
```

```
CAM table cleared.
```

clear capture-buffer

Use the **`clear capture-buffer`** command to clear the packet sniffing buffer.

Syntax

`clear capture-buffer`

User level

read-write

Context

general

Example

```
G350-001> clear capture-buffer
Done!
```

clear controller counters

Use the **`clear controller counters`** command to reset the controller counters.

Syntax

`clear controller counters` ***`controller_number`***

Parameters

Parameter	Description	Possible Values	Default Value
`controller_number`	The controller module number and port number		

User level

read-only

Context

general

Example

To clear counters for controller 3, port 1:

```
G350-001# clear controller counters 3/1
```

clear counters

Use the **`clear counters`** command to clear counters for the selected interface or the entire device.

Syntax

`clear counters [`*`interface_type interface_identifier`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
interface_ type	The type of interface		
interface_ identifier	The interface number. The format varies depending on the value of interface_type: For FastEthernet: **module/port** For Serial: **module/port:channel-group** For Vlan: **Vlan id** For LoopBack: **Loopback number**	For FastEthernet: **10/2** For Serial(USP): **2/1** For Serial (DS1): module/port: **2/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-3071** For Loopback: **1-99**	

User level

read-write

Context

general

Example

To clear counters on interface “Vlan 1”:

```
G350-001# clear counters Vlan 1
```

clear crypto isakmp

Use the **`clear crypto isakmp`** command to flush a specific ISAKMP SA or all the ISAKMP SAs.

Tip:

Use the command **`show crypto isakmp sa`** to display the connection IDs.

Tip:

It is recommended to use the command **`clear crypto sa all`** before running **`clear crypto isakmp`**.

Syntax

```
clear crypto isakmp [C-id]
```

Parameters

Parameter	Description	Possible Values	Default Value
`C-id`	The connection ID **Note**: If you do not enter a connection ID, the entire database is flushed.	**0 – 32,766**	

User level

read-write

Context

general

Example

To clear C-id 1:

```
G350-001# clear crypto isakmp 1
Done!
```

To clear the entire database:

```
G350-001# clear crypto isakmp
Done!
```

clear crypto sa all

Use the **`clear crypto sa all`** command to clear all or specific IPSec SAs (security association structures).

Syntax

```
clear crypto sa [all | counters | list id | peer ip address |
spi destination_address ipsec protocol_spi]
```

Parameters

Parameter	Description	Possible Values	Default Value
`all`	Keyword specifying that all IPSec SA counters should be cleared		
`counters`	Keyword specifying that all crypto IPSec SA counters should be cleared		
`list`	Keyword specifying that all crypto IPSec SAs associated with crypto-list ***`id`*** should be cleared		
`peer`	Keyword specifying that all crypto IPSec SAs associated with crypto peer having the address ***`ip address`*** should be cleared		
`spi`	Keyword specifying that specific IPSec by spi should be cleared		

User level

read-write

Context

general

Examples

```
G350-001# clear crypto sa all
Done!

G350-001(super)# clear crypto sa spi 1.0.0.2 esp 70045
Done!
```

clear crypto sa counters

Use the **`clear crypto sa counters`** command to clear the crypto SA counters.

Syntax

```
clear crypto sa counters
```

User level

read-write

Context

general

Example

```
G350-001# clear crypto sa counters
Done!
```

clear dot1x config

Use the **`clear dot1x config`** command to disable 802.1x on all ports and return values to the default settings.

Syntax

`clear dot1x config`

User level

admin

Example

```
Console> clear dot1x config
```

clear fragment

Use the **`clear fragment`** command to clear the fragment database and restore its default values.

Note:

No IP reassembly is performed on packets in transit through the router.

Syntax

`clear fragment`

User level

read-write

Context

general

clear frame-relay counters

Use the **`clear frame-relay counters`** command to clear the Frame Relay counters.

Syntax

`clear frame-relay counters [interface` ***`interface_name`*** **`]`**

Parameters

Parameter	Description	Possible Values	Default Value
`interface`	Keyword specifying that the counters should be cleared on the specified interface		
`interface_name`	The name of the interface		

User level

read-only

Context

general

Example

To clear the Frame Relay counters:

```
G350-001> clear frame-relay counters
```

To clear a specific Frame Relay interface’s counters:

```
G350-001> clear frame-relay counters interface “Serial 4/1.100”
```

clear ip dhcp-server binding

Binding is the allocation of an IP address to a client. Use the **`clear ip dhcp-server binding`** command to delete IP address binding. You can delete all bindings or the binding of a specific IP address. Clearing the binding of an IP address frees the IP address for reallocation by the DHCP server.

When the DHCP server detects an IP address conflict after attempting to allocate an IP address that is already in use, the server locks the IP address for half an hour by marking the IP address with client-identifier 00:00:00:00:00:00:00. If you have solved the conflict before half an hour, you can use this command to free the IP address for reallocation.

Syntax

`clear ip dhcp-server binding {`*`ip-address`*`|all}`

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	Clears any existing allocation of the specified IP address	1-32	
all	Clears all IP address allocations.		

User level

read-write

Context

general

Example

To clear the allocation of IP address 1.1.1.1:

```
G350-001# clear ip dhcp-server bindings 1.1.1.1
```

To clear all DHCP server IP address allocations:

```
G350-001# clear ip dhcp-server bindings all
```

clear ip dhcp server statistics

Use the **`clear ip dhcp server statistics`** command to clear the statistics of the DHCP server.

Syntax

`clear ip dhcp server statistics`

User level

read-write

Context

general

Example

To clear the statistics of the DHCP server:

```
G350-001# clear ip dhcp server statistics
```

clear ip route

Use the **`clear ip route`** command to delete all the dynamic routing entries from the routing table.

Syntax

`clear ip route * | {`*`ip_addr`*` [`*`ip_mask`*`]}`

Parameters

Parameter	Description	Possible Values	Default Value
`*`	Clear the entire routing table.		
`ip_addr`	The IP address of a specific dynamic routing entry to clear		
`ip_mask`	The IP mask of a specific dynamic routing subnet to clear		

User level

read-write

Context

general

Example

To clear the entire routing table:

```
G350-001# clear ip route *
```

To clear a range of entries:

```
G350-001# clear ip route 192.168.49.1 255.255.255.0
```

clear ip rtp header-compression

Use the **`clear ip rtp header-compression`** command to clear IP RTP header compression statistics either for all enabled interfaces or for a specific interface. To clear IP RTP compression statistics for all enabled interfaces, do not enter an interface type and number.

Note:

There is no renegotiation of parameters.

Syntax

```
clear ip rtp header-compression [interface_type interface_number]
```

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface		
interface_number	The interface number		

User level

read-only

Context

general

Example

To clear header compression statistics for all interfaces:

```
G350-001# clear ip rtp header-compression
```

clear ip tcp header-compression

Use the **`clear ip tcp header-compression`** command to clear TCP compression statistics either for all enabled interfaces or for a specific interface. To clear TCP compression statistics for all enabled interfaces, do not enter an interface type and number.

Syntax

```
clear ip tcp header-compression [interface_type interface_number]
```

Parameters

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface		
interface_number	The interface number		

User level

read-only

Context

general

Example

To clear TCP compression statistics for all enabled interfaces:

```
G350-001> clear ip tcp header-compression
```

clear ip traffic

Use the **clear ip traffic** command to clear the IP counters.

Syntax

clear ip traffic

User level

read-only

Context

general

clear logging file

Use the **`clear logging file`** command to delete the message log file being stored in non-volatile memory (NVRAM), including the history log, and open a new, empty log file.

Syntax

`clear logging file`

User level

read-write

Context

general

Example

To delete the message log:

```
G350-001# clear logging file
Done!
```

clear logging server

Use the **`clear logging server`** command to delete the specified Syslog message server from the Syslog server table.

Syntax

`clear logging server {`*`ip_address`*` | `*`hostname`*`}`

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the Syslog server		
hostname	The name of the Syslog server host		

User level

read-write

Context

general

Example:

To delete the Syslog message server with IP address 176.15.4.25:

```
G350-001# clear logging server 176.15.4.25
```

clear mgc list

Use the **`clear mgc list`** command to remove entries from the Media Gateway Controller list. Multiple entries can be removed together, by specifying a list of IP addresses separated by commas. If no arguments are provided, all entries are removed.

Syntax

`clear mgc list [`*`ipaddress1`*`,…]`

Parameters

Parameter	Description	Possible Values	Default Value
ipaddress1	The IP address of a call controller		

User level

read-only

Context

general

Example

To remove two Media Gateway Controllers from the list, with IP addresses of 132.236.73.2 and 177.13.2.45:

```
G350-001(super)# clear mgc list 132.236.73.2, 177.13.2.45
```

clear port mirror

Use the **`clear port mirror`** command to delete a port mirroring pair.

Syntax

`clear port mirror` ***`source_module/source_port dest_module/dest_port`***

Parameters

Parameter	Description	Possible Values	Default Value
source_ module	The module number of the source (mirrored) port		
source_ port	The port number of the source (mirrored) port		
dest_ module	The module number of the destination port		
dest_port	The port number of the destination port		

User level

read-write

Context

general

Example

To disable the mirroring of port 5/1 by port 5/3:

```
G350-001# clear port mirror 5/1 5/3
```

clear port static-vlan

Use the **`clear port static-vlan`** command to delete statically configured VLANs from the port.

Syntax

`clear port static-vlan` ***`module/port_range vlan_id`***

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port_range	The port number or range of port numbers		
vlan_id	The VLAN ID to remove		

User level

read-write

Context

general

Example

To remove VLAN 5 from port 3/10:

```
G350-001# clear port static-vlan 3/10 5
```

VLAN 5 is unbound from port 3/10

clear radius authentication server

Use the **clear radius authentication server** command to clear the primary or secondary RADIUS server IP address.

Syntax

```
clear radius authentication server {primary|secondary}
```

Parameters

Parameter	Description	Possible Values	Default Value
primary	Keyword specifying to clear the primary RADIUS server		
secondary	Keyword specifying to clear the secondary RADIUS server		

User level

admin

Context

general

Example

To clear the secondary RADIUS authentication server:

```
G350-001# clear radius authentication server secondary
```

clear screen

Use the **`clear screen`** command to clear the current terminal display.

Syntax

`clear screen`

User level

read-only

Context

general

clear snmp trap

Use the **`clear snmp trap`** command to clear an entry from the SNMP trap receiver table.

Syntax

`clear snmp trap {`*`rcvr_addr`*`|all}`

Parameters

Parameter	Description	Possible Values	Default Value
rcvr_addr	The IP address of the trap receiver (the SNMP management station) to remove		
all	Keyword used to clear all entries in the SNMP trap receiver table		

User level

read-write

Context

general

Example

To remove the SNMP trap server with IP address 192.122.173.82 from the table:

```
G350-001# clear snmp trap 192.122.173.82
SNMP trap receiver deleted.
```

clear ssh-client known-hosts

Use the **clear ssh-client known-hosts** command to clear the SSH known-host file content. This command is used to unlock the man-in-the-middle attack prevention mechanism, and allow SCP server authentication after an SCP server public key change.

Syntax

clear ssh-client known-hosts

User level

admin

Context

general

Example

```
G350-001(super)# clear ssh-client known-hosts
Done!
```

clear sync interface

Use the **`clear sync interface`** command to disassociate a previously specified interface as the primary or secondary clock synchronization source.

Note:

The primary interface must be disassociated before the secondary interface is disassociated.

Syntax

```
clear sync interface {primary | secondary}
```

Parameters

Parameter	Description	Possible Values	Default Value
`primary`	Keyword specifying the primary clock synchronization source		
`secondary`	Keyword specifying the secondary clock synchronization source		

User level

read-write

Context

general

Example

To disassociate the interface that is specified as the primary clock synchronization source:

```
G350-001# clear sync interface primary
```

clear utilization cpu

Use the **`clear utilization cpu`** command to disable CPU utilization measurements.

Syntax

`clear utilization cpu` ***`module`***

Parameters

Parameter	Description	Possible Values	Default Value
module	The module for which to disable CPU utilization measurements		

User level

read-write

Context

general

Example

To disable CPU utilization measurements for Module #10:

```
G350-001# clear utilization cpu 10
```

clear vlan

Use the **clear vlan** command to delete an existing VLAN and its interface. When you clear a VLAN, all ports assigned to that VLAN are returned to the default VLAN.

Syntax

clear vlan *vlan_id* | {name *vlan_name*}

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	The VLAN number		
name	Keyword specifying to identify the VLAN by the VLAN name.		
vlan_name	The VLAN name. If you wish to enter a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.		

User level

read-write

Context

general

Example

To delete VLAN 100:

```
G350-001# clear vlan 100
```

```
This command will assign all ports on vlan 100 to their default in the
entire management domain - do you want to continue (Y/N)?  y
```

```
VLAN 100 deletion successful
```

client-identifier

Use the **`client-identifier`** command to configure a reservation/manual pool. A reservation/manual pool reserves one IP address for a specific client. This command specifies a unique identifier for the client. The pool for which you configure a client identifier must contain one IP address only. This means that the start and end IP addresses of the pool must be equal. The DHCP server uses the client identifier to recognize the DHCP client and allocates the reserved IP address to the client. Use the **no** form of this command to clear a specified unique identifier for a DHCP client.

Syntax

`[no] client-identifier` ***`unique-identifier`***

Parameters

Parameter	Description	Possible Values	Default Value
`unique-identifier`	A unique identifier for a DHCP client, in the format ***`type`***:***`data`***	Hex string, any value. For Ethernet MAC use <type>:<data> format, where <type> is **01** and <data> is the MAC address of the device.	null hex string

User level

read-write

Context

dhcp pool

Example

To set the MAC address as a client identifier for an Ethernet MAC client with MAC address `00:11:22:33:44:55`:

```
G350-001(DHCP 5)# client-identifier 01:00:11:22:33:44:55
```

clock source

Use the **`clock source`** command to configure the clock source for an E1/T1 controller. Use the **no** form of the command to return the clock source to the default value of **line**.

Syntax

```
clock source {line | internal}
no clock source
```

Parameters

Parameter	Description	Possible Values	Default Value
line	Keyword that specifies to use an external clock		
internal	Keyword that specifies to synchronize to the internal clock		

User level

read-write

Context

Interface: Controller

Example

To specify that controller number 5 uses an external clock:

```
G350-001(controller:5/1)# clock source external
```

composite-operation

Use the **`composite-operation`** command to edit the specified composite operation. If the composite operation does not exist, it is created.

Syntax

`composite-operation` ***`index`***

Parameters

Parameter	Description	Possible Values	Default Value
`index`	The composite operation number	**12 – 19**	

User level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip qos-list, ip qos-list/dscp-table, ip qos-list/ip-rule

Example

To enter configuration mode for composite operation 13:

```
G350-001(QoS 440)# composite-operation 13
G350-001(QoS 440/CompOp 13)#
```

controller

Use the **`controller`** command to enter configuration mode for a specific controller.

Syntax

`controller {e1 | t1}` ***`module_number/port_number`***

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number to configure		
port_number	The port to configure		

User level

read-write

Context

general

Example

To enter configuration mode for a T1 controller on port 5/1:

```
G350-001# controller t1 5/1
```

cookie

Use the **cookie** command to set the cookie for the current list.

Syntax

cookie *cookie_number*

Parameters

Parameter	Description	Possible Values	Default Value
cookie_number	The ID number of the cookie	**0 – 268435455**	

User level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To specify the cookie for QoS list 440 as 257:

```
G350-001(QoS 440)# cookie 257
```

copy capture-file ftp

Use the **`copy capture-file ftp`** command to upload the packet sniffing buffer to a file using the ftp protocol.

Note:

> You must stop the packet sniffing service using the **`capture stop`** command before you can upload the buffer.

Syntax

`copy capture-file ftp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	The file name on the FTP server		
`ip`	The IP address of the FTP server		

User level

read-write

Context

general

Example

To upload the packet sniffing buffer to the g350.cap file on the FTP server at IP address 135.64.10.33:

```
G350-001# copy capture-file ftp g350.cap 135.64.10.33
```

copy capture-file scp

Use the **`copy capture-file scp`** command to upload the packet sniffing buffer to a file using the scp secure file transfer protocol.

Note:

You must stop the packet sniffing service using the **`capture stop`** command before you can upload the buffer.

Syntax

```
copy capture-file scp filename ip
```

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	The file name on the FTP server		
`ip`	The IP address of the FTP server		

User level

read-write

Context

general

Example

To upload the packet sniffing buffer to the g350.cap file on the FTP server at IP address 135.64.10.33:

```
G350-001# copy capture-file scp g350.cap 135.64.10.33
```

copy capture-file tftp

Use the **`copy capture-file tftp`** command to upload the packet sniffing buffer to a file using the tftp protocol.

Note:

You must stop the packet sniffing service using the **`capture stop`** command before you can upload the buffer.

Syntax

copy capture-file tftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name on the TFTP server		
ip	The IP address of the TFTP server		

User level

read-write

Context

general

Example

To upload the packet sniffing buffer to the g350.cap file on the TFTP server at IP address 135.64.10.33:

```
G350-001# copy capture-file tftp g350.cap 135.64.10.33
```

copy dhcp-binding ftp

Use the **copy dhcp-binding ftp** command to copy the dhcp bindings file to a remote server using FTP.

Syntax

copy dhcp-binding ftp *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User level

read-write

Context

general

Example

To copy the binding file with file name dhcp_binding.txt to the host with IP address 192.168.49.10:

```
G350-001# copy dhcp-binding ftp dhcp_binding.txt 192.168.49.10
```

copy dhcp-binding scp

Use the **`copy dhcp-binding scp`** command to copy the dhcp bindings file to a remote server using FTP.

Syntax

`copy dhcp-binding scp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	File name with full path	string	
`ip`	IP address of the host	IP address	

User level

read-write

Context

general

Example

To copy the binding file with file name dhcp_binding.txt to the host with IP address 192.168.49.10:

```
G350-001# copy dhcp-binding scp dhcp_binding.txt 192.168.49.10
```

copy dhcp-binding tftp

Use the **`copy dhcp-binding tftp`** command to copy DHCP bindings file to a remote server, using TFTP.

Syntax

```
copy dhcp-binding tftp filename ip
```

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name with full path	string	
ip	IP address of the host	IP address	

User level

read-write

Context

general

Example

To copy the binding file with file name dhcp_binding.txt to the host with IP address 192.168.49.10:

```
G350-001# copy dhcp-binding tftp dhcp_binding.txt 192.168.49.10
```

copy ftp EW_archive

Use the **`copy ftp EW_archive`** command to download Avaya G350 Manager software from an FTP server. The FTP command prompts for the username and password after the command is entered.

Syntax

```
copy ftp EW_archive filename ip
```

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name on the FTP server		
ip	The IP address of the FTP server		

User level

read-write

Context

general

Example

To download the g350.img file from the FTP server at IP address 135.64.10.33, using login dan:

```
G350-001# copy ftp EW_archive g350.img 135.64.10.33
```

Username: dan
Password:

copy ftp license-file

Use the **copy ftp license-file** command to download a VPN license from an FTP server.

Syntax

copy ftp license-file *filename ip*

Parameters

Parameter	Description	Possible Values	Default Value
filename	The filename of the VPN license, including the full path, on the FTP server		
ip	The IP address of the FTP server		

User level

admin

Context

general

Example

To download the VPN license `g350.lic` from the FTP site at IP address 198.87.134.153:

```
G350-001(super)# copy ftp license-file g350.lic 198.87.134.153
```

copy ftp module

Use the **`copy ftp module`** command to download firmware from an FTP server into a media module. The FTP command prompts for the username and password after the command is entered.

Syntax

`copy ftp module` ***`module_number filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
module_ number	The Media Module number		
filename	The file name on the FTP server		
ip	The IP address of the FTP server		

User level

read-write

Context

general

Example

To download the firmware file, mm.img, into media module 3 from the FTP site at IP address 135.64.10.33 using login dan:

```
G350-001# copy ftp module 3 mm.img 135.64.10.33
Username: dan
Password:
```

copy ftp phone-image

Use the **`copy ftp phone-image`** command to upload a phone script file to a remote server using FTP.

Syntax

`copy ftp phone-imageA|phone-imageB|phone-imageC|phone-imageD <`*`filename`*`> <`*`ip`*`>`

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the image file, including the full path.		
ip	The IP address of the host.		

User level

Read-write

Example

```
interface# > copy phone-imageA c:\IpphoneRelease\4602sape1_8.bin
192.168.49.10
```

copy ftp phone-script

Use the **`copy ftp phone-script`** command to download a file to a phone script bank using FTP.

Syntax

`copy ftp phone-scriptA|phone-scriptB <`*`filename`*`> <`*`ip`*`>`

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path.		
ip	The IP address of the host.		

User level

Read-write

Context

general

Example

```
interface# > copy ftp phone-scriptA 46xxupgrade.txt 192.168.49.10
```

copy ftp startup-config

Use the **`copy ftp startup-config`** command to download a configuration file from an FTP server. The command prompts for the username and password.

Note:

After you download the configuration file, the new configuration is not active until you reset the device.

Syntax

`copy ftp startup-config` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name on the FTP server		
ip	The IP address of the FTP server		

User level

read-write

Context

general

Example

To download the configuration file, g350.img, from the FTP server at IP address 135.64.10.33 using login dan:

```
G350-001# copy ftp startup-config g350.img 135.64.10.33
Username: dan
Password:

G350-001# reset
```

copy ftp SW_imageA

Use the **`copy ftp SW_imageA`** command to download a software image from an FTP server into Bank A. The command prompts for the username and password.

Syntax

`copy ftp SW_imageA` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name on the FTP server		
ip	IP address of the FTP server		

User level

read-write

Context

general

Example

To download the software image file, g350.img, from the FTP site at IP address 135.64.10.33 using login dan:

```
G350-001# copy ftp SW_imageA g350.img 135.64.10.33
Username: dan
Password:
```

copy ftp SW_imageB

Use the **`copy ftp SW_imageB`** command to download a software image from an FTP server into Bank B. The command prompts for the username and password.

Syntax

`copy ftp SW_imageB` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	File name on the FTP server		
ip	IP address of the FTP server		

User level

read-write

Context

general

Example

To download the software image file, g350.img, from the FTP site at IP address 135.64.10.33 using login dan:

```
G350-001# copy ftp SW_imageB g350.img 135.64.10.33
Username: dan
Password:
```

copy phone-script ftp

Use the **`copy phone-script ftp`** command to upload a phone script file to a remote server using FTP.

Syntax

`copy phone-scriptA|phone-scriptB ftp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path.		
ip	The IP address of the host.		

User level

Read-write

Context

general

Example

```
interface# > copy phone-scriptA ftp 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y
```

copy phone-script scp

Use the **`copy phone-script scp`** command to upload a phone script file to a remote server using SCP.

Syntax

`copy phone-scriptA|phone-scriptB scp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path.		
ip	The IP address of the host.		

User level

Read-write

Context

general

Example

```
interface# > copy phone-scriptA scp 46xxupgrade.txt 192.168.49.10
```

copy phone-script tftp

Use the **`copy phone-script`** command to upload a phone script file to a remote server via TFTP.

Syntax

`copy phone-scriptA | phone-scriptB tftp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	The name of the configuration file, including the full path.		
`ip`	The IP address of the host.		

User level

Read-write

Context

general

Example

```
interface# > copy phone-scriptA tftp 46xxupgrade.txt 192.168.49.10
```

copy running-config ftp

Use the **`copy running-config ftp`** command to upload the current configuration to a file on an FTP server. The command prompts for the username and password. Uncommitted changes to the configuration are included.

Note:

> After you change the configuration, run the **`copy running-config startup-config`** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

`copy running-config ftp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	File name to create on the FTP server		
`ip`	IP address of the FTP server		

User level

read-write

Context

general

Example

To upload the current configuration to the g350.cfg file on the ftp server at IP address 135.64.10.33 using login dan:

```
G350-001# copy running-config ftp c:\config_files\router1.cfg
135.64.10.33
Username: dan
Password:
```

copy running-config scp

Use the **`copy running-config scp`** command to upload the current configuration using the SCP secure protocol. The command prompts for the username and password. Uncommitted changes to the configuration are included.

Note:

After you change the configuration, run the **`copy running-config startup-config`** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

`copy running-config scp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	File name to create on the SCP server		
`ip`	IP address of the SCP server		

User level

read-write

Context

general

Example

```
G350-001# copy running-config scp c:\config_files\router1.cfg
192.168.49.10
Username: dan
Password:
```

copy running-config startup-config

Use the **`copy running-config startup-config`** command to commit the current configuration to NVRAM.

Syntax

`copy running-config startup-config`

User level

read-write

Context

general

Example

```
G350-001# copy running-config startup-config

Beginning copy operation .................... Done!
```

copy running-config tftp

Use the **`copy running-config tftp`** command to upload the current configuration to a file on a TFTP server. Uncommitted changes to the configuration are included.

To use this command, you need to have an active TFTP server. If Avaya Network Manager is running, you do not require an additional TFTP server.

Note:

After you change the configuration, run the **`copy running-config startup-config`** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

`copy running-config tftp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	Name of file to create on TFTP server		
ip	IP address of TFTP server		

User level

read-write

Context

general

Example

To upload the current configuration to the g350.cfg file on the TFTP server at IP address 135.64.10.33:

```
G350-001# copy running-config tftp g350.cfg 135.64.10.33
```

copy scp phone-script

Use the **copy scp phone-script** command to download a file to a phone script bank using SCP.

Syntax

copy scp phone-scriptA|phone-scriptB <*filename*> <*ip*>

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path.		
ip	The IP address of the host.		

User level

Read-write

Context

general

Example

```
interface# > copy scp phone-scriptA 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y
```

copy scp startup-config

Use the **`copy scp startup-config`** command to download a startup-config file using the SCP secure protocol. The command prompts for the username and password. Uncommitted changes to the configuration are not included.

Note:

After you change the configuration, run the **`copy running-config startup-config`** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

`copy scp startup-config` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	Name of file to create on SCP server		
`ip`	IP address of SCP server		

User level

read-write

Context

general

Example

```
G350-001# copy scp startup-config c:\config_files\router1.cfg
192.168.49.10
```

copy startup-config ftp

Use the **`copy startup-config ftp`** command to upload the current configuration to a file on an FTP server. The command prompts for the username and password. Uncommitted changes to the configuration are not included.

Note:

After you change the configuration, run the **`copy running-config startup-config`** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

```
copy startup-config ftp filename ip
```

Parameters

Parameter	**Description**	**Possible Values**	**Default Value**
filename	Name of file to create on the FTP server		
ip	IP address of the FTP server		

User level

read-write

Context

general

Example

To upload the current configuration to the g350.cfg file on the FTP server at IP address 135.64.10.33:

```
G350-001# copy startup-config ftp g350.cfg 135.64.10.33
```

copy startup-config scp

Use the **`copy startup-config scp`** command to upload the current configuration to a file on an SCP server. The command prompts for the username and password. Uncommitted changes to the configuration are not included.

Note:

> After you change the configuration, run the **`copy running-config startup-config`** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

`copy startup-config scp` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	Name of file to create on the SCP server		
`ip`	IP address of the SCP server		

User level

read-write

Context

general

Example

To upload the current configuration to the router1.cfg file on the SCP server at IP address 192.168.49.10:

```
G350-001# copy startup-config scp c:\config_files\router1.cfg 192.168.49.10
```

copy startup-config tftp

Use the **`copy startup-config tftp`** command to upload the current configuration to a file on a TFTP server. Uncommitted changes to the configuration are not included.

To use this command, you need to have an active TFTP server. If Avaya Network Manager is running, you do not require an additional TFTP server.

Note:

> After you change the configuration, run the **`copy running-config startup-config`** command to save the changes. If you do not save the changes, the device loses the changes when you reset it.

Syntax

```
copy startup-config tftp filename ip
```

Parameters

Parameter	Description	Possible Values	Default Value
filename	Name of file to create on TFTP server		
ip	IP address of TFTP server		

User level

read-write

Context

general

Example

To upload the current configuration to the g350.cfg file on the TFTP server at IP address 135.64.10.33:

```
G350-001# copy startup-config tftp g350.cfg 135.64.10.33
```

copy tftp EW_archive

Use the **`copy tftp EW_archive`** command to download the media gateway manager application into the media gateway via TFTP.

To use this command, you need to have an active TFTP server, and to create a file into which to download the data. If Avaya Network Manager is running, you do not require an additional TFTP server.

Syntax

`copy tftp EW_archive` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
`filename`	The manager image file name (full path)		
`ip`	The IP address of the host		

User level

read-write

Context

general

Example

To download the media gateway manager software, with filename of mgr.cfg, from the TFTP server located at IP address 192.168.49.10:

```
G350-001# copy tftp EW_archive c:\G350\mgr.cfg 192.168.49.10
```

copy tftp license-file

Use the **`copy tftp license-file`** command to download a VPN license from a TFTP server.

Syntax

`copy tftp license-file` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The filename of the VPN license, including the full path, on the TFTP server		
ip	The IP address of the TFTP server		

User level

admin

Context

general

Example

To download the VPN license `g350.lic` from the TFTP site at IP address 198.87.134.153:

```
G350-001(super)# copy tftp license-file g350.lic 198.87.134.153
```

copy tftp module

Use the **`copy tftp module`** command to download a new version of module software into a particular media module from a saved file, via TFTP.

To use this command, you need to have an active TFTP server, and to create a file into which to download the software. If Avaya Network Manager is running, an additional TFTP server is not required.

Note:

Perform the **`nvram initialize`** command prior to the **`copy tftp module`** command.

Syntax

`copy tftp module` ***`module_number filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number		
filename	The file name, including the full path		
ip	The IP address of the TFTP server		

User level

read-write

Context

general

Example

To download the software file mm1.cfg for media module 5 from the TFTP server 192.168.49.10:

```
G350-001# copy tftp module 5 c:\config\mm1.cfg 192.168.49.10
```

copy tftp phone-image

Use the **copy tftp phone-image** command to download a file to phone image bank A, B, C, or D.

Syntax

copy tftp phone-imageA | phone-imageB | phone-imageC | phone-imageD <*filename*> <*ip*>

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path.		
ip	The IP address of the host.		

User level

Read-write

Context

general

Example

```
interface# > copy tftp phone-imageA c:\IpphoneRelease\4602sape1_8.bin
192.168.49.10
```

copy tftp phone-script

Use the **copy tftp phone-script** command to download a file to phone script bank A or B.

Syntax

copy tftp phone-scriptA | phone-scriptB <*filename*> <*ip*>

Parameters

Parameter	Description	Possible Values	Default Value
filename	The name of the configuration file, including the full path.		
ip	The IP address of the host.		

User level

Read-write

Context

general

Example

```
interface# > copy tftp phone-scriptA file1.txt 135.64.100.205
Confirmation - do you want to continue (Y/N)? y
```

copy tftp startup-config

Use the **`copy tftp startup-config`** command to copy the media gateway configuration from the saved TFTP file to the Startup Configuration NVRAM.

To use this command, you need to have an active TFTP server, and to create a file into which to download the data. If Avaya Network Manager is running, an additional TFTP server is not required.

Syntax

`copy tftp startup-config` ***`filename ip`***

Parameters

Parameter	**Description**	**Possible Values**	**Default Value**
`filename`	The file name, including the full path		
`ip`	The IP address of the host		

User level

read-write

Context

general

Example

To copy the configuration file router1.cfg from the TFTP server 192.168.49.10 into the startup configuration:

```
G350-001# copy tftp startup-config c:\G350\router1.cfg 192.168.49.10
```

copy tftp SW_imageA

Use the **`copy tftp SW_imageA`** command to update the software image in Bank A of the media gateway.

To use this command, you need to have an active TFTP server, and to create a file into which to download the data. If Avaya Network Manager is running, an additional TFTP server is not required.

Syntax

`copy tftp SW_imageA` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name, including the full path		
ip	IP address of the host		

User level

read-write

Context

general

Example

To download the software file imgA.bin from the TFTP server 149.49.36.200 into boot bank A:

```
G350-001# copy tftp SW_imageA c:\imgA.bin 149.49.36.200
```

```
Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
```

copy tftp SW_imageB

Use the **`copy tftp SW_imageB`** command to update the software image in Bank B of the media gateway.

To use this command, you need to have an active TFTP server, and to create a file into which to download the data. If Avaya Network Manager is running, an additional TFTP server is not required.

Syntax

`copy tftp SW_imageB` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The file name, including the full path		
ip	IP address of the host		

User level

read-write

Context

general

Example

To download the software file imgB.bin from the TFTP server 149.49.36.200 into boot bank B:

```
G350-001# copy tftp SW_imageB c:\imgB.bin 149.49.36.200
```

```
Beginning download operation ...
This operation may take a few minutes...
Please refrain from any other operation during this time.
```

copy scp license-file

Use the **`copy scp license-file`** command to download a VPN license from an SCP server.

Syntax

`copy scp license-file` ***`filename ip`***

Parameters

Parameter	Description	Possible Values	Default Value
filename	The filename of the VPN license, including the full path, on the SCP server		
ip	The IP address of the SCP server		

User level

admin

Context

general

Example

To download the VPN license `g350.lic` from the SCP site at IP address 198.87.134.153:

```
G350-001(super)# copy scp license-file g350.lic 198.87.134.153
```

cos

Use the **cos** command to set the priority value for the current composite operation. Use the **no** form of the command to reset the priority to the default value of **no-change**.

Syntax

cos {*priority* | no-change}

no cos

Parameters

Parameter	**Description**	**Possible Values**	**Default Value**
priority	The priority value of the composite operation	**0 – 8**	
no-change	Keyword indicating that the priority is not changed		

User level

read-write

Context

ip qos-list composite-operation

Example

To set the priority for composite operation 12 to 3:

```
G350-001(QoS 440/CompOp 12)# cos 3
```

crypto ipsec df-bit

Use the **`crypto ipsec df-bit`** command to set the Don't-Fragment bit to one of the following modes:

- **`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.

Use the **`no`** form of the command to restore the Don't-Fragment bit to the default value: `copy`.

Syntax

```
[no] crypto ipsec df-bit {clear | copy}
```

Parameters

Parameter	Description	Possible Values	Default Value
`clear`	Clear the Don't-Fragment bit		
`copy`	Copy the Don't-Fragment bit		

User level

read-write

Context

interface

Example

```
G350-001(if:Serial 5/1)# crypto ipsec df-bit clear
Done!
```

crypto ipsec minimal-pmtu

Use the **`crypto ipsec minimal-pmtu`** command to set 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. Use the **`no`** form of the command to restore the minimal PMTU to the default value: `300`.

Syntax

```
[no] crypto ipsec minimal-pmtu bytes
```

Parameters

Parameter	Description	Possible Values	Default Value
bytes	The length of the minimum PMTU	**68-1400**	**300**

User level

read-write

Context

interface

Example

```
G350-001(if:Serial 5/1)# crypto ipsec minimal-pmtu 128
Done!
```

crypto ipsec transform-set

Use the **`crypto ipsec transform-set`** command to enter the IKE phase 2 (IPSec) transform-set context and create or edit IPSec parameters for the VPN tunnel. Use the **no** form of the command to delete IKE phase 2 (IPSec) parameters for the VPN tunnel.

Syntax

```
[no] crypto ipsec transform-set name
 {{esp-des | esp-3des | esp-aes} | [{esp-md5-hmac | esp-sha-hmac}] |
 esp-null {esp-md5-hmac | esp-sha-hmac}}
```

Note:

If you want to enable authentication only, you must enter the **`esp-null`** parameter.

Parameters

Parameter	Description	Possible Values	Default Value
name	The transform-set name	**1-32 characters, no spaces**	
esp-des	Encryption type: Encapsulation Security Protocol and Data Encryption Standard		
esp-3des	Encryption type: Encapsulation Security Protocol and Triple Data Encryption Standard		
esp-aes	Encryption type: Encapsulation Security Protocol and Advanced Encryption Standard		
esp-null	Encryption type: Encapsulation Security Protocol without encryption. **Note**: This option is intended for lab testing.		
esp-md5-hmac	Authentication type: Encapsulation Security Protocol, md5 hashing and keyed-hash mac		
esp-sha-hmac	Authentication type: Encapsulation Security Protocol, secure hash algorithm and keyed-hash mac		

User level

read-write

Context

general

Examples

Example 1001: To configure an IPSec transform set with encryption and authentication:

```
G350-001# crypto ipsec transform-set ts2 esp-des esp-md5-hmac
G350-001(config-transform:ts2)#
```

Example 2: To configure an IPSec transform set with authentication only:

```
G350-001# crypto ipsec transform-set ts3 esp-null esp-md5-hmac
G350-001(config-transform:ts3)#
```

Example 3: To enter the crypto IPSec transform-set context:

```
G350-001# crypto ipsec transform-set ts1
G350-001(config-transform:ts1)#
```

crypto isakmp invalid-spi-recovery

Use the **`crypto isakmp invalid-spi-recovery`** command to enable invalid SPI recovery (default setting). Use the **no** form of the command to disable invalid SPI recovery.

Syntax

`[no] crypto isakmp invalid-spi-recovery`

User level

read-write

Context

general

Example

```
G350-001# no crypto isakmp invalid-spi-recovery
Done!
```

crypto isakmp peer

Use the **`crypto isakmp peer`** command to enter the crypto ISAKMP peer context and create or edit an ISAKMP peer. Use the **no** form of the command to delete a remote VPN peer.

Note:

You cannot delete an ISAKMP peer that is referenced by a crypto map; you must first delete the peer from the crypto map by entering crypto map context using the **`crypto map`** command, and then delete the peer using the **`no set peer`** command.

Syntax

`[no] crypto isakmp peer address` ***`peer-address`***

Parameters

Parameter	Description	Possible Values	Default Value
`peer-address`	The IP address of the ISAKMP peer		

User level

read-write

Context

general

Example

```
G350-001# crypto isakmp peer address 149.49.70.1
G350-001(config-peer:149.49.70.1)#
```

crypto isakmp policy

Use the **`crypto isakmp policy`** command to enter the crypto ISAKMP policy context and create or edit IKE Phase 1 parameters.

Syntax

`crypto isakmp policy` ***`id`***

Parameters

Parameter	Description	Possible Values	Default Value
`id`	The identity of the ISAKMP policy	**1-20**	

User level

read-write

Context

general

Example

```
G350-001# crypto isakmp policy 1
G350-001(config-isakmp:1)#
```

crypto isakmp suggest-key

Use the **`crypto isakmp suggest-key`** command to generate a random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.

Syntax

`crypto isakmp suggest-key [key-length]`

Parameters

Parameter	Description	Possible Values	Default Value
`key-length`	The length of the key to be generated	**8-127**	**32**

User level

read-write

Context

general

Examples

```
G350-001# crypto isakmp suggest-key
The suggest key: GNpi1odGNBrB5z4GJLz156jDmRWAGFES

G350-001# crypto isakmp suggest-key 8
The suggest key: iEvKoQ1e
```

crypto key generate

Use the **`crypto key generate`** command to generate an SSH host key pair. You must generate the host key pair before the SSH service can be used. Stations that are currently active receive a warning message that the device public key has changed.

Note:

This command does not close active sessions.

Note:

This command can take several minutes to run (depending on CPU speed).

Syntax

```
crypto key generate dsa [key-size bit-number]
```

Parameters

Parameter	Description	Possible Values	Default Value
bit-number	The number of bits in the key	**512-2048**	1024

User level

admin

Context

general

Example

```
G350-001(super)# crypto key generate

Generating DSA key, This command may take a few minutes

......

Key was created.

Key version: SSH2, DSA

Key Fingerprint: dd:60:59:fa:e0:47:b8:db:e3:1c:17:8d:4c:14:9a:0f
root@avaya
```

crypto map

Use the **crypto map** command to enter crypto map context and create or edit a crypto map. Use the **no** form of the command to delete a specific crypto map.

Note:

You cannot delete a crypto map that is being used by an active crypto-list.

Syntax

```
[no] crypto map id
```

Parameters

Parameter	Description	Possible Values	Default Value
id	The crypto map ID	**1-50**	

User level

read-write

Context

general

Examples

```
G350-001# crypto map 10
G350-001(config-crypto:10)#

G350-001# no crypto map 10
Done!
```

de pre-mark

Use the **de pre-mark** command to specify the threshold, in percents of CIR, to begin marking non-high-priority packets (0-5) over the BC (committed burst) level and under the BE (excess burst) level as Delete Eligible (DE) packets. Use the **no** form of the command to return the threshold to its default value.

Syntax

```
de pre-mark threshold_percent
no de pre-mark
```

Parameters

Parameter	Description	Possible Values	Default Value
threshold_percent	The threshold percent	**1 – 100**	**100** (no pre-mark)

User level

read-write

Context

map-class frame-relay

de-buffer-size

Use the **`de-buffer-size`** command to set the buffer size for frames marked as drop-eligible. Use the **no** form of the command to return the drop-eligible buffer to its default size.

Syntax

`de-buffer-size` ***`size`***

`no de-buffer-size`

Parameters

Parameter	Description	Possible Values	Default Value
`size`	The drop-eligible (DE) buffer size, in packets		

User level

read-write

Context

Interface: Serial (DS1 FR L2, USP FR L2)

Example

To set the buffer size for drop-eligible frames to 200 packets:

```
G350-001(if:Serial 5/1:1)# de-buffer-size 200
```

default-metric

Use the **`default-metric`** command to set the default metric of redistributed routes for the OSPF protocol. Use the **no** form of this command to restore the default value.

Syntax

`default-metric` ***`default_metric`***

`no default-metric`

Parameters

Parameter	Description	Possible Values	Default Value
`default_ metric`	The default metric of redistributed routes	**1-65535**	**20**

User level

read-write

Context

Router-OSPF

Example

To set the default metric for redistributed routes to 50:

```
G350-001(router:ospf)# default-metric 50
```

default-metric

Use the **`default-metric`** command to set the default metric of redistributed routes for the RIP protocol. Use the **no** form of this command to restore the default value.

Syntax

`default-metric` ***`default_metric`***

`no default-metric`

Parameters

Parameter	Description	Possible Values	Default Value
`default_ metric`	The interface RIP route metric value	**1-16**	**1**

User level

read-write

Context

Router-RIP

Example

To set the default metric for redistributed routes to 5:

```
G350-001(router:rip)# default-metric 5
```

default-metric

Use the **`default-metric`** command to set the interface Routing Information Protocol (RIP) route metric value. Use the **no** form of this command to restore the default value.

Syntax

`default-metric` ***`number`***

`no default-metric`

Parameters

Parameter	Description	Possible Values	Default Value
`number`	The interface route metric value	**1-15**	**1**

User level

read-write

Context

Interface: Loopback (L2-L3, L3), Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), Fast Ethernet (L3, L2-L3), VLAN (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To set the default metric to 10:

```
G350-001(if:FastEthernet 10/2)# default-metric 10
```

default-router

Use the **default-router** command to set up to eight default router IP addresses in order of preference. Use the **no** form of this command to clear the default router IP address(es).

Syntax

```
[no] default-router ip-addr-list
```

Parameters

Parameter	Description	Possible Values	Default Value
ip-addr-list	A list of up to eight IP addresses for the default router.	A list of IP addresses separated by spaces	**0.0.0.0**

User level

read-write

Context

dhcp pool

Example

To set 164.35.2.4 and 135.64.102.3 as default router IP addresses:

```
G350-001(DHCP 5)# default-router 164.35.2.4 135.64.102.3
```

description

Use the **description** command to configure a description for the current interface. Use the **no** form of this command to clear the description of the current interface.

Syntax

```
description string
no description
```

Parameters

Parameter	Description	Possible Values	Default Value
string	The description of the interface		

User level

read-write

Context

Interface: serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2-L3, USP PPP L2, USP FR L2), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To specify the description for the VLAN 3 interface as “Marketing VLAN”:

```
G350-001(if:Vlan 3)# description "Marketing VLAN"
```

description

Use the **description** command to enter a description for the crypto map. Use the **no** form of the command to clear a description for the crypto map.

Syntax

[no] description *desc*

Parameters

Parameter	Description	Possible Values	Default Value
desc	The description of the crypto map. **Note**: if you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	**1-80 characters**	

User level

read-write

Context

crypto map

Example

```
G350-001(config-crypto:10)# description "crypto map 1"
Done!
```

description

Use the **`description`** command to enter a description for the ISAKMP policy. Use the **no** form of the command to clear a description for the ISAKMP policy.

Syntax

`[no] description` ***`desc`***

Parameters

Parameter	Description	Possible Values	Default Value
desc	The description of the ISAKMP policy. **Note**: if you wish to include spaces in the description, you must enclose the string in quotation marks (“”)	**1-80 characters**	

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmp:1)# description "isakmp policy 1"
Done!
```

description

Use the **`description`** command to enter a description for the ISAKMP peer. Use the **no** form of the command to clear a description for the ISAKMP peer.

Syntax

`[no] description` ***`desc`***

Parameters

Parameter	Description	Possible Values	Default Value
desc	The description of the ISAKMP peer. **Note**: if you wish to include spaces in the description, you must enclose the string in quotation marks (“”)	**1-80 characters**	

User level

read-write

Context

crypto isakmp peer

Example

```
G350-001(config-peer:135.64.102.109)# description "New York office"
Done!
```

destination-ip

Use the **`destination-ip`** command to specify the destination IP address of packets to which the current rule applies. Use the **no** form of the command to specify that the current rule will apply to all packets that do *not* have this destination IP address.

Syntax

`[no] destination-ip {host` ***`ip`*** **`} | any | {`** ***`ip wildcard`*** **`}`**

Parameters

Parameter	Description	Possible Values	Default Value
`host`	Keyword that specifies the current rule applies to a single host IP address		
`ip`	The destination IP address of the rule		
`any`	Keyword that specifies the current rule applies to any address		
`wildcard`	The range of IP addresses of the rule. 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 netmask.		

User level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule, ip crypto-list/ip-rule

Example

To specify that rule 22 applies to all packets having destination IP address 135.64.104.102:

```
G350-011(QoS 460/rule 22)# destination-ip host 135.64.104.102
```

To specify that rule 17 applies to packets whose destination IP address is in the range of 176.13.0.0 through 176.13.255.255:

```
G350-011(QoS 460/rule 17)# destination-ip 176.13.0.0 0.0.255.255
```

dir

Use the **`dir`** command to show the files that have been downloaded to the media gateway using the Avaya G350 Media Gateway Download interface and the SNMP MIB.

Syntax

`dir`

User level

read-only

Context

general

Example

To display a list of downloaded files:

```
G350-001> dir
M# file           ver num   file type     file location  file description
-- ----           --------  ---------     -------------  ----------------
1  MM714            53      SW RT Image     Nv-Ram          MM714 - image
2  MM710            8       SW RT Image     Nv-Ram          MM710 - image
4  MM712            0       SW RT Image     Nv-Ram          MM712 - image
5  MM722            51      SW RT Image     Nv-Ram          MM722 - image
6  MM312            50      SW RT Image     Nv-Ram          MM312 - image
7  Analog           0       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        0.11.1    SW Component  Flash Bank A  Software Image Bank A
10 G350-B        0.15.0    SW RT Image   Flash Bank B  Software Image Bank B
10 G350          N/A    SW Web Image     Nv-Ram        EmWeb application
10 G350-Booter   21.12.0   SW BootImage   Nv-Ram         Booter Image
10 dhcp-binding   N/A    DHCP Binding   Nv-Ram       IP Address Binding
```

disable link encryption

Use the **`disable link encryption`** command to disable H.248 signalling encryption.

Syntax

`disable link encryption`

User level

admin

Context

general

Example

To disable H.248 signalling encryption:

```
G350-001(super)# disable link encryption
Done!
```

disable media encryption

Use the **disable media encryption** command to disable Avaya media encryption (SRTP, AEA, RTP/AES).

Syntax

disable media encryption

User level

admin

Context

general

Example

To disable Avaya media encryption:

```
G350-001(super)# disable media encryption
Done!
```

disconnect ssh

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

Syntax

disconnect ssh session_id

Parameters

Parameter	Description	Possible Values	Default Value
session_id	The number of the SSH session to disconnect		

User level

admin

Context

general

distribution-list

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.

Syntax

`[no] distribution-list` ***`access_list_number type`*** **`[`*****`interface_type interface_number`*****`|`*****`protocol`*****`]`**

Parameters

Parameter	Description	Possible Values	Default Value
access_list_number	The number of the access list	**1-99**	
type	The type of the access list	**in, out**	
interface_type	The interface type		
interface_number	The interface number		
protocol	The protocol. This parameter is only relevant for outgoing list entries.	**static, ospf**	

User level

read-write

Context

Router: rip

Example

To apply distribution policy rule 10 to incoming router updates on the VLAN 1 interface:

```
G350-001(router:rip)# distribution-list 10 in "Vlan 1"
```

To apply distribution policy rule 20 to outgoing router updates on the Serial 2/1:1 interface:

```
G350-001(router:rip)# distribution-list 20 out "Serial 2/1:1":
```

To apply distribution policy rule 40 to outgoing router updates from OSPF:

```
G350-001(router:rip)# distribution-list 40 out ospf
```

dns-server

Use the **dns-server** command to set up to eight Domain Name Server (DNS) IP addresses. Use the **no** form of this command to clear the DNS IP addresses.

Syntax

[no] dns-server *ip-addr-list*

Parameters

Parameter	Description	Possible Values	Default Value
ip-addr-list	A list of up to eight IP addresses for the Domain Name Server	A list of IP addresses separated by spaces	**0.0.0.0**

User level

read-write

Context

dhcp pool

Example

To set 164.35.2.4 as the DNS IP address:

```
G350-001(DHCP 5)# dns-server 164.35.2.4
```

To set 164.35.2.4 and 135.64.102.3 as DNS IP addresses:

```
G350-001(DHCP 5)# dns-server 164.35.2.4 135.64.102.3
```

domain-name

Use the **`domain-name`** command to set a domain name string for the client. Use the **no** form of this command to clear the domain name.

Syntax

```
[no] domain-name domain name
```

Parameters

Parameter	Description	Possible Values	Default Value
domain name	The domain name	string, 1-255 bytes	null string

User level

read-write

Context

dhcp pool

Example

To set the domain name to “avaya.com”:

```
G350-001(DHCP 5)# domain-name avaya.com
```

dscp

Use the **`dscp`** command to specify the DSCP value that is set by the current policy operation. Use the **no** form of the command to specify that the current operation sets the DSCP value to the default.

Syntax

```
dscp {dscp_value | no-change}
```

```
no dscp
```

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The DSCP value	**0-63**	
no-change	The DSCP value is left unchanged		

User level

read-write

Context

ip qos-list composite-operation, ip capture-list ip-rule, ip pbr-list ip-rule

Note:

> In ip-rule context, this command tests packets to see if they match the specified DSCP value, but does not change the DSCP value.

Example

To specify that composite operation 17 sets the DSCP value of packets to 55:

```
G350-001(QoS 440/CompOp 17)# dscp 55
```

dscp-table

Use the **dscp-table** command to enter the DSCP table entry context for a particular DSCP value for the current QoS list. If the specified DSCP table entry does not exist, the system creates it.

Syntax

dscp-table *dscp_value*

Parameters

Parameter	Description	Possible Values	Default Value
dscp_value	The specific DSCP value to configure	**0-63**	

User level

read-write

Context

ip qos-list, capture-list

Example

To enter configuration mode for DSCP table entry 21:

```
G350-001(QoS 440)# dscp-table 21
```

ds-mode

Use the **`ds-mode`** command to specify the mode of the controller.

Note:

When you change the ds-mode, you must copy the running configuration to the startup configuration and reset the device.

Syntax

```
ds-mode {e1|t1}
```

Parameters

Parameter	Description	Possible Values	Default Value
`e1`	Keyword specifying to set the mode to E1		
`t1`	Keyword specifying to set the mode to T1		

User level

admin

Context

general

Example

To set the controller to operate in E1 mode:

```
G350-001(super)# ds-mode t1
```

To change ds-mode, copy the running configuration to the start-up configuration file, and reset the device.

duplex

Use the **duplex** command to control the duplex setting for the current interface.

Note:

This command functions only in **no autoneg** mode.

Syntax

```
duplex {full|half}
```

Parameters

Parameter	Description	Possible Values	Default Value
full	Keyword indicating that the interface is set to full duplex		
half	Keyword indicating that the interface is set to half duplex		

User level

read-only

Context

Interface: FastEthernet (L2, L2-L3)

Example

To specify full duplex for the FastEthernet interface:

```
G350-001(super-if:FastEthernet 1.1)# duplex full
```

dynamic-cac

Use the **dynamic-cac** command to set the dynamic CAC bearer bandwidth limit for the current interface. You can also specify an activation priority for the interface. In case more than one interface with a BBL value is up, the G350 reports the BBL of the interface with the highest activation priority.

Syntax

```
dynamic-cac bbl [activation_priority]
```

Parameters

Parameter	Description	Possible Values	Default Value
bbl	The bearer bandwidth for the current interface	0 - 100,000,000 Kbits/sec	-1
activation_ priority	The priority value of this interface	1-255	50

User level

read-write

Context

Interface: serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2-L3, USP PPP L2), FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3)

encapsulation

Use the **encapsulation** command to set the encapsulation mode for a serial interface. By default, the serial interface has PPP encapsulation. Use the **no** form of this command, which has no parameters, to return to the default.

Use the **encapsulation frame-relay** option to create a frame-relay interface of the IETF (RFC1490/RFC2427) type. This command deletes the PPP interface associated with the current serial interface. The PPP interface cannot be deleted if at least one IP interface is defined on it. Instead, the following message appears, “You cannot update this L2 interface since L3 interfaces are defined on it.”

Syntax

```
encapsulation {ppp | frame-relay type}
```

```
no encapsulation
```

Parameters

Parameter	Description	Possible Values	Default Value
ppp	Keyword indicating that the encapsulation be set to PPP		
frame-relay	Keyword indicating that the encapsulation be set to Frame Relay		
type	The value for the type of Frame Relay, ietf, for RFC 1490/RFC2427 encapsulation		

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, USP PPP L2, USP PPP L2-L3, USP FR L2)

Example

To create a Frame-Relay interface:

```
G350-001(if:Serial 2/1:1)# encapsulation frame-relay ietf
```

encapsulation pppoe

Use the **encapsulation pppoe** command to enable the PPPoE client. Use the **no** form of the command to return to disable the PPPoE client.

Note:

The **encapsulation pppoe** command fails if:

1. ’ip address’ is configured on the interface
2. The interface is part of a backup scheme
3. Dynamic CAC is configured on the interface

Syntax

encapsulation pppoe

no encapsulation

Parameters

Parameter	Description	Possible Values	Default Value
pppoe	Keyword indicating that the encapsulation be set to PPP Power Over Ethernet.		

User level

read-write

Context

Interface: Fast Ethernet

Example

To create a PPPoE interface:

```
G350-001(if:FastEthernet 10/2)# encapsulation pppoe
```

encryption

Use the **encapsulation** command to set the encryption algorithm for an ISAKMP policy. Use the **no** form of this command to clear the encryption algorithm.

Syntax

```
[no] encryption {des | 3des | aes}
```

Parameters

Parameter	Description	Possible Values	Default Value
encryption	The encryption algorithm to be used: **des** – Data Encryption Standard - 56 bits **3des** – Triple DES - 168 bits **aes** – Advanced Encryption Standard - 128 bits		**des**

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmp:1)# encryption 3des
Done!
```

end-ip-addr

Use the **end-ip-addr** command to set the end IP address of a DHCP pool IP address range. For manual/reservation leasing, set the end IP address to be identical to the start IP address.

Syntax

```
[no] end-ip-addr ip-addr
```

Parameters

Parameter	Description	Possible Values	Default Value
ip_addr	The end IP address of the DHCP pool IP address range	The end IP address must be larger than the start IP address. The number of IP addresses in one pool cannot exceed 256.	**0.0.0.0**

User level

read-write

Context

dhcp pool

Example

```
G350-001(DHCP 5)# end-ip-addr 135.64.120.4
```

erase phone-image

Use the **`erase phone-script`** command to delete a phone-image (A to D).

Syntax

`erase phone-imageA|phone-imageB|phone-imageC|phone-imageD`

User level

Read-write

Context

general

Example

```
interface# > erase phone-scriptA
Beginning erase operation .... Done!
```

erase phone-script

Use the **`erase phone-script`** command to delete phone-script A or phone-script B.

Syntax

`erase phone-scriptA|phone-scriptB`

User level

Read-write

Context

general

Example

```
interface# > erase phone-scriptA
Beginning erase operation .... Done!
```

erase startup-config

Use the **`erase startup-config`** command to reset the NVRAM parameters to the factory default values. This command is an alias for the command nvram initialize on page 249.

Syntax

```
erase startup-config
```

User level

read-write

Context

general

exit

Use the **`exit`** command to exit the current context. If you are in the root context, the **`exit`** command logs you out of the system.

Syntax

```
exit
```

User level

read-only

Context

all

Example

To exit the rule 22 configuration context, and then the access-control-list 330 context:

```
G350-001(ACL 330/ip rule 22)# exit

G350-001(ACL 330)# exit

G350-001#
```

fair-queue-limit

Use the **`fair-queue-limit`** command to specify the maximum number of packets that can be queued in the weighted fair queue. The allowable upper limit depends on the bandwidth configured for the interface.

Syntax

`fair-queue-limit size`

Parameters

Parameter	Description	Possible Values	Default Value
`size`	The maximum number of packets that can be queued in the weighted fair queue		

User level

admin

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when traffic shaping is configured

Example

```
G350-001(super-if:FastEthernet 10/2)# fair-queue-limit 500
```

fair-voip-queue

Use the **`fair-voip-queue`** command to enable Weighted Fair VoIP Queuing (WFVQ) on the current interface. WFVQ provides more fair service for data packets, and improves response time for interactive data applications (such as Telnet). 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.

Note:

> The commands **`fair-voip-queue`** and **`voip-queue`** are mutually exclusive, and cannot both appear in a configuration script.

Syntax

`fair-voip-queue`

User level

admin

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when traffic shaping is configured

Example

```
G350-001(super-if:FastEthernet 10/2)# fair-voip-queue
```

Done!

fdl

Use the **`fdl`** command to define the type of Facility Data Link loopback that the remote line is requested to enter. Use the **no** form of the command to disable FDL.

Note:

This command can only be used when ESF framing is defined.

Syntax

`fdl` ***`fdl_mode`***

`no fdl`

Parameters

Parameter	Description	Possible Values	Default Value
`fdl_mode`	The FDL type	**ansi, att, both**	

User level

read-write

Context

Interface: Controller (T1)

Example

To set the FDL type to ansi:

```
G350-001(controller:5/1)# fdl ansi
```

fragment chain

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.

Note:

No IP reassembly is performed on packets in transit through the router.

Syntax

`fragment chain` ***`chain_limit`***

`no fragment chain`

Parameters

Parameter	Description	Possible Values	Default Value
`chain_ limit`	The maximum number of fragments that can comprise a single IP packet	**2 – 2048**	**64**

User level

read-write

Context

general

Example

To set the maximum number of fragments for a single IP packet to 30:

```
G350-001# fragment chain 30
```

fragment size

Use the **`fragment size`** command to set the maximum number of fragmented IP packets to reassemble at any given time. Use the **`no`** form of this command to set the fragment size to its default value.

Note:

No IP reassembly is performed on packets in transit through the router.

Syntax

`fragment size` ***`database_limit`***

`no fragment size`

Parameters

Parameter	Description	Possible Values	Default Value
`database_limit`	The maximum number of packets undergoing re-assembly at any given time	**0-200**	**100**

User level

read-write

Context

general

Example

To set the maximum number of packets to reassemble to 150:

```
G350-001# fragment size 150
```

fragment timeout

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.

Note:

No IP reassembly of packets in transit through the router is performed.

Syntax

```
fragment timeout timeout
no fragment timeout
```

Parameters

Parameter	Description	Possible Values	Default Value
timeout	The maximum number of seconds to reassemble an IP packet	**5-120**	**10**

User level

read-write

Context

general

Example

To set the maximum time to reassemble packets to be 30 seconds:

```
G350-001# fragment timeout 30
```

frame-relay class-dlci

Use the **frame-relay class-dlci** command to associate a Virtual Channel with a named QoS or Traffic shaping template (map-class). Traffic shaping only works if it is enabled on the frame relay interface.

Use the **no** form of this command to return to the default map class.

Note:

The VC must exist and be associated with the sub-interface.

Syntax

```
[no] frame-relay class-dlci DLCI_number map_class_name
```

Parameters

Parameter	Description	Possible Values	Default Value
DLCI_number	The VC Data Link Channel Identifier	**16-1007**	
map_class_ name	The name of a user defined map class default - the default map class		

User level

read-write

Context

Interface: Serial (DS1 FR-SUB L2, DS1 FR-SUB L2-L3)

Example

To associate Virtual Channel number 17 with the map-class frame-relay named “myVoIpClass”:

```
G350-001(super-if:Serial 2/1:1)#frame-relay class-dlci 17 myVoIpClass
```

frame-relay interface-dlci

Use the **frame-relay interface-dlci** command to associate a frame relay Virtual Channel with this interface. This VC will be in the primary role (that is, will determine the operational status of the interface).

Use the **no** form of this command to delete the association of the VC and the sub-interface. To replace the currently configured interface-DLCI, use the **no** form of the command.

Syntax

[no] frame-relay interface-dlci *DLCI_number*

Parameters

Parameter	Description	Possible Values	Default Value
DLCI_number	The Virtual Channel Data Link Channel Identifier	**16-1007**	

User level

read-write

Context

Interface: Serial (DS1 FR-SUB L2, DS1 FR-SUB L2-L3)

Example

The following example will create and associate DLCI number 17 with the current sub-interface. This VC will carry all traffic (if no priority dlci-group is defined for this interface), and will be in the primary role.

```
G350-001(super-if:Serial 2/1:1)# frame-relay interface-dlci 17
```

frame-relay lmi-n391dte

Use the **`frame-relay lmi-n391dte`** command to set the number of status enquiry intervals that pass before issuing a full status enquiry message.

Use the **no** form of this command to set the number of status enquiry intervals to its default.

Syntax

```
[no] frame-relay lmi-n391dte polling_interval
```

Parameters

Parameter	Description	Possible Values	Default Value
polling_ interval	Interval in seconds	**1-255**	**6**

User level

read-write

Context

Interface: Serial (DS1 FR L2, USP FR L2)

Example

To set the number of seconds between status enquiry messages to 17 seconds:

```
G350-001(if:Serial 2/1:1)# frame-relay lmi-n391dte 17
```

frame-relay lmi-n392dte

Use the **`frame-relay lmi-n392dte`** command to set the maximum number of unanswered status enquiries the equipment accepts before declaring the interface down.

Use the **no** form of this command to revert to the default value.

Syntax

`[no] frame-relay lmi-n392dte` ***`threshold`***

Parameters

Parameter	Description	Possible Values	Default Value
`threshold`	Error threshold value	**1-10**	**3**

User level

read-write

Context

Interface: Serial (DS1 FR L2, USP FR L2)

Example

To set the maximum number of unanswered status enquiries allowed to 5:

```
G350-001(if:Serial 2/1:1)# frame-relay lmi-n392dte 5
```

frame-relay lmi-n393dte

Use the **`frame-relay lmi-n393dte`** command to set the number of status polling intervals over which the error threshold is counted (the monitored event count). To set the error threshold, refer to frame-relay lmi-n392dte on page 148. In other words, if within ***`events`*** number of events the station receives ***`error_threshold`*** number of errors, the interface is marked as down.

Use the **no** form of this command to revert to the default value.

Syntax

`[no] frame-relay lmi-n393dte` ***`events`***

Parameters

Parameter	Description	Possible Values	Default Value
events	The number of events	**1-10**	**4**

User level

read-write

Context

Interface: Serial (DS1 FR L2, USP FR L2)

Example

To set the number of events over which the error threshold is calculated to 5:

```
G350-001(if:Serial 2/1:1)# frame-relay lmi-n393dte 5
```

frame-relay lmi-type

Use the **frame-relay lmi-type** command to manually define the type of the Local Management Interface (LMI) to use.

Use the **no** form of this command to specify automatic detection of the LMI type (auto-sensing). If auto-sense fails, ANSI is used as the default.

Syntax

[no] frame-relay lmi-type *lmi_type*

Parameters

Parameter	Description	Possible Values	Default Value
lmi_type	The type of local management interface	**ansi** - LMI according to ANSI T1.617 [9] **q933a** - LMI according to ITU-T Q.933 [7] **autosense** **lmi-rev1** **disable**	

User level

read-write

Context

Interface: Serial (DS1 FR L2, USP FR L2)

Example

To select the q933a LMI type:

```
G350-001(if:Serial 2/1:1)# frame-relay lmi-type q933a
```

frame-relay priority-dlci-group

Use the **`frame-relay priority-dlci-group`** command to assign Virtual Channels to priority classifications, for supporting traffic separation. The first DLCI is assigned to the high priority traffic. Other DLCIs are assigned to Medium (L2:4-5), Normal (L2:2-3), and Low (L2:0-1) priorities. When fewer than 4 DLCIs are specified, the last DLCI on the command line is assigned to all the remaining unassigned priority classes.

Use the **no** form of this command to clear the current priority DLCI group.

Syntax

```
[no] frame-relay priority-dlci-group DLCI1 [DLCI2 [DLCI3 [DLCI4]]]
```

Parameters

Parameter	Description	Possible Values	Default Value
DLCI1	The DLCI assigned to the High priority traffic	**16-1007**	
DLCI2	The DLCI assigned to the Medium priority traffic	**16-1007**	
DLCI3	The DLCI assigned to the Normal priority traffic	**16-1007**	
DLCI4	The DLCI assigned to the Low priority traffic	**16-1007**	

User level

read-write

Context

Interface: Serial (DS1 FR-SUB L2, DS1 FR-SUB L2-L3)

Example

To assign VC number 17 to the High Priority traffic, VC number 18 to the Medium Priority traffic, and VC number 19 to the Normal to Low priority traffic:

```
G350-001(if:Serial 2/1:1.1)# frame-relay priority-dlci-group 17 18 19
```

frame-relay traffic-shaping

Use the **`frame-relay traffic-shaping`** command to turn on/off traffic shaping and Frame-Relay fragmentation. Virtual Channels that are not explicitly assigned to a map-class frame-relay, are assigned to the default map-class frame-relay.

Use the **no** form of this command to turn off traffic shaping.

Syntax

`[no] frame-relay traffic-shaping`

User level

read-write

Context

Interface: Serial (DS1 FR L2, USP FR L2)

Example

To enable traffic shaping on the interface:

```
G350-001(if:Serial 2/1:1)# frame-relay traffic-shaping
```

framing

Use the **`framing`** command to specify the frame type for an E1 or T1 data line. Use the **no** form of the command to restore the controller to the default frame type.

Syntax

`framing` ***`frame_type`***

`no framing`

Parameters

Parameter	Description	Possible Values	Default Value
frame_type	The framing method to use	**sf, esf, crc4, no-crc4, unframed**	For T1: **sf** For E1: **crc4**

User level

read-write

Context

Interface: Controller

Example

To set the frame type to extended super frame:

```
G350-001(controller:5/1)# framing esf
```

group

Use the **group** command to set the Diffie-Hellman group for an ISAKMP policy. Use the **no** form of the command to set the Diffie-Hellman group to the default.

Syntax

```
[no] group {1 | 2}
```

Parameters

Parameter	Description	Possible Values	Default Value
1 | 2	The Diffie-Hellman group for the ISAKMP policy	**1** or **2**	**1**

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmp:1)# group 1
Done!
```

hash

Use the **hash** command to set the hash method for an ISAKMP policy. Use the **no** form of the command to return the hash method to the default (sha).

Syntax

`[no] hash {sha | md5}`

Parameters

Parameter	Description	Possible Values	Default Value
hash	The hash method for the ISAKMP policy: **sha –** Secure Hash Algorithm **md5 –** Message Digest algorithm 5		**sha**

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmp:1)# hash md5
Done!
```

hostname

Use the **hostname** command to change the Command Line Interface (CLI) prompt. The prompt is written as **hostname-registration**, where the ***hostname*** is the value entered with the **hostname** command, and ***registration*** is the media gateway registration information. If the device is registered, the current media gateway number appears. If the device is not registered, question marks are displayed.

Use the **hostname** command with no parameters to display the current prompt value. Use the **no** form of this command to return the CLI prompt to the default.

Syntax

```
hostname [hostname_string]
no hostname
```

Parameters

Parameter	Description	Possible Values	Default Value
hostname_ string	The hostname	a string of up to 20 characters	**G350**

User level

read-write

Context

general

Example

To set the CLI prompt to “GTW-HQ”:

```
G350-001# hostname GTW-HQ
GTW-HQ-001# hostname
Session hostname is ’GTW-HQ’
```

To reset the CLI prompt to the default:

```
GTW-HQ-001# no hostname
G350-001#
```

icc-vlan

Use the **icc-vlan** command to set the current VLAN as the ICC-VLAN.

Syntax

```
icc-vlan
```

User level

read-write

Context

Interface: VLAN (L2, L2-L3)

Example

To set VLAN 2 as the ICC VLAN:

```
G350-001# interface vlan 2
G350-001(if:Vlan 2)# icc-vlan
```

icmp

Use the **icmp** command to specify that the current rule applies to a specific type of ICMP packet. Use the **no** form of this command to specify that the rule applies to all packets *except* those of the specified ICMP type.

Note:
The icmp command also sets the IP protocol to ICMP.

Syntax

[no] icmp {*name* | {*icmp_type icmp_code*}}

Parameters

Parameter	Description	Possible Values	Default Value
name	Specify that the rule applies to this ICMP name		
icmp_type	Specify that the rule applies to this icmp type	For an ip-rule: **0 – 256** For a QoS rule: **0 – 65535**	
icmp_code	Specify that the rule applies to this icmp code	For an ip-rule: **0 – 256** For a QoS rule: **0 – 65535**	

User level

read-write

Context

ip capture-list/ip-rule, ip access-control-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule

Example

To specify that rule 33 applies to any ICMP packet type except type 1 code 2:

```
G350-001(ACL 333/ip rule 33)# no icmp 1 2
```

To specify that rule 27 applies to ICMP error-reply packets:

```
G350-001(ACL 333/ip rule 27)# icmp Echo-Reply
```

icmp in-echo-limit

Use the **`icmp in-echo-limit`** command to set the maximum number of echo requests that can be received in one second. Use the **no** form of the command to the limit to its default value.

Syntax

`icmp in-echo-limit` ***`size`***

Parameters

Parameter	Description	Possible Values	Default Value
`size`	The number of echo requests	**1 – 10000**	

User level

read-write

Context

general

Example

To set the echo request limit at 500 packets per second:

```
G350-001# icmp in-echo-limit 500
```

idle-character

Use the **`idle-character`** command to set the bit pattern used to indicate an idle line. Use the **no** form of this command to restore the default value. For E1 and USP interfaces, the default value is **flags**. For T1 interfaces, the default is **marks**.

Syntax

`idle-character {flags|marks}`

`no idle-character`

Parameters

Parameter	Description	Possible Values	Default Value
`flags`	Keyword specifying that flags are transmitted to indicate an idle line		
`marks`	Keyword specifying that marks are transmitted to indicate an idle line		

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, USP PPP L2, USP PPP L2-L3, USP FR L2)

Example

To set the idle-character to marks:

```
G350-001(if:Serial 2/1)# idle-character marks
```

ignore dcd

Use the **`ignore dcd`** command to specify how the system monitors the line to determine if it is up or down. Specify **`ignore dcd`** to ignore DCD signals, and instead use DSR/CTS signals to determine the line's status. Use the **no** form of the command to specify that DCD signals are used to determine line status.

Syntax

`[no] ignore dcd`

User level

read-write

Context

Interface: Serial (USP FR-L2, USP PPP-L2, USP PPP L2-L3)

Example

To ignore DCD signals on an interface:

```
G350-001(if:Serial 2/1:1)# ignore dcd
```

interface Console

Use the **`interface Console`** command to enter the console interface configuration mode. The interface is created if it does not exist. Use the **no** form of this command to set the Console parameters to their default values.

Syntax

`[no] interface Console`

User level

read-write

Context

general

Example

To enter the Console interface context:

```
G350-001# interface Console
G350-001(if:Console)#
```

interface FastEthernet

Use the **`interface FastEthernet`** command to enter Interface FastEthernet configuration mode. Use the **no** form of this command to delete an IP interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

```
[no] interface FastEthernet [module/port[.ip_interface]]
```

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number of the interface	**10**	
port	The port number of the interface	**2**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User level

read-write

Context

general

Example

To create a FastEthernet interface and enter its context:

```
G350-001# interface FastEthernet 10/2
```

To create a Level 3 sub-interface on the FastEthernet interface:

```
G350-001# interface FastEthernet 10/2.1
```

To remove the Level 3 sub-interface:

```
G350-001# no interface FastEthernet 10/2.1
```

interface Loopback

Use the **`interface Loopback`** command to enter Interface Loopback configuration mode. Use the **no** form of this command to delete a loopback interface or sub-interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

```
[no] interface Loopback [interface_number[.ip_interface]]
```

Parameters

Parameter	Description	Possible Values	Default Value
interface_number	The number of the interface	**1-99**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User level

read-write

Context

general

Example

To create Loopback interface 1 and enter its configuration mode:

```
G350-001# interface Loopback 1
```

To create a Layer 3 sub-interface:

```
G350-001# interface Loopback 1.1
```

To delete the Layer 3 sub-interface:

```
G350-001# no interface Loopback 1.0
```

interface serial

Use the `interface serial` command to enter serial interface or sub interface configuration mode. If the specified interface or sub interface does not exist, the system creates it and enters its configuration mode.

Use the **no** form of the command to delete the interface. The **no** form can only be used to delete sub L3 and sub frame relay interfaces. The command fails for USP interfaces and when higher or lower layers are defined for that interface.

Syntax

`[no] interface Serial` ***`module/if_number`*** **`[`*`if_link_type`*`]`**

For USP interfaces ***if_number*** has the syntax:

port[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

For DS1 interfaces ***if_number*** has the syntax:

port:***channel_group***[.***ip_interface*** | {.***sub_interface***[.***ip_interface***]}]

Parameters

Parameter	Description	Possible Values	Default Value
port	The port number of the interface		
channel_group		For E1: **0-30** For T1: **0-23**	
sub_interface		**1-127**	
ip_interface		**0-1024**	
if_link_type		**point-to-point**	

User level

read-write

Context

general, Interface: Serial (FR SUB)

Example

To create point to point sub-interface number 17 over channel group 2 over E1/T1 controller number 1:

```
G350-001# interface Serial 2/1:2.17 point-to-point
```

interface tunnel

Use the **`interface tunnel`** command to enter Interface Tunnel configuration mode. Use the **no** form of this command to delete an interface tunnel.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

```
[no] interface tunnel tunnel_number
```

Parameters

Parameter	Description	Possible Values	Default Value
`tunnel_number`	The number of the interface	**1-99**	

User level

read-write

Context

general

Example

To create interface tunnel 1 and enter its configuration mode:

```
G350-001> interface tunnel 1
```

interface usb-modem

Use the **`interface usb-modem`** command to enter configuration context for the usb-modem. Use the **`no`** form of the command to reset the usb-modem settings to their factory defaults.

The usb-modem interface always exists, but is disabled by default. Use the **`no shutdown`** command to enable the interface.

The default settings for the usb-modem are:

`Interface status`	`DOWN`
`IP address`	`10.3.0.3`
`Netmask`	`255.255.255.0`
`timeout`	`no timeout`
`PPP speed`	`38400 bps`
`Async modem-init-string`	`"AT S7=45 S0=2 L1 V1 X4 &c1 E0 Q0"`

Syntax

`[no] interface usb-modem`

User level

read-write

Context

general

interface vlan

Use the **`interface vlan`** command to enter Interface VLAN configuration mode. Use the **no** form of this command to delete the interface.

If the specified interface does not exist, the system creates it and enters its configuration mode.

Syntax

`[no] interface vlan` ***`vlan_id`*****`[.`*****`ip_interface`*****`]`**

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	The VLAN ID number of this interface	**1-3071**	
ip_interface	The IP sub-interface number within this interface. A number of IP interfaces may be bound to a Layer 3 interface.	**0-1024**	

User level

read-write

Context

general

Example

To create VLAN 2 and enter its configuration context:

```
G350-001# interface Vlan 2
```

To create a sub interface 1 on VLAN 2:

```
G350-001(if:Vlan 2)# interface Vlan 2.1
```

To delete sub interface 1 of VLAN 2:

```
G350-001# no interface Vlan 2.1
```

invert txclock

Use the **invert txclock** command to invert the transmit clock signal from the data communications equipment (DCE). Use the **no** form of the command to restore the signal to not inverted.

Syntax

[no] invert txclock

User level

read-write

Context

Interface: Serial (USP FR L2, USP PPP L2, USP PPP L2-L3)

Example

To invert the transmit clock signal on an interface:

```
G350-001(if:Serial 2/1:1)# invert txclock
```

ip access-control-list

Use the **ip access-control-list** command to enter configuration mode for the specified policy access control list. If the specified list does not exist, the system creates it and enters its configuration mode.

Syntax

```
ip access-control-list list_number
```

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The Access Control list number	**300-399**	**300**

User level

read-write

Context

general

Example

To create access control list 320 and enter its configuration mode:

```
G350-001# ip access-control-list 320
G350-001(ACL 320)#
```

ip access-group

Use the **ip access-group** command to activate a specific Access Control list for a specific direction, on the current interface. Use the **no** form of this command to suspend the Access Control list for a specific direction.

Note:

You cannot edit the active Access Control list.

Syntax

```
ip access-group policy_list_number direction
```

```
no ip access-group direction
```

Parameters

Parameter	Description	Possible Values	Default Value
policy_list_number	The Access Control list number	**300-399**	**300**
direction	The direction of the packets to which the policy is applied.	**in, out**	

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Loopback (L2, L2-L3), FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3), VLAN (L2, L2-L3)

Example

To enable access control list 310 for outbound packets on the FastEthernet interface:

```
G350-001(if:FastEthernet 10/2)# ip access-group 310 out
```

ip address

Use the **ip address** command to assign an IP address and mask to an interface. Use the **no** form of this command to delete an IP interface.

Syntax

```
ip address ip_address mask [admin_state]
no ip address
```

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address assigned to the interface		

Parameter	Description	Possible Values	Default Value
mask	Mask for the associated IP subnet		
admin_state	The administration status. This parameter is not used with the Console interface.	**up, down**	**up**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Console, USB-modem, Loopback (L2-L3, L3), Tunnel (L2-L3, L3),

Example

To assign the IP address 192.168.22.33 with mask 255.255.255.0 to the Fast Ethernet interface:

```
G350-001(if:FastEthernet 10/2)# ip address 192.168.22.33 255.255.255.0
```

ip admin-state

Use the **`ip admin-state`** command to set the administrative state of an IP interface. The default state is **`up`**.

Syntax

```
ip admin-state up|down
```

Parameters

Parameter	Description	Possible Values	Default Value
up	Keyword specifying the administrative state of the IP interface is set to up (active)		
down	Keyword specifying the administrative state of the IP interface is set to down (inactive)		

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

ip bootp-dhcp network

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 remove the specified network.

Note:

> More than one network can be configured. For requests to servers, all configured networks are used. The networks are used on a round-robin basis.

Syntax

```
ip bootp-dhcp network ip_net
```

```
no ip bootp-dhcp network [ip_net]
```

Parameters

Parameter	Description	Possible Values	Default Value
ip_net	The IP subnet		

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To select the network 192.168.169.0 as the network from which an address should be allocated for BOOTP/DHCP requests:

```
G350-001(if:Vlan 1.20)# ip bootp-dhcp network 192.168.169.0
```

ip bootp-dhcp relay

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.

Syntax

`[no] ip bootp-dhcp relay`

User level

read-write

Context

general

Example

To enable relaying of BOOTP and DHCP requests:

```
G350-001# ip bootp-dhcp relay
```

To disable relaying of BOOTP and DHCP requests:

```
G350-001# no ip bootp-dhcp relay
```

ip bootp-dhcp server

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.

Syntax

`[no] ip bootp-dhcp server` ***`ip_address`***

Parameters

Parameter	Description	Possible Values	Default Value
`ip_address`	The IP address of the server		

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To add station 192.168.37.46 as a BOOTP/DHCP server to handle BOOTP/DHCP requests:

```
G350-001(if:Vlan 1.2)# ip bootp-dhcp server 192.168.37.46
```

ip broadcast-address

Use the **ip broadcast-address** command to update the interface broadcast address.

Syntax

```
ip broadcast-address bc_addr
```

Parameters

Parameter	Description	Possible Values	Default Value
bc_addr	The broadcast IP address		

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3)

Example

To set the broadcast address for the VLAN 1 interface to 192.168.255.255:

```
G350-001(if:Vlan 1)# ip broadcast-address 192.168.255.255
```

ip capture-list

Use the **`ip capture-list`** command to enter the specified capture-list context. If the specified capture-list does not exist, it is created.

Syntax

`ip capture-list capture_list_id`

`no ip capture-list capture_list_id`

Parameters

Parameter	Description	Possible Values	Default Value
`capture_list_id`	The capture list number	**500-599**	

User level

read-write

Context

general

Example

```
DR-006(super)# ip capture-list 501
DR-006(super/Cap 501)#
```

ip crypto-group

Use the **`ip crypto-group`** command to activate a crypto-list in the context of the interface on which the crypto-list is activated. The command applies to the following interfaces:

- Serial
- FastEthernet

Use the **no** form of the command to deactivate a crypto-list.

Note:

> The **`ip crypto-group`** command applies also to the VLAN interface, but this option is not recommended.

Note:

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`** command in the context of the interface on which the crypto-list is activated.

Syntax

`[no] ip crypto-group crypto-list-id`

Parameters

Parameter	Description	Possible Values	Default Value
`crypto_list_id`	The crypto-list number	**901-999**	

User level

read-write

Context

interface

Examples

```
G350-001(if:Serial 5/1)# no ip crypto-group
Done!
```

```
G350-001(if:Serial 5/1)# ip crypto-group 901
Done!
```

ip crypto-list

Use the **`ip crypto-list`** command to enter crypto-list context and create or edit a crypto-list. Use the **no** form of the command to delete a crypto-list.

Note:

You cannot delete an active crypto-list. You must first deactivate the list, using the **no** form of the **`ip crypto-group`** command.

Syntax

`[no] ip crypto-list` ***`index`***

Parameters

Parameter	Description	Possible Values	Default Value
index	The crypto-list number	**901-999**	

User level

read-write

Context

general

Example

```
G350-001# ip crypto-list 901
G350-001(Crypto 901)#
```

ip default-gateway

Use the **ip default-gateway** command to define a default gateway (router). Use the **no** form of this command to remove the default gateway.

Syntax

ip default-gateway {*ip_address* | {*interface_type interface_number*}} [*cost*] [*preference*] [permanent]

no ip default-gateway

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the router		
interface_type	The interface type		
interface_number	The interface number		
cost	The path cost		**1**
preference	The preference	**High, Low**	**Low**
permanent	Keyword that specifies not to disable the router if the interface is down		

User level

read-write

Context

general

Example

To set the default gateway to the IP address 132.55.4.45, having a cost value of 4 with high preference:

```
G350-001# ip default-gateway 132.55.4.45 4 high
```

To set the default gateway to be the Serial interface:

```
G350-001# ip default-gateway Serial 5/1:1.1 permanent
```

To remove the default gateway:

```
G350-001# no ip default-gateway
```

ip dhcp activate pool

When you create a DHCP pool, the pool remains inactive until you activate it. This allows you to modify the pool configuration with no effect on network devices. Use the **`ip dhcp activate pool`** command to activate the pool. Use the **no** form of this command to deactivate the pool. When you deactivate a pool, the binding information of all IP addresses from the pool that were allocated is erased.

Syntax

`[no] ip dhcp activate pool` ***`pool_id`***

User level

read-write

Context

general

Example

To activate DHCP pool 5:

```
G350-001# ip dhcp activate pool 5
```

To deactivate DHCP pool 5:

```
G350-001# no dhcp activate pool 5
```

ip dhcp pool

Use the **`ip dhcp pool`** to create a DHCP pool or to enter the context of a DHCP pool. Use the **no** form of this command to delete a DHCP pool.

Note:

> You cannot delete an active DHCP pool. Use the **no** form of the **`dhcp-pool`** command to deactivate a pool. When you deactivate the pool, any associated binding information is erased.

Syntax

`[no] ip dhcp pool` ***`pool-num`***

Parameters

Parameter	Description	Possible Values	Default Value
pool-num	The DHCP pool index	**1-32**	

User level

read-write

Context

general

Example

To enter the context of pool 5:

```
G350-001# ip dhcp pool 5
G350-001(DHCP 5)#
```

To delete pool 5:

```
G350-001# no ip dhcp pool 5
```

ip dhcp ping packets

Use the **`ip dhcp ping packets`** command to enable the sending of a ping packet by the DHCP server to check if the IP address it is about to allocate is already in use by another client. The purpose of this feature is to prevent IP address congestion. Use the **no** form of this command to disable the sending of these ping packets.

Note:

Sending a ping packet before each IP address allocation reduces the rate at which DHCP clients can get new IP addresses from the server. Therefore, by default, ping packets are not sent.

Syntax

```
[no] ip dhcp ping packets
```

User level

read-write

Context

general

Example

To configure the DHCP server not to send ping packets to an IP address before assigning the IP address to a requesting client:

```
G350-001(DHCP 5)# no ip dhcp ping packets
```

ip dhcp ping timeout

Use the **`ip dhcp ping timeout`** command to set the ping timeout. This is the time the DHCP server waits for a reply to a sent ping packet before allocating an IP address to a DHCP client. A lack of reply after the configured timeout indicates that the IP address is not in use and therefore can be allocated.

Syntax

```
ip dhcp ping timeout timeout
```

Parameters

Parameter	Description	Possible Values	Default Value
timeout	The amount of time, in milliseconds, that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment.	**25-1000 ms**	**500**

User level

read-write

Context

general

Example

To set the ping timeout to one second:

```
G350-001(DHCP 5)# ip dhcp ping timeout 1000
```

ip dhcp-server

By default, DHCP server is inactive. Use the **dhcp-server** command to activate the DHCP server on the G350. Use the **no** form of this command to deactivate the DHCP server.

Syntax

[no] ip dhcp-server

User level

read-write

Context

general

Example

To enable DHCP server:

```
G350-001# ip dhcp-server
```

To disable DHCP server:

```
G350-001# no ip dhcp-server
```

ip directed-broadcast

Use the **`ip directed-broadcast`** command to enable net-directed broadcast forwarding. Use the **no** form of this command to disable net-directed broadcasts on an interface.

Syntax

```
[no] ip directed-broadcast
```

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3)

ip distribution access-default-action

Use the **`ip distribution access-default-action`** command to set the default action for a specific RIP distribution policy list.

Syntax

```
ip distribution access-default-action list_number default_action
```

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The distribution list number	**1-99**	
default_action	The default action	**default-action-deny, default-action-permit**	

User level

read-write

Context

general

Example

To specify the default action for distribution policy list 1 is to deny packets:

```
G350-001# ip distribution access-default-action 1
default-action-deny
```

ip distribution access-list

Use the **`ip distribution access-list`** command to create a distribution Policy rule. Use the **no** form of this command to delete a distribution list rule. Apply the distribution rule using the **`distribution-list`** command.

Syntax

ip distribution access-list *policy_list_number access_list_index action* {{*router_ip* [*router_wildcard*]}|any}

no ip distribution access-list *access_list_number* [*access_list_index*]

Note:

If a list index is not given in the **`no ip distribution access-list`** command, all rules are deleted.

Parameters

Parameter	Description	Possible Values	Default Value
policy_list_number	The policy list number	**1-99**	
access_list_index	The access list index number	**1–9999**	
action	The action to perform	**permit, deny**	
router_ip	The IP router address of the network		
router_wildcard	The IP network wildcard address		
any	Keyword that specifies the value can be any IP address		

User level

read-write

Context

general

Example

To create distribution list 1, whose default action is to discard information from the network 10.10.0.0:

```
G350-001# ip distribution access-list 1 23 deny 10.10.0.0 0.0.255.255
```

To configure RIP distribution access list number 2 permitting distribution and learning of router 10.1.1.1:

```
G350-001# ip distribution access-list 2 24 permit 10.1.1.1
```

To configure RIP distribution access list number 20 permitting distribution and learning of all networks:

```
G350-001# ip distribution access-list 20 4 permit any
```

To remove RIP distribution access list number 2:

```
G350-001# no ip distribution access-list 2 25
```

ip distribution access-list-cookie

Use the **`ip distribution access-list-cookie`** command to set the list cookie.

Syntax

`ip distribution access-list-cookie` ***`list_id cookie`***

Parameters

Parameter	Description	Possible Values	Default Value
`list_id`	The ID of the distribution list	**1-99**	
`cookie`	The cookie number	integer	

User level

read-write

Context

general

Example

To set list 4 to have cookie 12345:

```
G350-001# ip distribution access-list-cookie 4 12345
```

ip distribution access-list-copy

Use the **`ip distribution access-list-copy`** command to copy the distribution access list.

Syntax

`ip distribution access-list-copy` ***`source_list destination_list`***

Parameters

Parameter	Description	Possible Values	Default Value
`source_list`	The source distribution access list	**1-99**	
`destination_list`	The destination distribution access list	**1-99**	

User level

read-write

Context

general

Example

To copy distribution list 1 to list 3:

```
G350-001# ip distribution access-list-copy 1 3
```

ip distribution access-list-name

Use the **`ip distribution access-list-name`** command to set the distribution list name.

Syntax

`ip distribution access-list-name` ***`distribution_list_number name`***

Parameters

Parameter	Description	Possible Values	Default Value
distribution_ list_number	The number of the distribution list	**1-99**	
name	The distribution list name		

Note:

To define a name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

User level

read-write

Context

general

Example

To name distribution access-list #5 as “evening”:

```
G350-001# ip distribution access-list-name 5 evening
```

To name distribution access-list #22 as “Daily Job”:

```
G350-001# ip distribution access-list-name 22 “Daily Job”
```

ip distribution access-list-owner

Use the **ip distribution access-list-owner** command to set the distribution list owner.

Syntax

ip distribution access-list-owner *policy_list_number owner*

Parameters

Parameter	Description	Possible Values	Default Value
policy_list_number	The distribution list number	**1-99**	
owner	The distribution list owner		

Note:

To define a name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

User level

read-write

Context

general

Example

To specify Jane Wiley as the owner of distribution list 78:

```
G350-001# ip distribution access-list-owner 78 “Jane Wiley”
```

ip http

Use the **ip http** command to enable the HTTP server. Use the **no** form of the command to disable the HTTP server.

Syntax

```
ip http [port port_number]
```

```
[no] ip http
```

Parameters

Parameter	Description	Possible Values	Default Value
port_number		**1-65535**	**80**

User level

admin

Context

general

ip icmp

Use the **`ip icmp`** command to enable ICMP services. Use the **no** form of the command to disable ICMP services.

Syntax

```
ip icmp [echo]
```

```
no ip icmp
```

Parameters

Parameter	Description	Possible Values	Default Value
echo	Enables ICMP only for echo packets and destination unreachable packets		

User level

read-write

Context

general

ip icmp redirect

Use the **`ip icmp redirect`** command to enable the ICMP redirect service. If the ICMP service is down, the command fails and returns an error message. Use the **no** form of the command to disable the ICMP redirect service.

Syntax

```
[no] ip icmp redirect
```

ip 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.

Syntax

```
[no] ip icmp-errors
```

User level

read-write

Context

general

ip max-arp-entries

Use the **`ip max-arp-entries`** command to specify the maximum number of ARP cache entries allowed in the ARP cache. Use the **no** form of this command to restore the default value. In order for this command to take effect, you must copy the running configuration to the startup configuration and reset the device.

Syntax

```
ip max-arp-entries value
no ip max-arp-entries
```

Parameters

Parameter	Description	Possible Values	Default Value
value	The maximum number of entries allowed in the IP address table. When you decrease the number of entries, it may cause the table to be relearned more frequently. If you do not enter a value, the current ARP Cache size is displayed.	**128-16384**	**4096**

User level

read-write

Context

general

Example

To set the maximum number of ARP cache entries to 8000:

```
G350-001# ip max-arp-entries 8000
```

To restore the maximum number of ARP cache entries to the default value:

```
G350-001# no ip max-arp-entries
```

ip netbios-rebroadcast

Use the **`ip netbios-rebroadcast`** command to enable the forwarding of NETBIOS packets on an interface. If no value is provided for ***`direction`***, the **both** option is applied as the default value.

Use the **no** form of this command to disable forwarding of NETBIOS packets on an interface.

Syntax

`ip netbios-rebroadcast [`*`direction`*`]`

`no ip netbios-rebroadcast`

Parameters

Parameter	Description	Possible Values	Default Value
`direction`	The NETBIOS rebroadcasts mode	**both** - NETBIOS packets received on the interface are rebroadcast to other interfaces and NETBIOS packets received on other interfaces are rebroadcast to this interface. **disable** - NETBIOS packets are not rebroadcast in or out of this interface.	**both**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L3, USP PPP L2-L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3)

Example

To enable rebroadcasting of NETBIOS packets received by and sent from the FastEthernet interface:

```
G350-001(if:FastEthernet 10/2)# ip netbios-rebroadcast both
```

ip netmask-format

Use the **`ip netmask-format`** command to specify the format of netmasks in the **`show`** command output. Use the **no** form of this command to restore the format to the default format.

Syntax

`ip netmask-format` ***`mask_format`***

`no ip netmask-format`

Parameters

Parameter	Description	Possible Values	Default Value
`mask_format`	The format of the netmasks	**bitcount** - Addresses are followed by a slash and the total number of bits in the netmask, such as 17. **decimal** - The network masks are in dotted decimal notation, such as 255.255.255.0. **hexadecimal** - The network masks are in hexadecimal format as indicated by the leading 0X, such as 0XFFFFFF00.	decimal

User level

read-write

Context

general

Example

To display netmasks in bitcount format:

```
G350-001# ip netmask-format bitcount
```

ip next-hop-list

Use the **`ip next-hop-list`** command to enter the context of the specified next hop list. If the list does not exist, it is created. Use the **no** form of this command to delete the specified next hop list.

Syntax

```
ip next-hop-list next_hop_number
```

```
no ip next-hop-list next_hop_number
```

Parameters

Parameter	Description	Possible Values	Default Value
`next_hop_number`	The number of the next hop list	1-20	

User level

read-write

Context

general

Example

```
G350-001# ip next-hop-list 2
```

```
G350-001(super-next hop list 2)#
```

ip ospf authentication

Use the **`ip ospf authentication`** command to specify the authentication type for an interface. Use the **no** form of the command to remove the authentication type for an interface.

Syntax

`ip ospf authentication` ***`auth_type`***

`no ip ospf authentication`

Parameters

Parameter	Description	Possible Values	Default Value
auth_type	The type of authentication	**message-digest, null**	**null**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To set the OSPF authentication for the FastEthernet interface as “message-digest”:

```
G350-001(if:FastEthernet 10/2)# ip ospf authentication message-digest
```

ip ospf authentication-key

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.

Syntax

`ip ospf authentication-key` ***`key`***

`no ip ospf authentication-key`

Parameters

Parameter	Description	Possible Values	Default Value
key	The interface authentication password	string (1-8 chars)	

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To set the authentication password for the VLAN 1 interface as “my_pass”:

```
G350-001(if:Vlan 1)# ip ospf authentication-key my_pass
```

ip ospf cost

Use the **ip ospf cost** command to statically configure the interface cost metric. Use the **no** form of this command to return to dynamic calculation of the cost.

Syntax

ip ospf cost *cost*

no ip ospf cost

Parameters

Parameter	Description	Possible Values	Default Value
cost	The price assigned to each interface for the purpose of determining the shortest path.	**1-65535**	**1**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To set the cost metric for the VLAN 1 interface to 10:

```
G350-001(if:Vlan 1)# ip ospf cost 10
```

ip ospf dead-interval

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.

Syntax

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The interval in seconds	**1-415029**	**40**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To specify an interval of 15 seconds to wait before declaring a neighbor dead:

```
G350-001(if:Vlan 1)# ip ospf dead-interval 15
```

ip ospf hello-interval

Use the **`ip ospf hello-interval`** command to specify the time interval between hello packets the router sends. Use the **no** form of this command to set the hello-interval to its default value.

Syntax

`ip ospf hello-interval` ***`seconds`***

`no ip ospf hello-interval`

Parameters

Parameter	Description	Possible Values	Default Value
`seconds`	The interval in seconds	**1-65535**	**10**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To specify an interval of five seconds between hello packets:

```
G350-001(if:Vlan 1)# ip ospf hello-interval 5
```

ip ospf message-digest-key

Use the **`ip ospf message-digest-key`** command to specify the message-digest key for the interface. This command enables OSPF MD5 authentication. Use the **no** form of the command to remove an old MD5 key.

Syntax

`ip ospf message-digest-key` ***`key_id algorithm key`***

`no ip ospf message-digest-key` ***`key_id`***

Parameters

Parameter	Description	Possible Values	Default Value
key_id	The OSPF key ID	**1-255**	**10**
algorithm		md5	
key	The OSPF password		

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To specify the message-digest key to be 3 with password mypwd:

```
G350-001(if:FastEthernet 10/2)# ip ospf message-digest-key 3 md5 mypwd
```

ip ospf network point-to-multipoint

Use the **ip ospf network point-to-multipoint** command to specify the network type as point-to-multipoint for the interface, and to increase the OSPF timers appropriately. Use the **no** form of the command to return the interface to point-to-point topology.

Syntax

```
[no] ip ospf network point-to-multipoint
```

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To specify a network type of point-to-multipoint for the VLAN 1 interface:

```
G350-001(if:Vlan 1)# ip ospf network point-to-multipoint
```

ip ospf priority

Use the **ip ospf priority** command to configure interface priority, which is used during the election of a designated router. Use the **no** form of this command to set the OSPF priority to its default value.

Syntax

ip ospf priority *priority*

no ip ospf priority

Parameters

Parameter	Description	Possible Values	Default Value
priority	The interface priority	**0-255**	**1**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L3, L2-L3)

Example

To set the interface OSPF priority to 17:

```
G350-001(if:Vlan 1)# ip ospf priority 17
```

ip ospf router-id

Use the **`ip ospf router-id`** command to configure the IP address of the router interface.

Syntax

`ip ospf router-id` ***`router_id`***

Parameters

Parameter	Description	Possible Values	Default Value
`router_id`	The IP address of the router		lowest existing IP interface

User level

read-write

Context

general

Example

To set the IP address of the router interface to 192.168.49.1:

```
G350-001# ip ospf router-id 192.168.49.1
```

ip pbr-group

Use the **`ip pbr-group`** command to apply the specified pbr list to the current interface. The pbr list is applied to ingress packets only. Use the **no** form of the command to disable the specified pbr list.

Syntax

`ip pbr-group list_number`

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The list number of the pbr list to be applied to ingress packets of the current interface	801-899	

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

```
G350-001> ip pbr-group 811
```

ip pbr-list

Use the **ip pbr-list** command to enter context of the specified pbr-list. If the list does not exist, it is created. Use the **no** form of the command to suspend the specified pbr-list.

Syntax

```
ip pbr-list list_number
```

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The list number of the policy list being entered	801-899	

User level

read-write

Context

general

Example

```
G350-001# ip pbr-list 802
G350-001(super-PBR 802)#
```

ip policy-list-copy

Use the **`ip policy-list-copy`** command to copy an existing policy list to a new list.

Note:
The source and destination lists must be of the same type. For example, you cannot copy an access control list to a QoS list.

Syntax

`ip policy-list-copy` ***`source_list destination_list`***

Parameters

Parameter	Description	Possible Values	Default Value
`source_list`	The list number of the policy list to copy	For access control lists: **300 – 399** For QoS lists: **400 – 499**	
`destination_list`	The list number of the policy to copy to	For access control lists: **301 – 399** For QoS lists: **401 – 499**	

User level

read-write

Context

general

Example

To copy the settings of access control list 330 to list 340:

```
G350-001# ip policy-list-copy 330 340
```

ip proxy-arp

Use the **`ip proxy-arp`** command to enable proxy ARP on an interface. Use the **no** form of this command to disable proxy ARP on an interface.

Syntax

```
[no] ip proxy-arp
```

User level

read-write

Context

Interface: FastEthernet (L2-L3, L3), VLAN (L2-L3, L3)

Example

To disable proxy ARP on an interface:

```
G350-001(if:Vlan 1)# no ip proxy-arp
```

ip qos-group

Use the **`ip qos-group`** command to activate the specified QoS list on the given interface. You must first create the QoS list using the **`ip qos-list`** command.

Syntax

```
ip qos-group policy_list direction
```

Parameters

Parameter	Description	Possible Values	Default Value
policy_list	The policy list number	**400-499**	**400**
direction	The direction of packets to which the policy applies.	**in, out**	

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To apply QoS list 440 to all incoming packets on the Vlan 1 interface:

```
G350-001(if:Vlan 1)# ip qos-group 440 in
```

ip qos-list

Use the **`ip qos-list`** command to enter configuration mode for the specified QoS list. If the QoS list does not exist, the system creates it and enters its configuration mode.

Syntax

`ip qos-list` ***`list_number`***

Parameters

Parameter	Description	Possible Values	Default Value
`list_number`	The policy list number	**400-499**	**400**

User level

read-write

Context

general

Example

To create QoS list 440 and enter its configuration context:

```
G350-012# ip qos-list 440
G350-012(QoS 440)#
```

ip redirects

Use the **`ip redirects`** command to enable the sending of redirect messages on the current interface. Use the **no** form of this command to disable redirect messages. By default, sending of redirect messages on the interface is enabled.

Syntax

```
[no] ip redirects
```

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3)

ip rip authentication key

Use the **`ip rip authentication key`** command to set the authentication string used on the current interface. Use the **no** form of this command to clear the password.

Syntax

```
ip rip authentication key password
```

```
no ip rip authentication key
```

Parameters

Parameter	Description	Possible Values	Default Value
password	The authentication string for the interface	string (1-16 chars)	

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To set the authentication string on the VLAN 1 interface to “hush-hush”:

```
G350-001(if:Vlan 1)# ip rip authentication key hush-hush
```

ip rip authentication mode

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.

Syntax

```
ip rip authentication mode [simple|none]
no ip rip authentication mode
```

Parameters

Parameter	Description	Possible Values	Default Value
`simple`	Keyword indicating that the clear text authentication should be used		
none	Keyword indicating that no authentication should be used		

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To specify that RIP packets use simple authentication mode:

```
G350-001(if:FastEthernet 10/2)# ip rip authentication mode simple
```

ip rip default-route-mode

Use the **`ip rip default-route-mode`** command to enable learning of the default route received by the RIP protocol. Use the **no** form of this command to disable listening to default routes.

Syntax

`ip rip default-route-mode` ***`mode`***

`no ip rip default-route-mode`

Parameters

Parameter	Description	Possible Values	Default Value
mode	The default mode	**talk-listen** — RIP sends and receives default route updates on the interface. **talk-only** — RIP sends, but does not receive, default route updates on the interface.	**talk-listen**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To specify that the RIP protocol sends, but does not receive, default route updates on the VLAN 1 interface:

```
G350-001(if:Vlan 1)# ip rip default-route-mode talk-only
```

ip rip poison-reverse

Use the **`ip rip poison-reverse`** command to enable split-horizon with poison-reverse on the current interface. Use the **no** form of this command to disable the poison-reverse mechanism.

The split-horizon technique prevents information about routes from exiting the router interface through which the information was received. This prevents routing loops.

Poison-reverse updates explicitly indicate that a network or subnet is unreachable. Poison-reverse updates are sent to defeat large routing loops.

Syntax

```
[no] ip rip poison-reverse
```

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

ip rip rip-version

Use the **`ip rip rip-version`** command to specify the RIP version running on the interface basis.

Syntax

```
ip rip rip-version [1|2]
```

Parameters

Parameter	Description	Possible Values	Default Value
1	Keyword indicating that RIP version 1 packets should be used		
2	Keyword indicating that RIP version 2 packets should be used		

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To specify that RIP version 2 packets should be running on the Serial 2/1:1 interface:

```
G350-001(if:Serial 2/1:1)# ip rip rip-version 2
```

ip rip send-receive-mode

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, send report).

Syntax

`ip rip send-receive-mode` ***`mode`*** **`[`*`default_route_metric`*`]`**

`no ip rip send-receive-mode`

Parameters

Parameter	Description	Possible Values	Default Value
mode	The RIP send and receive mode	**talk-listen** – RIP receives and transmits updates on the interface. **talkdefault-listen** – RIP receives updates on the interface and sends only a default route. **listen-only** – RIP receives updates on the interface and does not transmit them.	**talk-listen**
default_ route_metric	The route metric index	**1 - 15**	

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To set the RIP protocol to receive and transmit update on the Serial interface:

```
G350-001(if:Serial 2/1:1)# ip rip send-receive-mode talk-listen
```

ip rip split-horizon

Use the **`ip rip split-horizon`** command to enable the split-horizon mechanism on the current interface. Use the **no** form of this command to disable the split-horizon mechanism. By default split-horizon is enabled.

The split-horizon mechanism prevents information about routes from exiting the router interface through which the information was received. This prevents routing loops.

Syntax

```
[no] ip rip split-horizon
```

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L2-L3, USP PPP L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

ip route

Use the **`ip route`** command to establish a static route. Use the **no** form of this command to remove a static route.

Syntax

```
[no] ip route ip_addr mask
{{next_hop [next_hop [next_hop]] | interface_type interface_number}
[cost] [preference] [permanent] | Null0}
```

Parameters

Parameter	Description	Possible Values	Default Value
ip_addr	The IP address of the network		
mask	The mask of the static route		
next_hop	The next hop address in the network		
interface_type	The interface type		
interface_number	The interface number		
cost	The path cost		**1**
preference	The preference of the route	**High, Low**	**Low**
permanent	Keyword that specifies that the route is not disabled if the interface is down		
Null0	Keyword that creates a static discard route		

User level

read-write

Context

general

Example

To create a static route on IP address 132.55.0.0 with subnet mask 255.255.0.0 following the path 132.55.4.45, with cost of 3 and priority of high:

```
G350-001# ip route 132.55.0.0 255.255.0.0 132.55.4.45 3 high
```

To remove the static route defined for IP address 134.66.0.0:

```
G350-001# no ip route 134.66.0.0 255.255.0.0
```

To create a static discard route on IP address 134.66.0.0:

```
G350-001# ip route 134.66.0.0 255.255.0.0 Null0
```

ip routing

Use the **`ip routing`** command to enable IP routing.

Syntax

`ip routing`

User level

read-write

Context

general

ip rtp compression-connections

Use the **`ip rtp compression-connections`** command to control the number of Real-Time Transport Protocol (RTP) connections supported on the current interface. Use the **no** form of this command to restore the default. This command also sets the number of connections in the non-TCP space, not just RTP.

Note:

This command automatically enables TCP header compression on the current interface.

Syntax

`[no] ip rtp compression-connections` ***`number`***

Parameters

Parameter	Description	Possible Values	Default Value
`number`	The total number of connections in the non-TCP space to support on the current interface	**3-1000**	**16**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To allow 48 RTP connections on the Serial interface:

```
G350-001(if:Serial 2/1:1.1) ip rtp compression-connections 48
```

ip rtp header-compression

Use the **`ip rtp header-compression`** command to enable RTP header compression on the current interface. Use the **no** form of this command to disable RTP compression on the current interface.

Syntax

`[no] ip rtp header-compression`

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To enable RTP header compression on a Serial interface:

```
G350-001(if:Serial 2/1:1.1) ip rtp header-compression
```

ip rtp max-period

Use the **`ip rtp max-period`** command to set the maximum number of compressed headers that can be sent between full headers.

Syntax

`[no] ip rtp max-period` ***`number`***

Parameters

Parameter	Description	Possible Values	Default Value
number	The maximum number of compressed headers that can be sent until a full header is sent	**32-65535**	**256**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To allow a maximum of 512 compressed headers to be sent before a full header must be sent:

```
G350-001(if:Serial 2/1:1.1)# ip rtp max-period 512
```

ip rtp max-time

Use the **ip rtp max-time** command to set the maximum number of seconds between full headers.

Syntax

ip rtp max-time *number*

Parameters

Parameter	Description	Possible Values	Default Value
number	The maximum number of seconds between full headers	**1-255**	**5**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To allow no more than 15 seconds to pass between the sending of full headers:

```
G350-001(if:Serial 2/1:1.1)# ip rtp max-time 15
```

ip rtp non-tcp-mode

Use the **`ip rtp non-tcp-mode`** command to set the type of IP header compression to perform. 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 incompatible with non-ietf mode.

Syntax

`ip rtp non-tcp-mode {ietf | non-ietf}`

Parameters

Parameter	Description	Possible Values	Default Value
`ietf`	Keyword specifying ietf mode		
`non-ietf`	Keyword specifying non-ietf mode		

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To set the Serial interface to perform IPHC RFC header compression:

```
G350-001(if:Serial 2/1:1.1)# ip rtp non-tcp-mode ietf
```

ip rtp port-range

Use the **`ip rtp port-range`** command to set the range of UDP ports considered as RTP on the current interface. Set the range to be identical to the peer's configuration.

Some vendors use port range 49,152 through 65,535. For interoperability, the same port range should be used.

Syntax

`ip rtp port-range {`*`min`*`} {`*`max`*`}`

Parameters

Parameter	Description	Possible Values	Default Value
min	The starting port range to be considered RTP	**1025-65535**	**2048**
max	The ending port range to be considered RTP	**1025-65535**	**65535**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3)

Example

To specify that ports in the range 49,152 through 65535 are RTP ports:

```
G350-001(if:Serial 2/1:1.1)# ip rtp port-range 49152 65535
```

ip simulate

Use the **`ip simulate`** command to test the action of a policy on a simulated packet.

Syntax

`ip simulate` ***`policy_list_number direction`*** **`[`*`priority`*`] [`*`dscp_value`*`]`**
`source destination` **`[`*`protocol`*`[`*`source_port`***
`destination_port` **`[`*`established`*`]]]`**

Parameters

Parameter	Description	Possible Values	Default Value
policy_list_ number	The number of the policy	**300-499**	For ACL: **300** For Qos: **400**
direction	The direction	**in, out**	
priority	The priority	**fwd0-fwd7**	
dscp_value		**dscp0-dscp63**	
source	The source IP address		
destination	The destination IP address		
protocol	The protocol to use	**ip, tcp, udp, 1-255**	
source_port	The source port of the simulated packet	**1-65535**	
destination_ port	The destination port of the simulated packet	**1-65535**	
established	The value of the TCP established bit		

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), Loopback (L2, L2-L3), FastEthernet (L2-L3, L3), Tunnel (L2, L2-L3), VLAN (L2, L2-L3)

Example

To simulate the effects of applying access control list 330 to a packet entering the media gateway through the Fast Ethernet interface, from IP address 192.67.85.12 to IP address 192.67.54.25:

```
G350-001(if:FastEthernet 10/2)# ip simulate 330 in 192.67.85.12
192.67.54.25 ip
```

ip snmp-server

Use the **`ip snmp-server`** command to enable the SNMP agent for the G350. Use the **no** form of the command to disable the SNMP agent for the G350. Disabling the SNMP agent also blocks SNMP traps. However, users can change SNMP configuration settings even when the agent is disabled.

Syntax

`ip snmp-server [volatile]`

no ip snmp-server

Parameters

Parameter	Description	Possible Values	Default Value
`volatile`	specifies that the SNMP agent is only enabled temporarily, until the system is reset		

User level

admin

Context

general

Example

```
G350-001(ACL 330)> ip snmp-server volatile
```

ip ssh

Use the **`ip ssh`** command to enable the SSH service, and set configuration parameters. Use the **no** form of the command to disable the SSH service, and close any open connections currently using SSH. When disabling the service, the G350 issues a message listing all current management interfaces. If SSH is currently the only enabled management interface, the user is warned that the remote connection will be lost.

Note:

In order to enable SSH to be used, you must configure the server host key. See the **`crypto-key generate`** command.

Note:

Changing the port number does not break any active connections.

Syntax

```
ip ssh [port port_number]
```

```
no ip ssh
```

Parameters

Parameter	Description	Possible Values	Default Value
port_number	The new default value of the SSH port. Changing a port number does not tear down active connections so the operator that issued the request will stay connected and will not have to reopen an SSH session.	**1-65535**	22

User level

admin

Context

general

ip tcp decompression-connections

Use the **ip tcp decompression-connections** command to control the number of TCP connections that can be decompressed on the current interface. Use the **no** form of this command to restore the default. This command only exists in a PPP encapsulated interface.

Note:

The device is currently not capable of actively compressing TCP connections, rather it decompresses TCP connections compressed on the other side of the link.

Syntax

```
[no] ip tcp decompression-connections [number]
```

Parameters

Parameter	Description	Possible Values	Default Value
number	The maximum number of compressed TCP connections received on this interface that can be decompressed	**3-256**	**16**

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, USP PPP L2, USP PPP L2-L3)

Example

To specify that a maximum of 20 TCP connections can be decompressed on the Serial interface:

```
G350-001(if:Serial 2/1:1)# ip tcp decompression-connections 20
```

ip telnet

Use the **ip telnet** command to enable the Telnet server. Use the **no** form of the command to disable the Telnet server.

Note:

For security reasons, this command can only be executed from the Console port.

Note:

The **ip telnet** command is a secured command and will not be displayed together with the running configuration (using the **show running-config** command). To see the status of this command, use the **show protocol** command (refer to show protocol on page 477).

Syntax

```
ip telnet [port port_number]
```

no ip telnet

Parameters

Parameter	Description	Possible Values	Default Value
port_number	Changes the default port of the Telnet server	**1-65535**	**23**

User level

admin

Context

general

ip telnet-client

Use the **ip telnet-client** command to enable the Telnet client. Use the **no** form of the command to disable the Telnet client.

Note:

For security reasons, this command can only be executed from the console port.

Note:

The **ip telnet** command is a secured command and will not be displayed together with the running configuration (using the **show running-config** command). To see the status of this command, use the **show protocol** command (refer to show protocol on page 477).

Syntax

```
[no] ip telnet-client
```

User level

admin

Context

general

ip tftp-server

Use the **`ip tftp-server`** command to enable the TFTP server. Use the **`no ip tftp-server`** command to disable the TFTP server.

Syntax

`[no] ip tftp-server`

User level

Read-write

Context

general

Example

```
interface# > ip tftp-server
```

ip tftp-server file-system size

Use the **`ip tftp-server file-system-size`** command to set the TFTP file system size. Use the **`no ip tftp-server file-system-size`** command to reset the TFTP file system size.

Syntax

`[no] ip tftp-server file-system-size <`*`size`*`>`

Parameters

Parameter	**Description**	**Possible Values**	**Default Value**
size	The TFTP server total fie size in kb.	**256 to 19456**	18560

User level

Read-write

Context

general

Example

```
interface# > ip tftp-server file-system-size 18128
To change ip tftp-server file system size, copy the running configuration to the
start-up configuration file, and reset the device
```

ip vrrp

Use the **`ip vrrp`** command to create a virtual router on the current interface. Use the **no** form of this command to delete a virtual router.

Syntax

`[no] ip vrrp` ***`vr_id`***

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To create virtual router #1 on the Vlan 2 interface:

```
G350-001(if:Vlan 2)# ip vrrp 1
```

ip vrrp address

Use the **`ip vrrp address`** command to assign an IP address to the virtual router. Use the **no** form of this command to remove an IP address from a virtual router.

Syntax

`[no] ip vrrp` ***`vr_id`*** **`address`** ***`ip_address`***

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID number.	**1-255**	
ip_address	The IP address to assign to the virtual router		

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To assign address 10.0.1.2 to virtual router 1:

```
G350-001(if:Vlan 2)# ip vrrp 1 address 10.0.1.2
```

ip vrrp auth-key

Use the **ip vrrp auth-key** command to set the virtual router simple password authentication for the virtual router ID. Use the **no** form of this command to disable simple password authentication for the virtual router instance.

Syntax

[no] ip vrrp *vr_id* auth-key *key_string*

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	
key_string	The password string		

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify the password authentication for virtual router 1 as “sec01”:

```
G350-001(if:Vlan 2)# ip vrrp 1 auth-key sec01
```

ip vrrp override addr owner

Use the **`ip vrrp override addr owner`** command to accept packets addressed to the IP address associated with the virtual router, such as ICMP, SNMP, and Telnet (if it is not the IP address owner and it is the master). Use the **no** form of this command to discard these packets.

Syntax

`[no] ip vrrp` ***`vr_id`*** **`override addr owner`**

Parameters

Parameter	Description	Possible Values	Default Value
`vr_id`	The virtual router ID	**1-255**	

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify that virtual router 1 accepts ICMP, SNMP, and Telnet packets:

```
G350-001(if:Vlan 2)# ip vrrp 1 override addr owner
```

ip vrrp preempt

Use the **`ip vrrp preempt`** command to configure the router to preempt a lower priority master for the virtual router ID. Use the **no** form of this command to disable preemption for the virtual router instance. By default, preemption is enabled.

Syntax

```
[no] ip vrrp vr_id preempt
```

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify that virtual router 1 preempts a lower priority master:

```
G350-001(if:Vlan 2)# ip vrrp 1 preempt
```

ip vrrp primary

Use the **`ip vrrp primary`** command to set the primary address that is 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 the virtual router instance. By default, the primary address is selected automatically by the device.

Syntax

```
[no] ip vrrp vr_id primary ip_address
```

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	
ip_address	The primary IP address of the virtual router. This address should be one of the router addresses on the fabric.		

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify the source IP address for virtual router 1 as 192.168.66.23:

```
G350-001(if:Vlan 2)# ip vrrp 1 primary 192.168.66.23
```

ip vrrp priority

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.

Syntax

[no] ip vrrp *vr_id* priority *pri_value*

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	
pri_value	The priority value	**1-254**	

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To specify the priority of virtual router 1 as 10:

```
G350-001(if:Vlan 2)# ip vrrp 1 priority 10
```

ip vrrp timer

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.

Syntax

[no] ip vrrp *vr_id* timer *value*

Parameters

Parameter	Description	Possible Values	Default Value
vr_id	The virtual router ID	**1-255**	
value	The advertisement transmit time in seconds	**1-255**	

User level

read-write

Context

Interface: FastEthernet (L2-L3, L2), VLAN (L2-L3, L2)

Example

To set the virtual router advertisement timer value for virtual router 3 to 2 seconds:

```
G350-001(if:Vlan 2)# ip vrrp 3 timer 2
```

ip-fragments-in

Use the **`ip-fragments-in`** command to specify the action taken on incoming IP fragmentation packets for the current access control list. Use the no form of the command to return to the default treatment of IP fragmentation packets.

Syntax

`ip-fragments-in` ***`operation`***

`no ip-fragments-in`

Parameters

Parameter	**Description**	**Possible Values**	**Default Value**
`operation`	The name of the pre-defined composite operation to execute.	**Deny, Deny-Notify-Rst, Permit, Deny-Notify, Deny-Rst**	

User level

read-write

Context

ip access-control-list

Example

To execute the Deny-Notify composite-operation when IP fragmentation packets are received:

```
G350-001(ACL 330)# ip-fragments-in Deny-Notify
```

ip-option-in

Use the **`ip-option-in`** command to specify the treatment of packets carrying an IP option that enter the current interface. Use the **no** form of the command to return to the default treatment of IP option packets.

Syntax

`ip-option-in` ***`action`***

`no ip-option-in`

Parameters

Parameter	Description	Possible Values	Default Value
action	The action to take	**permit, deny, deny-notify, deny-rst, deny-notify-rst**	

User level

read-write

Context

ip access-control-list

Example

To specify that incoming packets with an IP option are permitted:

```
G350-001(ACL 330)# ip-option-in permit
```

ip-protocol

Use the **ip-protocol** command to specify that the current rule applies to packets having the specified IP protocol. Use the **no** form of this command to specify that the current rule applies to all packets *except* those having the specified IP protocol.

Syntax

```
[no] ip-protocol protocol_name | protocol_number
```

Parameters

Parameter	Description	Possible Values	Default Value
protocol_name	Name of the IP protocol to match		
protocol_number	Number of the IP protocol to match	**1-255**	

User level

read-write

Context

ip access-control-list/ip-rule, ip capture-list/ip-rule, ip pbr-list/ip-rule, ip qos-list/ip-rule

Example

To specify that rule 22 applies to all packets having an IP protocol of IGMP:

```
G350-001(ACL 330/ip rule 22)# ip-protocol igmp
```

ip-rule

Use the **ip-rule** command to enter configuration mode for the specified rule. If the specified rule does not exist, the system creates it and enters its configuration mode.

Syntax

ip-rule {*rule_index* | default}

Parameters

Parameter	Description	Possible Values	Default Value
rule_index	Number of the rule to edit	**1 – 9999**	
default	ip-rule number 10,000 (last rule in the ordered list of rules)		

User level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To enter configuration mode for ip-rule 22:

```
G350-001(ACL 330)# ip-rule 22
G350-001(ACL 330/ip rule 22)#
```

ip-rule

Use the **`ip-rule`** command to enter ip-rule context and create or modify a specific rule. Use the **no** form of the command to delete a specific rule.

Syntax

`[no] ip-rule {`*`index`*` | default}`

Parameters

Parameter	Description	Possible Values	Default Value
`index`	Number of the ip-rule	**1 – 1000**	
`default`	ip-rule number 10,000 (last rule in the ordered list of rules)		

User level

read-write

Context

ip crypto-list

Example

```
G350-001(Crypto 901)# ip-rule 21
G350-001(Crypto 901/ip rule 21)#
```

isakmp-policy

Use the **`isakmp-policy`** command to set the ISAKMP policy for the ISAKMP peer. Use the **no** form of the command to delete the ISAKMP policy for the ISAKMP peer.

Note:

> You cannot delete an ISAKMP policy that is referenced by an ISAKMP peer that is, in turn, referenced by an active crypto map.

Syntax

`[no] isakmp-policy `*`id`*

Parameters

Parameter	Description	Possible Values	Default Value
id	The ID of the ISAKMP policy	**1 – 20**	

User level

read-write

Context

crypto isakmp peer

Example

```
G350-001(config-peer:149.49.70.1)# isakmp-policy 20
Done!
```

keepalive

Use the **keepalive** command to enable PPP keepalive, in order to maintain a persistent connection. Entering keepalive without a parameter returns the keepalive to its default value. Use the **no** form of this command to disable PPP keepalive.

Syntax

[no] keepalive [*seconds*]

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds between PPP keepalive messages. Entering keepalive 0 disables keepalive.	**0-32767**	**10**

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, USP PPP L2, USP PPP L2-L3, USP FR L2)

Example

To enable PPP keepalive, and generate a message every 300 seconds:

```
G350-001(if:Serial 2/1)# keepalive 300
```

keepalive

Use the **`keepalive`** command to enable the extended keepalive mechanism on an interface. Extended keepalive provides status information about the interface based on the IP state of the link. Use the **no** form of the command to disable extended keepalive on the interface.

Syntax

`keepalive` ***`ip_address next_hop_mac_address`***

no keepalive

Parameters

Parameter	Description	Possible Values	Default Value
`ip_address`	The destination address whose status is reported on		
`next_hop_ mac_address`	The next hop address (for the Ethernet port only)		

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To enable extended keepalive on the FastEthernet 10/2 interface for destination IP address 192.15.6.34:

```
G350-001(if:FastEthernet 10/2)# keepalive 192.15.6.34
```

keepalive failure-retries

Use the **`keepalive`** failure-retries command to specify the number of keepalive packets that are sent without a response before the interface is declared to be down. Using this command without a parameter resets the failure-retry value to the default value of 4.

Syntax

`keepalive` failure-retries ***`retries`***

Parameters

Parameter	Description	Possible Values	Default Value
`retries`	The number of retries	**1-32**	**4**

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To specify that the FastEthernet interface is declared down after 10 keepalive packets are sent without response:

```
G350-001(if:FastEthernet 10/2)# keepalive failure-retries 10
```

keepalive interval

Use the **`keepalive interval`** command to specify the interval in seconds between keepalive packets. Using this command without a parameter resets the interval value to its default.

Syntax

`keepalive` interval ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The interval between keepalive packets, in seconds.	**1-36**	**5**

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To set the interval between keepalive packets on the FastEthernet 10/2 interface to be 15 seconds:

```
G350-001(if:FastEthernet 10/2)# keepalive interval 15
```

keepalive source-address

Use the **keepalive source-address** command to specify the source IP address of the keepalive packets. Using this command with no parameter resets the source IP address value to the IP address of the interface.

Syntax

keepalive source-address *ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The source IP address of the keepalive packets		

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To set the source IP address of the keepalive packets on the FastEthernet interface to be 192.15.6.34:

```
G350-001(if:FastEthernet 10/2)# keepalive source-address 192.15.6.34
```

keepalive success-retries

Use the **`keepalive success-retries`** command to specify the number of keepalive packets that must be sent and successfully responded to before the interface is declared to be up. Using this command without a parameter resets the success-retry value to the default value.

Syntax

`keepalive` success-retries ***`retries`***

Parameters

Parameter	Description	Possible Values	Default Value
`retries`	The number of successful keepalive packets to require	**1-32**	**1**

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To specify that 5 keepalive packets must be send and successfully responded to in order for the FastEthernet interface to be declared up:

```
G350-001(if:FastEthernet 10/2)# keepalive success-retries 5
```

keepalive timeout

Use the **`keepalive timeout`** command to specify the time in seconds within which a keepalive response must be received. Using this command without a parameter resets the keepalive service to its default timeout value.

Syntax

`keepalive` timeout ***`seconds`***

no keepalive

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds to wait for a response	**1-10**	**1**

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To specify a timeout value of 6 seconds for keepalive packets on the FastEthernet interface:

```
G350-001(if:FastEthernet 10/2)# keepalive timeout 6
```

lease

Use the **`lease`** command to set the lease of a DHCP pool.

Syntax

`lease {`*`seconds`*`|infinite}`

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The duration of the lease, in seconds	Unsigned integer 32	**691200** (8 days)
infinite	Sets the lease to permanent		

User level

read-write

Context

dhcp pool

Example

To set a lease of 1 day:

```
G350-001(DHCP 5)# lease 86400
```

lifetime

Use the **lifetime** command to set the lifetime of the ISAKMP SA in seconds. Use the **no** form of the command to return the lifetime to the default value.

Note:

You cannot change the lifetime settings of an ISAKMP policy referenced by an ISAKMP peer that is linked to a crypto map.

Syntax

```
[no] lifetime seconds
```

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds defining the lifetime of the ISAKMP SA	**60-86,400** **(1 min. to 24 hrs)**	**86,400**

User level

read-write

Context

crypto isakmp policy

Example

```
G350-001(config-isakmmp:1)# lifetime 100
Done!
```

line

Use the **`line`** command to add a line to the current banner message.

Syntax

`line` ***`number`*** **`[`*****`string`*****`]`**

Parameters

Parameter	Description	Possible Values	Default Value
`number`	The line number to add the specified text	**1–24**	
`string`	The text to display on the specified line		

Note:

To define a string that includes spaces, enclose the entire string in quotation marks (for example, “New York”).

User level

admin

Context

banner login, banner post-login

Example

To specify text for the third line of the banner displayed after a successful login:

```
G350-001(super-banner-post-login)# line 3 “Welcome to the G350 Media
Gateway CLI Interface”
```

linecode

Use the **`linecode`** command to specify the type of line-code transmission for the an E1 line. Use the **no** form of the command to restore the default line-code value of **hbd3**.

Note:

Normally the E1 service provider determines which type of line-code is required for your E1 circuit.

Syntax

```
linecode {ami|hdb3}
```

Parameters

Parameter	Description	Possible Values	Default Value
`ami`	Keyword that specifies the Alternate Mode Inversion line-code type		
`hbd3`	Keyword that specifies the High-Density Bipolar 3 line-code type		

User level

read-write

Context

Interface: Controller (E1)

Example

To set the line-code type to ami:

```
G350-001(controller:5/1)# linecode ami
```

linecode

Use the **`linecode`** command to specify the type of line-code transmission for the a T1 line. Use the **no** form of the command to restore the default line-code value of **b8zs**.

Note:

Normally the T1 service provider determines which type of line-code is required for your T1 circuit.

Syntax

```
linecode {ami|b8zs}
```

Parameters

Parameter	Description	Possible Values	Default Value
ami	Keyword that specifies the Alternate Mode Inversion line-code type		
b8zs	Keyword that specifies the B8ZS line-code type		

User level

read-write

Context

Interface: Controller (T1)

Example

To set the line-code type to ami:

```
G350-001(controller:5/1)# linecode ami
```

load-interval

Use the **load-interval** command to set the load calculation interval for an interface. Use the **no** form of the command to restore the load calculation to its default value.

Note:

The load interval must be in increments of 30 seconds.

Syntax

```
load-interval seconds
no load-interval
```

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The load calculation interval, in seconds. This parameter must be divisible by 30.	**30-600**	**300**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP PPP L2-L3, USP PPP L2, USP FR L2), FastEthernet (L2, L2-L3), VLAN (L2-L3, L2), Loopback (L2-L3, L2), Tunnel (L2, L2-L3)

Example

To set the load calculation interval to 60 seconds:

```
G350-001(if:Serial 2/1:1)# load-interval 60
```

local-address

Use the **`local-address`** command to set the local IP address for the IPSec tunnels derived from the crypto-list. Use the **no** form of the command to delete the local IP address.

Note:

You must configure a local address before activating a list.

Note:

You cannot change or delete the local address of an active list.

Syntax

```
[no] local-address {ip-interface-address}
```

Parameters

Parameter	Description	Possible Values	Default Value
`ip-interface-address`	The local IP address.		

User level

read-write

Context

ip crypto-list

Example

```
G350-001(crypto 901)# local-address 192.168.49.1
Done!
```

loopback diag

Use the **`loopback diag`** command to activate a Loopback signal on the Serial interface. Use the **no** form of the command to deactivate the Loopback signal.

Syntax

`[no] loopback diag`

User level

read-write

Context

Interface: Controller

Example

To activate a Loopback signal on the current interface:

```
G350-001(if:Serial 5/1)# loopback diag
```

loopback local

Use the **`loopback local`** command to activate a Loopback signal on the Serial interface. Use the **no** form of the command to deactivate the Loopback signal.

Syntax

`loopback local` ***`loopback_type`***

`no loopback local`

Parameters

Parameter	Description	Possible Values	Default Value
loopback_type	The type of information to loop back	line, payload	

User level

read-write

Context

Interface: Controller

Example

To activate a loopback signal with payload information:

```
G350-001(if:Serial 5/1)# loopback local payload
```

loopback remote

Use the **loopback remote** command to request a remote station to activate a Loopback signal on the Serial interface. Use the **no** form of the command to deactivate the Loopback signal.

Syntax

loopback remote *loopback_type*

no loopback remote

Parameters

Parameter	Description	Possible Values	Default Value
loopback_type	The type of information to loop back	line, payload	

User level

read-write

Context

Interface: Controller (T1)

Example

To request that a loopback signal be sent with payload information:

```
G350-001(if:Serial 5/1)# loopback remote payload
```

map-class frame-relay

Use the **map-class frame-relay** command to create a QoS template named ***map_class_name***, which can later be assigned to DLCIs.

Use the **no** form of this command to delete a map class.

Note:

This command fails if the map class is currently associated with a DLCI.

Syntax

[no] map-class frame-relay *map_class_name*

Parameters

Parameter	Description	Possible Values	Default Value
map_class_name	The name of a map class configured by the user		

User level

read-write

Context

general

Example

To create a map class named mySVoip1:

```
G350-011# map-class frame-relay mySVoip1
G350-011(map-class)#
```

mtu

Use the **mtu** command to set the current interface's Maximum Transmission Unit (MTU). Use the **no** form of this command to restore the interface's MTU to its default value.

Note:

The ***size_in_bytes*** parameter specifies the Layer 3 packet size. Layer 2 headers are added to the packet afterwards. The Layer 2 headers vary in size, depending on the type of interface. Thus the total size of the MTU is the sum of the ***size_in_bytes*** value and the Layer 2 headers.

Syntax

```
[no] mtu size_in_bytes
```

Parameters

Parameter	Description	Possible Values	Default Value
size_in_ bytes	The Maximum Transmission Unit in bytes	**64-1500**	**1500**

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3)

Example

To specify the Maximum Transmission Unit for the Serial 2/1:1 interface to be 1000 bytes:

```
G350-001(if:Serial 2/1:1)# mtu 1000
```

name

Use the **name** command to assign a name to the specified list or operation. Use the **no** form of the command to return the name to the default value.

Syntax

```
[no] name name
```

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the list or operation. **Note**: if you wish to include spaces in the description, you must enclose the string in quotation marks (“”).	String of 1-31 characters.	

User level

read-write

Context

dhcp pool, dhcp pool vendor specific, dhcp pool option, ip qos-list, ip qos-list dscp-table, ip qos-list composite-operation, ip access-control-list, ip next-hop-list, ip capture-list, ip pbr-list.

Example

To specify the name of access control list 330 as “Admin13”:

```
G350-001(ACL 330)# name Admin13
```

network

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.

Syntax

```
[no] network ip_address [wildcard_mask]
```

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the network of directly connected networks		
wildcard_mask	The wildcard mask address number		

User level

read-write

Context

Router: RIP

Example

To specify that RIP is used on all interfaces connected to the network 192.168.37.0:

```
G350-001(router:rip)# network 192.168.37.0
```

network

Use the **network** command to enable OSPF in this network. Use the **no** form of this command to disable OSPF in this network. The default value is disabled.

Syntax

network *net_addr* [*wildcard_mask* [area *area_id*]]

Parameters

Parameter	Description	Possible Values	Default Value
net_addr	The IP address		
wildcard_mask	The wildcard mask		
area	Keyword specifying an area		
area_id	The area ID number		

User level

read-write

Context

Router: ospf

Example

To enable OPSF on the range of IP addresses from 192.168.0.0 to 192.168.255.255 in area ID 0.0.0.0:

```
G350-001(router:ospf)# network 192.168.0.0 0.0.255.255 area 0.0.0.0
```

next-hop

Use the **next-hop** command to specify the next-hop policy to use when the current rule is applied.

Syntax

next-hop {list list_number | DBR}

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The next-hop list to be used for the current rule	**1-20**	
DBR	Use destination based routing (not policy based routing) for the current rule		

User level

read-write

Context

ip-pbr-list/ip-rule

Examples

```
G350-001# next-hop list 1
```

```
G350-001# next-hop DBR
```

next-hop-interface

Use the **`next-hop-interface`** command to add the specified interface to the next hop path for this next-hop list. Use the **no** form of this command to delete an interface from the next-hop list.

Syntax

```
next-hop-interface {index | interface_name}
```

```
no next-hop-interface {index}
```

Parameters

Parameter	Description	Possible Values	Default Value
index	The index in the array of next-hops belonging to the specific next-hop-list	**1-20**	
interface_name	The specified next-hop interface name	The layer2 interfaces: (Serial, Gre Tunnel, null0).	

User level

read-write

Context

ip next-hop-list

Example

```
G350-001> next-hop-interface 3 Serial5/1:0
```

next-hop-ip

Use the **next-hop-ip** command to add the specified ip address to the next hop path for this next-hop list. Use the **no** form of this command to delete an ip address from the next-hop list.

Syntax

next-hop-ip {index | ip_address}

no next-hop-ip {index}

Parameters

Parameter	Description	Possible Values	Default Value
hop_number	The index in the array of next-hops belonging to the specific next-hop-list	**1-20**	
ip_address	The specified next-hop IP address		

User level

read-write

Context

ip next-hop-list

Example

```
G350-001> next-hop-ip 2 149.49.200.2
```

next-server

Use the **next-server** command to specify the IP address of the next server in the boot process of a DHCP client. Use the **no** form of this command to clear the next server IP address.

Syntax

[no] next-server *ip-address*

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The IP address of the next server in the boot process of a DHCP client	IP address	**0.0.0.0**

User level

read-write

Context

dhcp pool

Example

To set 1.1.1.1 as the IP address of the next server in the boot process of a DHCP client:

```
G350-001(DHCP 5)# next-server 1.1.1.1
```

To clear the next server IP address:

```
G350-001(DHCP 5)# no next-server
```

nrzi-encoding

Use the **`nrzi-encoding`** command to enable the non-return-to-zero inverted (NRZI) line coding format on the specified interface. Use the **no** form of the command to disable NRZI encoding.

Syntax

`[no] nrzi-encoding`

User level

read-write

Context

Interface: Serial (USP FR L2, USP PPP L2, USP PPP L2-L3)

nvram initialize

Use the **nvram initialize** command to reset the NVRAM parameters to the factory default values. This command is an alias for **erase startup-config** (refer to erase startup-config on page 140).

Syntax

nvram initialize

User level

read-write

Context

general

Example

To reset the configuration parameters for the device:

```
G350-001# nvram initialize
This command will restore factory defaults, and can disconnect your
telnet session
*** Reset *** - do you want to continue (Y/N)? Y
Connection closed by foreign host.
```

option

Use the **option** command to create a DHCP general option or to enter the context of a DHCP general option. Use the **no** form of this command to clear a DHCP general option.

Syntax

[no] option ***option-num***

Parameters

Parameter	Description	Possible Values	Default Value
option-num	The index of the DHCP option	**1-255** The following are exceptions: options configurable with specific commands and options that are part of the DHCP protocol, which are: 0, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 255.	

User level

read-write

Context

dhcp pool

Example

To enter the context for option 42:

```
G350-001(DHCP 5)# option 42
G350-001(DHCP 5/option 42)#
```

owner

Use the **owner** command to specify the owner of the current list.

Syntax

owner ***owner_name***

Parameters

Parameter	Description	Possible Values	Default Value
owner_name	Name of the owner	string	

User level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list, ip crypto-list

Example

To set the owner of access control list 330 as “MGAdmin3”:

```
G350-001(ACL 330)# owner MGAdmin3
```

passive-interface

Use the **`passive-interface`** command to suppress OSPF routing updates on the interface.

Syntax

`passive-interface {interface_name | net_address}`

Parameters

Parameter	Description	Possible Values	Default Value
`interface_name`	Name of the interface on which to suppress routing updates		
`net_address`	IP address of the interface on which to suppress routing updates		

User level

read-write

Context

router ospf

Example

To suppress OSPF routing updates on the Fast Ethernet interface:

```
G350-001(router:ospf)# passive-interface FastEthernet 10/2.1
```

To suppress OSPF routing updates on the interface at IP address 192.168.1.1:

```
G350-001(router:ospf)# passive-interface 192.168.1.1
```

ping

Use the **`ping`** command to send ICMP packets to a target system. The ping command is useful for checking host reachability and network connectivity.

Syntax

`ping` ***`host`*** **`[`*****`interval`*** **`[`*****`size`*****`[`*****`timeout`*****`[`*****`source_address`*****`]]]]`**

Parameters

Parameter	Description	Possible Values	Default Value
`host`	The IP address of the target system		
`interval`	The number of seconds between successive ICMP packets	**1-256**	**1**
`size`	The size, in bytes, of the packet sent when pinging	**22-65500**	**50**
`timeout`	The timeout in seconds	**1-10**	
`source_address`	IP address from which to send the ICMP packets		

User level

read-only

Context

general

Example

To send test 50-byte packets to IP address 192.168.49.1 from IP address 192.168.49.4 every three seconds, timing out after five seconds:

```
G350-001> ping 192.168.49.1 3 50 5 192.168.49.4
```

pmi

Use the **pmi** command to define this interface as the Primary Management Interface for the system.

Syntax

pmi

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L3, DS1 FR-SUB L2-L3, DS1 FR-SUB L3, USP PPP L3, USP PPP L2-L3), FastEthernet (L2-L3, L3), VLAN (L2-L3, L3), Loopback (L2-L3, L3), Tunnel (L2-L3, L3)

Example

To define the VLAN 1 interface as the Primary Management Interface:

```
G350-001# interface vlan 1
G350-001(if:Vlan 1)# pmi
```

ppp authentication

Use the **ppp authentication** command to select the authentication method used when closing a PPP server or client session.

Note:

> The value set for **ppp authentication**, affects both the USB-modem and the Console interface, simultaneously.

Syntax

ppp authentication {pap|chap|none}

Parameters

Parameter	Description	Possible Values	Default Value
pap	Keyword indicating the Password Authentication Protocol. An unencrypted password is sent for authentication. This is the default.		
chap	Keyword indicating the Challenge Handshake Authentication Protocol. An encrypted password is sent for authentication		
none	Keyword indicating that no password is sent		

User level

read-write

Context

Interface: Console, USB-modem

Example

To select the CHAP authentication protocol:

```
G350-001(if:CON)# ppp authentication chap
```

ppp chap hostname

Use the **ppp chap hostname** command to override the device hostname for PPP CHAP authentication.

Syntax

ppp chap hostname *string*

no ppp chap hostname

Parameters

Parameter	Description	Possible Values	Default Value
string	The username assigned by the broadband internet service provider		no

User level

Read-write

Context

Interface: Fast Ethernet

Example

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

ppp chap password

Use the **ppp chap password** command to set the CHAP password for authentication with a remote peer.

Note:

Executing the **copy running-config startup-config** command stores the configured CHAP password to the NVRAM and not to the ’startup-config’ file.

Note:

This command sets the CHAP secret for cases where the device is a CHAP responder, and the console port **ppp chap-secret** command sets the CHAP secret for cases where the device is a CHAP initiator.

Syntax

ppp chap password ***secret***

Parameters

Parameter	Description	Possible Values	Default Value
secret	The CHAP password.		

User level

Read-write

Context

Interface: Fast Ethernet

Example

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

ppp chap refuse

Use the **`ppp chap refuse`** command to prevent authentication with CHAP, even when a chap secret is configured.

Syntax

`ppp chap refuse`

`no ppp chap refuse`

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(super-if:FastEthernet 10/2)# ppp chap refuse
```

ppp chap-secret

Use the **`ppp chap-secret`** command to configure the shared secret used in PPP sessions with CHAP authentication.

Note:

> The value set for **`ppp chap-secret`** affects both the USB-modem and the Console interface, simultaneously.

Syntax

`ppp chap-secret` ***`chap_secret`***

Parameters

Parameter	Description	Possible Values	Default Value
chap_secret	The shared secret string	4-32 chars	

User level

admin

Context

Interface: Console, USB-modem

Example

To set the shared secret to “mypwd3”:

```
G350-001(super-if:CON)# ppp chap-secret mypwd3
PPP shared secret for CHAP authentication is set
```

ppp pap refuse

Use the **ppp pap refuse** command to prevent authentication with PAP, even when a pap-sent password is configured.

Syntax

ppp pap refuse

no ppp pap refuse

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(super-if:FastEthernet 10/2)# ppp pap refuse
```

ppp pap-sent username

Use the **ppp pap-sent username** command to set the Password Authentication Protocol (PAP) password for authentication with the remote peer.

Note:

Executing the **copy running-config startup-config** command stores the configured username/password to the NVRAM and not to the ’startup-config’ file.

Syntax

ppp pap-sent username <*username*> password <*password*>

no ppp pap-sent username

Parameters

Parameter	Description	Possible Values	Default Value
username	The remote peer PAP username		
password	The remote peer PAP password		

User level

Read-write

Context

Interface: Fast Ethernet

Example

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

ppp timeout ncp

Use the **ppp timeout ncp** command to set the maximum time, in seconds, that PPP allows for negotiation of a network layer protocol. If no network protocol is negotiated within the given time, the connection is terminated. Use the **no** form of the command to disable the timeout feature.

Syntax

```
[no] ppp timeout ncp seconds
```

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The time in seconds that PPP allows for negotiation of a network layer protocol	**1-65535**	

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2-L3, USP PPP L2)

Example

To specify that PPP will allow 60 seconds for negotiation of a network protocol:

```
G350-001# ppp timeout ncp 60
```

ppp timeout retry

Use the **ppp timeout retry** command to set the maximum time to wait for a response during PPP negotiation. Use the **no** form of the command to restore the timeout value to its default.

Syntax

```
[no] ppp timeout retry seconds
```

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The authentication timeout in seconds	**1-255**	2

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2-L3, USP PPP L2)

Example

To specify that PPP will wait up to 30 seconds for a response during negotiation:

```
G350-001# ppp timeout retry seconds
```

pppoe-client persistent delay

Use the **`pppoe-client persistent delay`** command to configure the interval between pppoe-client dial attempts.

Syntax

`pppoe-client persistent delay <`*`seconds`*`>`

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The time in seconds to wait.	**5-10000**	30

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(super-if:FastEthernet 10/2)# pppoe-client persistent delay 1
```

pppoe-client persistent max-attempts

Use the **`pppoe-client persistent max-attempts`** command to limit the number of consecutive connection establishment retires. When the number is reached, the PPPoE client stops trying to establish connections. To restart the connection attempts, use the **`shutdown`** and **`no shutdown`** command sequence.

Syntax

`pppoe-client persistent max-attempts` ***`number`***

`no pppoe-client persistent max-attempts`

Parameters

Parameter	Description	Possible Values	Default Value
`number`	The number of attempts.	**0-10000**	**0** (no limit)

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(super-if:FastEthernet 10/2)# pppoe-client persistent
max-attempts 0
```

pppoe-client service-name

Use the **`pppoe-client service-name`** command to set the PPPoE Client service-name. You can use the **`pppoe-client service-name`** command to force the PPPoE client to connect only to access concentrators that support a specific service-name. If not set, the PPPoE client attempts to automatically discover the service name by initiating PADI frames with a blank service name.

Syntax

`pppoe-client service-name` ***`string`***

`no pppoe-client service-name` ***`string`***

Parameters

Parameter	Description	Possible Values	Default Value
`string`	The service name.		

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(super-if:FastEthernet 10/2)# pppoe-client service-name isp1
```

pppoe-client wait-for-ipcp

Use the **`pppoe-client wait-for-ipcp`** command to configure the amount of time between PPPoE tunnel establishment and IPCP tunnel establishment. The PPPoE client terminates the PPPoE tunnel if this time is exceeded.

Note:

> The PPP stack has a somewhat similar command: **`ppp timeout ncp`**. However while this command only terminates the LCP, the **`pppoe-client wait-for-ipcp`** command terminates the PPPoE tunnel.

Syntax

`pppoe-client wait-for-ipcp` ***`seconds`***

`no pppoe-client wait-for-ipcp` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The number of seconds to wait.	**5-10000**	**20**

User level

Read-write

Context

Interface: Fast Ethernet

Example

```
G350-001(super-if:FastEthernet 10/2)# pppoe-client wait-for-ipcp 30
```

pre-classification

Use the **`pre-classification`** command to specify which priority tag the current QoS list uses for data flows. Use the **no** form of the command to reset the QoS list to use the default priority tag, **trust-cos-dscp**.

Syntax

```
pre-classification tag_type
no pre-classification
```

Parameters

Parameter	Description	Possible Values	Default Value
tag_type	The type of priority tag used with data flows	**untrusted,** **trust-cos,** **trust-dscp,** **trust-cos-dscp**	

User level

read-write

Context

ip qos-list

Example

To specify that the current QoS list uses the dscp priority tag:

```
G350-001(QoS 440)# pre-classification trust-dscp
```

pre-shared-key

Use the **`pre-shared-key`** CLI command to configure the IKE pre-shared key. Use the **no** form of the command to delete the IKE pre-shared key.

Tip:

You can use the command **`crypto isakmp suggest-key`** **`on page 116`** to generate a key.

Syntax

[no] pre-shared-key *key*

Parameters

Parameter	Description	Possible Values	Default Value
key	The pre-shared key	1-127 characters.	32 chars

User level

read-write

Context

crypto isakmp peer

Example

```
G350-001(config-peer:149.49.70.1)# pre-shared-key GNpi1odGNBrB5z4GJLzI56jDmRWAGFES
Done!
```

priority-queue

{TBD}

protect crypto map

Use the **protect crypto map** command to protect traffic that matches this rule, by applying the IPSec processing configured by the specific crypto map.

Use the **no protect** command to specify that traffic matching this IP rule should not be protected. Traffic that matches this rule bypasses IPSec processing, and continues unprotected.

Note:

> You cannot enable or disable crypto map protection when the crypto-list is active. You must first deactivate the list using the **no ip crypto-group** command in the context of the interface on which the crypto-list is activated.

Syntax

`protect crypto map` ***`crypto-map-id`***

`no protect`

Parameters

Parameter	Description	Possible Values	Default Value
`crypto-map-id`	The ID of the crypto map	**1-50**	

User level

read-write

Context

crypto map/ip-rule

Examples

```
G350-001(crypto 901/ip rule 21)# protect crypto map 5
Done!
```

```
G350-001(crypto 901/ip rule 22)# no protect
Done!
```

queue-limit

Use the **`queue-limit`** command to set the packet size of the various queues. Use the **no** form of the command to restore the packet size to its default value, using the interface bandwidth.

Note:

The **`queue-limit`** command is not applicable in fair-voip-queue mode.

Syntax

`queue-limit` ***`queue_id size`***

`no queue-limit`

Parameters

Parameter	Description	Possible Values	Default Value
queue_id	The queue priority ID	**1** (highest) - **4** (lowest)	
size	The size of the queue, in packets	The total number of packets in all queues cannot exceed 5000.	

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP PPP L2-L3, USP PPP L2), FastEthernet(L2-L3, L2)

Example

To specify a size of 200 for queue 1:

```
G350-001(if:Serial 2/1:1)# queue-limit 1 200
```

redistribute

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.

Syntax

```
[no] redistribute protocol
```

Parameters

Parameter	Description	Possible Values	Default Value
protocol	The protocol to be used	**static, connected, rip**	

User level

read-write

Context

Router: ospf

Example

To redistribute static routing information into OSPF:

```
G350-001(router:ospf)# redistribute static
```

redistribute

Use the **redistribute** command to redistribute routing information from another protocol into RIP. Use the **no** form of this command to restore the default value, disable redistribution by RIP.

Syntax

[no] redistribute *protocol*

Parameters

Parameter	Description	Possible Values	Default Value
protocol	The protocol to be used	**static, OSPF**	

User level

read-write

Context

Router-RIP

Example

To redistribute OSPF routing information into RIP:

```
G350-001(router:rip)# redistribute ospf
```

release voip-dsp

Use the **`release voip-dsp`** command to end a BTR test on the VoIP engine. See also: busyout voip-dsp on page 48, test voip-dsp on page 549.

Note:

Status changes that occur during the test create SNMP traps.

Note:

View the results of the most recent BTR test with the **`show mm`** command (refer to show mm on page 461).

Syntax

```
release voip-dsp
```

User level

read-write

Context

general

remote

Use the **`remote`** command to reset the far end counters on a T1 line.

Syntax

`remote` ***`fdl_request_type`***

Parameters

Parameter	Description	Possible Values	Default Value
`fdl_request_type`	The type of counters to reset	reset-performance-monitoring-counters, reset-errored-esf-data	

User level

read-write

Context

Interface: Controller (T1)

Example

To reset performance monitoring counters:

```
G350-001(controller:5/1)# remote reset-performance-monitoring-counters
```

reset

Use the **`reset`** command to reset a specified system resource. The command performs a hard reset of the specified entity, returning any selectable parameters to their startup configuration values and setting all hardware and firmware to a known state.

Note:

If the Supervisor modules are in Active/Standby configuration, resetting the active supervisor causes the standby supervisor to take over and become active.

Note:

The reset command does not work while the configuration is being saved.

Syntax

`reset [module` ***`module_number`*** **`| voip | chassis]`**

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Keyword indicating to reset a module		
`module_number`	The module to reset		
`voip`	Keyword indicating to reset the VoIP engine		
`chassis`	Keyword indicating to reset the G350 and all its media modules		

User level

read-write

Context

general

Example

To reset the VoIP engine:

```
G350-001# reset voip
This command will perform a hard reset.
Do you want to continue (Y/N)? y
```

retstatus

Use the **`retstatus`** command to show whether or not the last CLI command you performed was successful.

Syntax

`retstatus`

User level

read-only

Context

general

Example

To display the status of the most recently executed command:

```
G350-001> retstatus
Succeeded
G350-001> retstatus
Failed
```

rmon alarm

Use the **`rmon alarm`** command to create an RMON alarm entry. Use the **no** form of this command to destroy a specific RMON alarm.

Note:

> The ***`rising_event`*** and ***`falling_event`*** events must be defined before using the **`rmon alarm`** command (refer to rmon event on page 272).

Syntax

```
rmon alarm alarm_num variable interval sample_type
 rising-threshold rising_threshold_value rising_event
 falling-threshold falling_threshold_value falling_event
 startup_alarm owner
```

```
no rmon alarm alarm_num
```

Parameters

Parameter	Description	Possible Values	Default Value
alarm_num	The index number of this alarm		
variable	The OID of the statistic to monitor		
interval	The number of seconds		
sample_type	The type of sample used for the alarm	**absolute, delta**	
rising_ threshold_ value	The value above which the rising_event will be triggered		
rising_ event	The event index to trigger when rising_threshold_value is exceeded		
falling_ threshold_ value	The value below which the falling_event will be triggered		
falling_ event	The event index to trigger when falling_threshold_value is reached		
startup_ alarm	The prerequisite condition for triggering the alarm for the first time	rising, falling, risingOrFalling	
owner	The username of the alarm owner		

User level

read-write

Context

general

Example

To create 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
```

rmon event

Use the **rmon event** command to create an RMON event entry. The RMON event can then be triggered as part of an RMON alarm. To create an RMON alarm, refer to rmon alarm on page 270. Use the **no** form of this command to delete a specific RMON event entity.

Syntax

rmon event *event_num event_type* description *description* owner *owner*

no rmon event *event_num*

Parameters

Parameter	Description	Possible Values	Default Value
event_num	The index number of the event		
event_type	The type of event	**log, trap, logAndTrap, none**	
description	The event description		
owner	The username of the event owner		

User level

read-write

Context

general

Example

To create an RMON event entry:

```
G350-001# rmon event 32 trap description resetTrap owner config
```

```
event 32 was created successfully
```

rmon history

Use the **`rmon history`** command to create an RMON history entry. Use the **`no`** form of this command to delete an existing history entry.

Syntax

```
rmon history history_index module/port interval interval
 buckets buckets owner owner
```

```
no rmon history history_index
```

Parameters

Parameter	Description	Possible Values	Default Value
history_index	The index of the history item		
module	The module number		
port	The port on the specified module		
interval	The bucket interval for the history item		
buckets	The number of time intervals over which to save history data		
owner	The username of the history item owner		

User level

read-write

Context

general

Example

To create an RMON history entry:

```
G350-001# rmon history 32 10/2 interval 20 buckets 100 owner config
history index 32 was created successfully
```

router 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, and disable OSPF globally.

Syntax

```
[no] router ospf
```

User level

read-write

Context

general

router rip

Use the **`router rip`** command to enable the RIP and to enter the **`router configuration`** context. Use the **no** form of this command to restore the default value, and disable RIP.

Syntax

```
[no] router rip
```

User level

read-write

Context

general

router vrrp

Use the **`router vrrp`** command to enable VRRP routing globally. Use the **no** form of this command to disable VRRP routing.

Note:

You cannot activate both VRRP and SRRP protocols at the same time.

Syntax

`[no] router vrrp`

User level

read-write

Context

general

rtp-stat clear

Use the **`rtp-stat clear`** command to reset the RTP statistics application. When you reset the application, all counters are reset and the RTP statistics history is erased.

Syntax

`rtp-stat clear`

User level

read-write

Context

General

Example

```
G350-001# rtp-stat clear
```

rtp-stat event-threshold

Use the **`rtp-stat event-threshold`** command to set thresholds on the QoS event counters incremented by the RTP statistics application. If one or more event threshold is exceeded during an RTP stream and the RTP statistics application is configured to generate QoS SNMP traps, a trap is generated upon termination of the RTP stream. Use the **`rtp-stat qos-trap`** command to configure the RTP statistics application to automatically generate QoS traps. Use the **`rtp-stat threshold`** command to configure the QoS metric thresholds. Event thresholds should be configured such that the sending of a trap corresponds to a customer's actual experience of QoS problems during the stream.

Syntax

```
rtp-stat event-threshold
   {all|codec-loss|codec-rtt|echo-return-loss|loss|remote-loss|rtt|
   jitter|remote-jitter|ssrc-change} num
```

```
no rtp-stat event-threshold
   {all|codec-loss|codec-rtt|echo-return-loss|loss|remote-loss|rtt|
   jitter|remote-jitter|ssrc-change}
```

Parameters

Parameter	Description	Possible Values	Default Value
`all`	Sets all event thresholds to the specified number		
`codec-loss`	Sets the event threshold for the codec-loss metric		
`codec-rtt`	Sets the event threshold for the codec-rtt metric		
`echo-return-loss`	Sets the event threshold for the echo-return-loss metric		
`loss`	Sets the event threshold for the loss metric		
`remote-loss`	Sets the event threshold for the remote-loss metric		
`rtt`	Sets the event threshold for the rtt metric		
`jitter`	Sets the event threshold for the jitter metric		
`remote-jitter`	Sets the event threshold for the remote-jitter metric		
`ssrc-change`	Sets the event threshold for the ssrc-change metric		
num	The number of events		

User level

read-write

Context

General

Example

To set rtp-stat event-thresholds:

```
G350-001(super)# rtp-stat event-threshold echo-return-loss 2
Done!
```

rtp-stat fault

Use the **`rtp-stat fault`** command to configure the RTP statistics application to send QoS fault and/or clear traps. A QoS fault trap is sent when a specified number of active RTP sessions have QoS indicators over the configured thresholds. A QoS clear trap is sent after a QoS fault trap when the number of active RTP sessions with QoS indicators over the configured thresholds reduces to a specified number.

Syntax

`rtp-stat fault [`*`fault`*` [`*`clear`*`]]`

`[no] rtp-stat fault`

Parameters

Parameter	Description	Possible Values	Default Value
`fault`	A minimum number of sessions suffering bad QoS to trigger the QoS fault condition	**1-100**	
`clear`	A maximum number of sessions that suffer from bad QoS to clear the QOS fault condition	**0-99**	

User level

read-write

Context

General

Example

To set fault/clear trap boundary:

```
G350-001(super)# rtp-stat fault 1 0


The fault trap boundary was set to 1 (default: 3)
The clear trap boundary was set to 0}
```

rtp-stat min-stat-win

Use the **`rtp-stat min-stat-win`** command to set the minimum statistic window for the RTP statistics application. That is, the minimum number of observed RTP sequence increments for which the application evaluates packet loss. Use the **no** form of this command to reset the minimum statistic window.

The G350 VoIP engine evaluates the current received packet loss in fixed intervals of 6 to 12 seconds. The G350 VoIP engine postpones loss estimation to the next interval if the number of received packets is less than the minimum statistic window.

Syntax

`[no] rtp-stat min-stat-win` ***`packets`***

Parameters

Parameter	Description	Possible Values	Default Value
`packets`	The minimum number of observed RTP sequence increments for which the application evaluates packet loss	**10-1000**	

User Level

read-write

Example

To set the minimum statistic window to 50:

```
G350-001# rtp-stat min-stat-win 50
```

rtp-stat qos-trap

Use the **`rtp-stat qos-trap`** command to configure the RTP Statistics application to automatically send a QoS trap upon the termination of an RTP stream in which one or more QoS event counters exceeded their configured thresholds. The traps are sent by an SNMP agent to the SNMP trap manager on the CM server. They are converted to syslog messages and stored in the messages file on the CM server hard disk. Use the **no** form of this command to disable RTP statistic QoS traps.

Syntax

```
[no] rtp-stat qos-trap
```

User Level

read-write

Context

General

Example

To enable the RTP statistic QoS trap:

```
G350-001#  rtp-stat qos-trap
The RTP statistics QoS trap is enabled
```

To disable the RTP statistic QoS trap:

```
G350-001# no rtp-stat qos-trap
The RTP statistics QoS trap is disabled.
```

rtp-stat qos-trap-rate-limit

Use the **`rtp-stat qos-trap-rate-limit`** command to configure the QoS trap rate limiter. The trap rate limiter limits the rate at which QoS traps are sent to the SNMP trap manager on the media server. The trap rate limiter uses a token bucket scheme, in which the maximum number of QoS traps that can be sent is stored as a number of tokens in a virtual bucket. The number increments by one at a specified interval and is limited to a maximum by a specified bucket size.

Syntax

```
rtp-stat qos-trap-rate-limit token-interval bucket-size
```

Parameters

Parameter	Description	Possible Values	Default Value
token-interval	The interval, in hundredths of seconds, between additions of a token to the bucket.	**10-100000**	**1000**
bucket-size	The maximum number of tokens stored in the bucket.	**1-1000**	**5**

User Level

read-write

Context

General

rtp-stat service

Use the **rtp-stat service** command to enable the RTP statistic application. Use the **no** form of this command to disable the RTP statistic application. By default, the RTP statistic application is disabled.

Syntax

```
[no] rtp-stat-service
```

User Level

Admin

Example

To enable the RTP statistic application:

```
G350-001 (super)# rtp-stat-service
The RTP statistics service is enabled.
```

To disable the RTP statistic application:

```
G350-001 (super)# no rtp-stat-service
The RTP statistics service is disabled.
```

rtp-stat threshold

Use the **`rtp-stat threshold`** command to set thresholds for QoS metrics sampled by the RTP statistics application. For each threshold, a counter increments every time the metric exceeds the threshold during the RTP stream. Thresholds are also configured on the event counters, using the **`rtp-stat event-threshold`** command.

Syntax

```
rtp-stat threshold
   {codec-loss|average-codec-loss|loss|average-loss|remote-loss|
   average-remote-loss} percentage
```

```
rtp-stat threshold {codec-rtt|rtt|jitter|remote-jitter} milliseconds
```

```
rtp-stat threshold echo-return-loss dbm
```

```
no rtp-stat threshold
   {all|codec-loss|average-codec-loss|codec-rtt|
   echo-return-loss|loss|average-loss|remote-loss|
   average-remote-loss|rtt|jitter|remote-loss|echo-return-loss}
```

Parameters

Parameter	Description	Possible Values	Default Value
`codec-loss`	The percentage of time the codec plays fill frames due to lack of valid RTP frames		
`average-codec-loss`	The average codec loss sampled during the RTP stream		
`loss`	The percentage of RTP packets lost in the network. The G350 VoIP engine evaluates the current received packet loss in fixed intervals of 6 to 12 seconds. The G350 VoIP engine postpones loss estimation until the next interval if the number of packets received is less than the minimum statistic window. The minimum statistic window is configured with the **`rtp-stat min-stat-win`** command.		
			1 of 2

Parameter	Description	Possible Values	Default Value
`average-loss`	The average packet loss sampled during the RTP stream		
`remote-loss`	The percentage of RTP packets lost in the network as experienced by the remote RTP receiver. The local RTP receiver learns about its remote peer statistics from RTCP packets		
`average-remote-loss`	The average network loss experienced by the remote RTP receiver sampled during the RTP stream		
`percentage`		**0.0-100.0**	
`codec-rtt`	The last estimation of the codec Round Trip Time (in milliseconds). Round Trip Time is the time taken for a message to get to the remote peer and back to the local receiver. In order to reflect the round-trip-delay experienced by the user, this metric includes the internal delay (including jitter buffer delay, codec delay, and packetization delay) inside the G350 and the IP phone and an estimation of the remote internal delay.		
`rtt`	The network RTT. This metric does not include internal delay.		
`jitter`	Variation in delay of packet delivery to the local peer		
`remote-jitter`	Variation in delay of packet delivery to the remote peer		
`milliseconds`		**0-5000**	
`echo-return-loss`	The echo cancellation loss on the TDM bus		
`db`		**0-100**	
`all`	Clears all configured thresholds		
			2 of 2

User Level

read-write

Context

General

Example

To set rtp-stat thresholds:

```
G350-001(super)# rtp-stat threshold echo-return-loss 5
Done!
```

sat

Use the **sat** command to provide a shortcut method to access the System Access Terminal (SAT) so that Avaya Communication Manager translation work can be performed. See the description for session on page 284 for more information. The Media Server must configure the SAT port to 5023.

Syntax

```
sat
```

User level

read-only

Context

general

server-name

Use the **server-name** command to specify the optional server name in the boot process of a DHCP client. Use the **no** form of this command to clear the optional server name.

Syntax

[no] server-name ***server-name***

Parameters

Parameter	Description	Possible Values	Default Value
server-name	A name for the optional server, enclosed in quotes	string, **1-64** bytes	null string

User level

read-write

Context

dhcp pool

Example

To set the optional server name to “avaya”:

```
G350-001(DHCP 5)# server-name "avaya"
```

To clear the optional server name:

```
G350-001(DHCP 5)# no server-name
```

session

Use the **session** command to provide the means to establish a session with the active Media Gateway Controller, SAT, or the device. Specifying **session mgc** takes the user to the LINUX shell login. Specifying **session icc** accesses the S8300. Adding the **sat** parameter takes the user to the SAT login.

This is an alias to Telnet. The **mgc** option Telnets to the active Media Gateway Controller.

Note:

> Note: for **session mgc sat**, and **session icc sat** to access the Media Server SAT terminal, the SAT port must be configured to 5023 on the Media Server. For **session mgc** and **session icc**, the Media Server should allow access to the Telnet port (23).

Syntax

session {mgc [sat] | icc [sat]}

User level

read-only

Context

general

Example

To establish a session with the active Media Gateway Controller:

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

set boot bank

Use the **set boot bank** command to set the system boot bank for the active Supervisor Module.

Syntax

set boot bank ***value***

Parameters

Parameter	Description	Possible Values	Default Value
value	Boot bank name	**bank-a** - set the boot bank to A **bank-b** - set the boot bank to B	

User level

read-write

Context

general

Example

To specify that the media gateway boots from boot bank A:

```
G350-001# set boot bank bank-A
boot bank set to bank-A
```

set contact-closure admin

Use the **`set contact-closure admin`** command to specify how the contact closure relay is controlled.

Note:

The **`set contact-closure pulse-duration`** command does not affect the **`set contact-closure admin manual`** command.

Syntax

```
set contact-closure admin module/port:relay
 {mgc | manual-trigger | manual-off}
```

Parameters

Parameter	Description	Possible Values	Default Value
module	Module number of the contact closure port	**10**	
port	Port number of the contact closure port	**1**	
relay	Contact closure relay	**1,2**	
mgc	Contact closure is controlled by the call controller		
manual-trigger	Contact closure relay is triggered		
manual-off	Contact closure relay is not triggered		

User level

read-write

Context

general

Example

To specify that contact closure for relay 2 of port 1 on module 10 is controlled by the call controller:

```
G350-001# set contact-closure admin 10/1:2 mgc
```

set contact-closure pulse-duration

Use the **`set contact-closure pulse-duration`** command to set the pulse duration for a contact closure relay. Pulse duration is the amount of time for the relay to return to normal after the call controller triggers it.

Syntax

```
set contact-closure pulse-duration module/port:relay time
```

Parameters

Parameter	Description	Possible Values	Default Value
module	Module number of the contact closure port	**10**	
port	Port number of the contact closure port	**1**	
relay	Relay number	**1,2**	
time	Amount of time until the relay returns to normal, in seconds	**1 – 60**	

User level

read-write

Context

general

Example

To set the pulse duration to 3 seconds for relay 2 of port 1 on module 10:

```
G350-001# set contact-closure pulse-duration 10/1:2 3
```

set dot1x max-req

Use the **`set dot1x max-req`** command to set the maximum number of times the port tries to retransmit requests to the Authenticated Station before the session is terminated.

Note:

Time period settings affect all external ports.

Syntax

```
set dot1x max-req count
```

Parameters

Parameter	Description	Possible Values	Default Value
count	Number of attempts	**1-10**	**2**

User Level

admin

Context

general

Example

```
G350-001# set dot1x max-req 5
```

set dot1x quiet-period

Use the **set dot1x quiet-period** command to set the minimal time between authentication attempts.

Note:

Time period settings affect all external ports.

Syntax

```
set dot1x quiet-period seconds
```

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds.	**0-65535**	**60**

User Level

admin

Example

```
G350-001# set dot1x quiet-period 45
```

set dot1x re-authperiod

Use the **`set dot1x re-authperiod`** command to set the idle time between re-authentication attempts.

Note:

Time period settings affect all external ports.

Syntax

`set dot1x re-authperiod` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds	**0-65535**	**3600**

User Level

admin

Context

general

Example

```
G350-001# set dot1x re-authperiod 7200
```

set dot1x server-timeout

Use the **`set dot1x server-timeout`** command to set the server retransmission timeout period for all ports. This is the maximum time that the port will wait for a reply from the Authentication Server.

Note:

Timeout settings affect all external ports.

Syntax

set dot1x server-timeout *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds	**0-65535**	**30**

User Level

admin

Context

general

Example

```
G350-001# set dot1x server-timeout 15
```

set dot1x supp-timeout

Use the **set dot1x supp-timeout** command to set the maximum time that the switch will wait for a reply from the Authenticated Station before the session is terminated.

Note:

Timeout settings affect all external ports.

Syntax

set dot1x supp-timeout *seconds*

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds	**0-65535**	**30**

User Level

admin

Context

general

Example

```
G350-001# set dot1x supp-timeout 15
```

set dot1x system-auth-control disable

Use the **`set dot1x system-auth-control disable`** command to globally disable the PBNAC (802.1x) feature.

Syntax

`set dot1x system-auth-control disable`

User Level

admin

Context

general

Example

```
G350-001# set dot1x system-auth-control disable
```

set dot1x system-auth-control enable

Use the **`set dot1x system-auth-control enable`** command to globally enable the PBNAC (802.1x) feature.

Syntax

`set dot1x system-auth-control enable`

User Level

admin

Context

general

Example

```
G350-001# set dot1x system-auth-control enable
```

set dot1x tx-period

Use the **`set dot1x tx-period`** command to set the time interval between attempts to access the Authenticated Station.

Note:

Time period settings affect all external ports.

Syntax

`set dot1x tx-period` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	Number of seconds.	0 to 65535	30

User Level

admin

Context

general

Example

```
G350-001 (super)# set dot1x tx-period 15
```

set dscp

Use the **`set dscp`** command to set the DSCP value in the tunneled packet. Use the **no** form of this command to take the DSCP value from the original header (default setting).

Syntax

`[no] set dscp` ***`dscp-value`***

Parameters

Parameter	Description	Possible Values	Default Value
dscp-value	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.	**0-63**	

User level

read-write

Context

crypto map

Examples

```
G350-001(config-crypto:1)# set dscp 10
Done!

G350-001(config-crypto:1)# no set dscp
Done!
```

set etr

Use the **set etr** command to enable or disable Emergency Transfer Relay (ETR) mode, or to allow the gateway to control ETR mode automatically.

Note:

In ETR mode, the TRK and LINE 1 ports are connected. All other telephone ports stop operating.

Note:

If a call is in progress when the communications problem ends, the gateway does not turn off ETR mode automatically. If you specify **manual-off**, the call terminates.

Syntax

set etr *module* {auto | manual-on | manual-off}

Parameters

Parameter	Description	Possible Values	Default Value
module	Module number	**1-7**	
auto	Allow the gateway to control ETR mode automatically		
manual-on	Set ETR mode to on		
manual-off	Set ETR mode to off		

User level

read-write

Context

general

Example

To specify that the gateway will control ETR mode automatically on module 7:

```
G350-001# set etr 7 auto
```

set icc-monitoring

Use the **set icc-monitoring** command to control heartbeat monitoring of an Inter Carrier Cable (ICC) or Local Survivable Processor (LSP).

Syntax

set icc-monitoring {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enable heartbeat monitoring		
disable	Disable heartbeat monitoring		

User level

read-write

Context

general

set logging file

Use the **`set logging file`** command to manage the logging of system messages to non-volatile memory (NVRAM).

Syntax

`set logging file {enable | disable | condition {all`|***`MsgFacility`***}{**none**|***`severity`***}}

Parameters

Parameter	Description	Possible Values	Default Value
`enable`	Enable logging to the file sink		
`disable`	Disable logging to the file sink		
`condition`	Define a filter rule for logging		
`all`	Apply the filter condition to all MsgFacilities		
`MsgFacility`	Apply the filter condition to a specific MsgFacility	**boot, system, router, config, temp, filesys, fan, supply, security, cascade, qos, switchfabric, lag, vlan, rip, ldap, snmp**	
			1 of 2

Parameter	Description	Possible Values	Default Value
none	Do not log messages to the file sink		
severity	Only log messages whose severity level is equal to or more severe than the specified level. 0 is the highest severity and 7 the lowest severity.	Use the text value or its numeric equivalent: **emergency (0),** **alert (1),** **critical (2),** **error (3),** **warning (4),** **notification (5),** **informational (6),** **debugging (7)**	
			2 of 2

User level

read-write

Context

general

Example

To filter VLAN messages sending only those having a severity of critical or greater:

```
G350-001# set logging file condition vlan critical
```

set logging server access-level

Use the **`set logging server access-level`** command to define the access level associated with a Syslog server sink. You cannot specify an admission level higher than the assigned level.

Syntax

`set logging server access-level` ***`admission_level`*** **`{`*`ip_address`*` | `*`hostname`*`}`**

Parameters

Parameter	Description	Possible Values	Default Value
admission_ level		**read-only, read-write, admin**	
ip_address	The IP address of the Syslog server		
hostname	The name of the Syslog server host		

User level

read-write

Context

general

Example

To specify a read-write access level for the Syslog server at IP address 172.5.16.33:

```
G350-011# set logging server access-level read-write 172.5.16.33
```

set logging server

Use the **set logging server** command to define a new Syslog output server for remote logging of system messages. A maximum of three Syslog servers can be configured. A new Syslog server is created in disabled mode.

Syntax

set logging server *ip_address*

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the Syslog server		

User level

read-write

Context

general

Example

To define a Syslog server at IP address 147.2.3.66:

```
G350-001# set logging server 147.2.3.66
```

set logging server condition

Use the **`set logging server condition`** command to specify a filter for messages sent to the specified Syslog server. Messages can be filtered by source system, severity, or both.

Syntax

`set logging server condition {all | `*`Msgfacility`*`} {none | `*`severity`*`}` ***`ip_address`***

Parameters

Parameter	Description	Possible Values	Default Value
`all`	Apply this filter to all message facility systems		
`MsgFacility`	Apply this filter to messages produced by a specific system	**boot, system, router, config, temp, filesys, fan, supply, security, cascade, qos, switchfabric, lag, vlan, ospf, rip, ldap, snmp**	
none	Do not log any messages		
`severity`	Only log messages whose severity level is equal to or more severe than the specified level (0 is the highest severity, 7 the lowest)	Use the text value or its numeric equivalent: **emergency (0),** **alert (1),** **critical (2),** **error (3),** **warning (4),** **notification (5),** **informational (6),** **debugging (7)**	
`ip_address`	The IP address of the Syslog server		

User level

read-write

Context

general

Example

To filter fan messages for the Syslog server at IP address 168.23.1.15, so that only fan messages of warning-level severity or greater are sent:

```
G350-001# set logging server condition fan warning 168.23.1.15
```

set logging server facility

Use the **`set logging server facility`** command to define an output facility for the specified Syslog server.

Syntax

```
set logging server facility facility ip_address
```

Parameters

Parameter	Description	Possible Values	Default Value
facility	The facility used in Syslog reports	**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)	
ip_address	The IP address of the Syslog server		

User level

read-write

Context

general

Example

To specify that messages for the specified Syslog server be sent to the mail output facility:

```
G350-001# set logging server facility mail 168.12.1.15
```

set logging server enable/disable

Use the **`set logging server enable/disable`** command to enable or disable a specific Syslog server.

Syntax

`set logging server {enable | disable}` ***`ip_address`***

Parameters

Parameter	Description	Possible Values	Default Value
`enable`	Enable logging for the Syslog server		
`disable`	Disable logging for the Syslog server		
`ip_address`	The IP address of the Syslog server		

User level

read-write

Context

general

Example

To enable logging for the Syslog server at IP address 168.12.1.13:

```
G350-001# set logging server enable 168.12.1.13
```

set logging session

Use the **`set logging session`** command to manage message logging for the current console session.

Syntax

```
set logging session {enable | disable | condition {all | MsgFacility}
{none | severity}}
```

Parameters

Parameter	Description	Possible Values	Default Value
`enable`	Enable logging to the console session		
`disable`	Disable logging to the console session		
`condition`	Define a filter rule for logging		
`all`	Apply the filter condition to all MsgFacilities		
`MsgFacility`	Apply the filter condition to a specific MsgFacility	**boot, system, router, config, temp, filesys, fan, supply, security, cascade, qos, switchfabric, lag, vlan, rip, ldap, snmp, isakmp, ipsec**	
none	Do not log messages to the console session		
`severity`	Only log messages whose severity level is equal to or more severe than the specified level (0 is the highest severity, 7 the lowest)	Use the text value or its numeric equivalent: **emergency (0),** **alert (1),** **critical (2),** **error (3),** **warning (4),** **notification (5),** **informational (6),** **debugging (7)**	**6**

User level

read-write

Context

general

Example

To filter config messages for the session, sending only those config messages of alert severity or greater:

```
G350-001# set logging session condition config alert
```

set logout

Use the **`set logout`** command to set the number of minutes until the system automatically disconnects an idle session.

Syntax

`set logout [`*`timeout`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`timeout`	Number of minutes until the system automatically disconnects an idle session. Setting the value to 0 disables the automatic disconnection of idle sessions.	**0-99**	**15**

User level

read-write

Context

general

Example

To set the system to disconnect idle sessions automatically after 20 minutes:

```
G350-001# set logout 20
```

To disable the automatic disconnection of idle sessions:

```
G350-001# set logout 0
```

set mediaserver

Use the **`set mediaserver`** command to set media server management ports.

Syntax

```
set mediaserver ip_address1 ip_address2 port name
```

Parameters

Parameter	Description	Possible Values	Default Value
ip_address1	Controller IP address used for registration		
ip_address2	Management interface IP address		
port	Service port number		
name	Service type	**telnet, sat**	

User level

read-write

Context

general

Example

To set media server management sat port 3023 to have a controller IP address of 135.6.8.99 and a management IP address of 135.34.54.2:

```
G350-563# set mediaserver 135.6.8.99 135.34.54.2 3023 sat
```

set mgc list

Use the **`set mgc list`** command to permit the creation of a list of valid Media Gateway Controller(s). The user can configure up to four IP addresses separated by commas.

Note:

The **`set mgc list`** command appends the new controllers to the existing list of controllers, if any.

Syntax

`set mgc list {`*`ipaddress1`*`,…}`

Parameters

Parameter	Description	Possible Values	Default Value
ipaddress1	The IP address of the call controller		

User level

read-write

Context

general

Example

To specify two Media Gateway Controllers at IP addresses 132.236.73.2 and 119.52.3.27:

```
G350-001# set mgc list 132.236.73.2, 119.52.3.27
```

set peer

Use the **`set peer`** command to attach a peer to a crypto map. Use the **no** form of the command to remove a peer from the crypto map.

Note:

You can only change the peer of a crypto map when the map is inactive.

Syntax

`set peer {`*`ip-address`*`}`

`no set peer`

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The remote peer IP address		

User level

read-write

Context

crypto map

Examples

```
G350-001(config-crypto:1)# set peer 149.49.52.135
Done!
```

set pfs

Use the **set pfs** command to specify 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.

Use the **no** form of the command to disable PFS for IKE phase 2 (default setting).

Syntax

```
[no] set pfs [group1 | group 2]
```

Note:

Using **set pfs** with no parameters sets the pfs group to 1.

Parameters

Parameter	Description	Possible Values	Default Value
group1	Specifies that IKE employs the 768-bit Diffie-Hellman prime modulus group		
group 2	Specifies that IKE employs the 1,024-bit Diffie-Hellman prime modulus group		

User level

read-write

Context

crypto ipsec transform-set

Example

```
G350-001(config-transform:ts1)# set pfs group1
Done!
```

set port auto-negotiation-flowcontrol-advertisement

Use the **`set port auto-negotiation-flowcontrol-advertisement`** command to set the flowcontrol advertisement for the specified port when performing autonegotiation.

Syntax

`set port auto-negotiation-flowcontrol-advertisement` ***`module/port`***
`{no-flowcontrol|asym-tx-only|sym-only|sym-and-asym-rx}`

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
`no-flowcontrol`	The port will advertise no pause capabilities.		
`asym-tx-only`	The port will advertise asymmetric Tx pause capabilities only.		
`sym-only`	The port will advertise symmetric pause capabilities only.		
`sym-and-asym-rx`	The port will advertise both symmetric and asymmetric Rx pause capabilities.		

User level

read-write

Context

general

Example

To specify that port 5 of module 2 will advertise asymmetric Tx pause capabilities only:

```
G350-011# set port auto-negotiation-flowcontrol-advertisement 2/5
asym-tx-only
```

```
Port 2/5 pause capabilities was set
```

set port classification

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 media gateway.

Syntax

`set port classification` ***`module/port`*** **`{regular | valuable}`**

Parameters

Parameter	Description	Possible Values	Default Value
`module`	The module number		
`port`	The port number. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
`regular`	Keyword specifying that port classification be set to regular		
`valuable`	Keyword specifying that port classification be set to valuable		

User level

read-write

Context

general

Example

To set the port classification for port 3 of module 5 to valuable:

```
G350-001# set port classification 5/3 valuable
Port 5/3 classification has been changed.
```

set port disable

Use the **set port disable** command to disable a port or range of ports.

Syntax

set port disable *module/port*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-write

Context

general

Example

To disable port 1 on module 4:

```
G350-001# set port disable 4/1
Port 4/1 disabled.
```

set port dot1x initialize

Use the **`set port dot1x initialize`** command to initialize 802.1x on a port.

Syntax

`set port dot1x initialize` ***`mod/port`***

Parameters

Parameter	Description	Possible Values	Default Value
mod/port	Number of the module and port on the module		

User level

admin

Context

general

Example

```
Console> set port dot1x initialize 2/3
dot1x port 4/1 initializing...
dot1x initialized on port 4/1.
```

set port dot1x port-control

Use the **`set port dot1x port-control`** command to set the dot1x parameter per port.

Syntax

```
set port dot1x port-control mod/port {force-authorize |
force-unauthorize | auto}
```

Parameters

Parameter	Description	Possible Values	Default Value
mod/port	Number of the module and port on the module		
force-authorize	The port is always in forwarding state		
force-unauthorize	The port is always in blocking state		
auto	Port blocking depends on authorization outcome		**auto**

User level

admin

Context

general

Example

```
Console> set port dot1x port-control 1/2 auto
Port 4/1 dot1x port-control is set to auto.
```

set port dot1x re-authenticate

Use the **set port dot1x re-authenticate** command to set the port to re-authenticate.

Syntax

set port dot1x re-authenticate *mod/port*

Parameters

Parameter	Description	Possible Values	Default Value
mod/port	Number of the module and port on the module		

User level

admin

Context

general

Example

```
Console> set port dot1x re-authenticate 4/1
dot1x port 4/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 4/1 authorized.
```

set port dot1x re-authentication

Use the **`set port dot1x re-authentication`** command to set the re-authentication mode per port.

Syntax

`set port dot1x re-authentication` ***`mod/port`*** **`{enable | disable}`**

Parameters

Parameter	Description	Possible Values	Default Value
`mod/port`	Number of the module and port on the module		
`enable`	Keyword to enable automatic re-authentication		
`disable`	Keyword to disable automatic re-authentication		**disable**

User level

admin

Context

general

Example

```
Console> set port dot1x re-authentication 1/2 enable
Port 1/2 re-authentication enabled.
```

set port duplex

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. An error message is generated if you try to set the transmission type of auto negotiation Fast Ethernet ports to half-duplex or full-duplex mode.

Syntax

`set port duplex` ***`module/port`*** **`{full|half}`**

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
`full`	Set full-duplex transmission		
`half`	Set half-duplex transmission		

User level

read-write

Context

general

Example

To set port 1 on module 4 to full duplex:

```
G350-001# set port duplex 4/1 full
Port 4/1 set to full-duplex.
```

set port edge admin state

Use the **`set port edge admin state`** command to specify whether or not a port is considered to be an edge port.

Syntax

`set port edge admin state` ***`module/port admin_state`***

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
`admin_state`	The type of the specified port	**edge-port, non-edge-port**	

User level

read-write

Context

general

Example

To specify that port 3 of module 10 is an edge port:

```
G350-011# set port edge admin state 10/3 edge-port
```

set port enable

Use the **`set port enable`** command to enable a port or a range of ports.

Syntax

`set port enable [`*`module/port`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-write

Context

general

Example

To enable port 3 of module 10:

```
G350-147# set port enable 10/3
Port 10/3 enabled.
```

set port flowcontrol

Use the **`set port flowcontrol`** command to set the send/receive mode for flow-control frames (IEEE 802.3x or proprietary) for a full duplex port. Each direction (send or receive) can be configured separately.

Syntax

```
set port flowcontrol {receive | send | all} module/port {off | on |
proprietary}
```

Parameters

Parameter	Description	Possible Values	Default Value
`receive`	Indicates whether the port can receive its administrative status from a remote device. This option is only available for Gigabit Ethernet modules with negotiation set to off.		
`send`	Indicates whether the local port can send its administrative status to a remote device. This option is only available for Gigabit Ethernet modules with negotiation set to off.		
`all`	Send and receive (symmetric flow control) Used with **on** indicates that the local port acts upon and sends flow control frames. Used with **off** indicates that the local port discards and does not send flow control frames.		
`module`	Number of the module		
`port`	Number of the port on the module		
`off`	Used with **receive** to turn off an attached device's ability to send flow-control packets to a local port. Used with **send** to turn off the local port's ability to send administrative status to a remote device.		
`on`	Used with **receive** to specify that a local port receives administrative status from a remote device. Used with **send**, to specify that a local port sends administrative status to a remote device.		
`proprietary`	Used with **all** to indicate that the local port acts on and sends Avaya proprietary flow control frames		

User level

read-write

Context

general

Example

To specify that port 1 receives administrative status from a remote device:

```
G350-147# set port flowcontrol receive 5/1 on
```

```
Port 5/1 flow control receive administration status set to on
(port will require far end to send flowcontrol)
```

To specify that port 1 cannot send administrative status to a remote device:

```
G350-147# set port flowcontrol send 5/1 off
```

```
Port 5/1 flow control send administration status set to off
(port will send flowcontrol to far end)
```

set port level

Use the **set port level** command to set the priority level of a port or range of ports on the switching bus. Packets traveling through a port set at normal priority are served only after packets traveling through a port set at high priority are served.

Syntax

set port level *module/port* [*value*]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
value	Priority level	**0-7**	

User level

read-write

Context

general

Example

To set the priority level of port 1 on module 3 to 5:

```
G350-147# set port level 3/1 5
```

```
Port 3/1 level set to 5
```

set port mirror

Use the **`set port mirror`** command to define a port mirroring source-destination pair. The second port receives a copy of all packets sent to and received by the first port.

Syntax

`set port mirror source-port` ***`module/port`*** **`mirror-port`** ***`module/port`*** **`sampling`** ***`sampling_value`*** **`direction`** ***`direction_value`***

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
sampling_ value	Specifies whether to allow or disable sampling of the transmissions	**always, disable**	
direction_ value	The direction of transmissions to mirror	**rx, tx, both**	

User level

read-write

Context

general

Example

To set up port mirroring from port 3/1 to port 5/1 for all packets sent and received:

```
G350-001# set port mirror source-port 3/1 mirror-port 5/1 sampling
always direction both
```

set port name

Use the **`set port name`** command to configure a name for a port. If you do not specify a name, the port name displays as **NO NAME**.

Syntax

`set port name` ***`module/port`*** **`[`*`name`*`]`**

Parameter

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
`name`	The port name	maximum 16-character string	

User level

read-write

Context

general

Example

To name port 21 of module 4 to “arthur”

```
G350-147# set port name 4/21 arthur

Port 4/21 name set.
```

Note:

If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

set port negotiation

Use the **`set port negotiation`** command to enable or disable auto-negotiation on the specified port. Auto-negotiation uses a link negotiation protocol to determine the highest connection parameters available to connected ports and configures the port speed and duplex setting of both ports. This command applies to Fast Ethernet or Gigabit Ethernet ports.

If negotiation is disabled, the user can set the speed and duplex of the Fast Ethernet ports.

Syntax

```
set port negotiation module/port {enable|disable}
```

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
`enable`	Enable port negotiation protocol		
`disable`	Disable port negotiation protocol		

User level

read-write

Context

general

Example

To disable autonegotiation on port 1, module 4:

```
G350-147# set port negotiation 4/1 disable
```

```
Link negotiation protocol disabled on port 4/1.
```

set port point-to-point admin status

Use the **`set port point-to-point admin status`** command to manage the connection type of the port.

Syntax

`set port point-to-point admin status` ***`module/port admin_status`***

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
`admin_status`	The connection type of the port	**force-true** — specify that the port is connected point-to-point **force-false** — specify that this port is shared media **auto** — try to automatically detect the connection type of the port	

User level

read-write

Context

general

Example

To specify that the connection type of port 2 is automatically detected:

```
G350-001# set port point-to-point admin status 10/2 auto
```

set port powerinline

Use the **`set port powerinline`** command to enable or disable the load detection process on the port. The load detection process is used to power devices using Power over Ethernet (PoE).

Syntax

`set port powerinline` ***`module_number/port_number`*** **`{enable | disable}`**

Parameters

Parameter	Description	Possible Values	Default Value
`module_number`	The module number		
`port_number`	The port number. A range of ports can also be specified. For example, to specify ports 1-3 on module 3, use the syntax 3/1-3.		
`enable`	Enable load detection on this port		
`disable`	Disable load detection on this port		

User level

read-write

Context

general

Example

To enable load detection on ports 3/1, 3/2, and 3/3:

```
G350-001# set port powerinline 3/1-3 enable
```

set port powerinline priority

Use the **`set port powerinline priority`** command to configure the priority level of powering the port.

Note:

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

Syntax

```
set port powerinline priority module_number/port_number priority
```

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number		
port_number	The port number. A range of ports can be specified. For example, to specify ports 1-3 on module 3, use the syntax 3/1-3.		
priority	The priority level of powering the port	**Critical, High, Low**	

User level

read-write

Context

general

Example

To set powering priority to High for ports 3/1, 3/2, and 3/3:

```
G350-001# set port powerinline priority 3/1-3 high
```

set port powerinline type

Use the **set port powerinline type** command to set the type of powered device connected to the PoE port.

Syntax

```
set port powerinline type module/port_number string
```

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module.		
port_number	Number of the port on the module.		
string	A description of the type of powered device connected to this port.		

User level

admin

Context

general

Example

```
Console> set port powerinline type 6/1-3 telephone
```

set port redundancy

Use the **set port redundancy** command to globally enable or disable port redundancy on the device. Using this command does not delete existing redundancy entries.

Syntax

```
set port redundancy {enable|disable}
```

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enable port redundancy on the device		
disable	Disable port redundancy on the device		

User level

read-write

Context

general

Example

To enable port redundancy:

```
G350-147# set port redundancy enable
All redundancy schemes are now enabled
```

set port redundancy on|off

Use the **`set port redundancy on|off`** command to define or remove redundancy pairs. A redundancy port acts as a backup port in case the primary port fails. The port can be any port that does not belong to a LAG or a LAG interface. Ensure that there is **no** redundancy scheme already defined on any of the ports.

Syntax

`set port redundancy` ***`prim_module/prim_port second_module/second_port`***
`{on|off} [`*`redundancy_name`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
prim_module	The module number of the primary port		
prim_port	Primary port of the redundancy scheme		
second_module	The module number of the backup port		
second_port	Backup port of the redundancy scheme		
on	Keyword specifying to define the redundancy pair		
off	Keyword specifying to remove the redundancy pair		
redundancy_name	Name for the redundancy scheme		

User level

read-write

Context

general

Example

To specify that port 12 of module 4 acts as a backup port for port 7 on module 3, and to name the redundancy pair red1:

```
G350-147# set port redundancy 3/7 4/12 on red1
```

```
red1: Port 4/12 is redundant to port 3/7.
Port redundancy is active - entry is effective immediately
```

Note:

If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

set port redundancy-intervals

Use the **set port redundancy-intervals** command to configure the two time constants that determine redundancy switchover parameters.

Syntax

set port redundancy-intervals ***min_time_between_switchovers*** **{*switchback_interval* | none}**

Parameters

Parameter	Description	Possible Values	Default Value
min_time_ between_ switchovers	The minimum time, in milliseconds, between redundancy switchovers for each pair	**0 – 65000**	
switchback_ interval	The period, in milliseconds, the primary port link has to be “up” before the system switches back Specify **0** to indicate the system never switches back Specify **1** to indicate that switchback occurs immediately after the primary port link returns	**0 – 65000**	
none	Do not switch		

User level

read-write

Context

general

Example

To specify a delay of 100 milliseconds before switching to the backup port, and a requirement that the primary port be up for 20 milliseconds before control is returned:

```
G350-147# set port redundancy-intervals 100 20
```

set port spantree

Use the **`set port spantree`** command to enable or disable spanning tree for specific ports.

Syntax

`set port spantree {enable|disable} [`*`module/port`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`enable`	Keyword specifying that spanning tree mode should be enabled		
`disable`	Keyword specifying that spanning tree mode should be disabled		
`module`	The module number		
`port`	The port number		

User level

read-write

Context

general

Example

To enable spanning tree on port 1 of module 3:

```
P480-1# set port spantree enable 3/1
port 3/1 was enabled on spantree
```

set port spantree cost

Use the **`set port spantree cost`** command to set the spanning tree cost of a port. This value defines which port will be allowed to forward traffic if two ports with different costs cause a loop.

Syntax

```
set port spantree cost [module/port] [value]
```

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		
value	Number representing the cost. A lower value specifies precedence of a port to forward traffic.	**1-65535**	

User level

read-write

Context

general

Example

To set the spanning tree cost of port 4/2 to 4096:

```
G350-147# set port spantree cost 4/2 4096
port 4/2 spantree cost is 4096
```

set port spantree force-protocol-migration

Use the **`set port spantree force-protocol-migration`** command to force the port to send a rapid spanning tree hello packet (Bridge Protocol Data Unit).

Syntax

```
set port spantree force-protocol-migration module/port
```

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		

User level

read-write

Context

general

Example

To force port 2 of module 10 to send a hello packet:

```
G350-001# set port spantree force-protocol-migration 10/2
```

set port spantree priority

Use the **`set port spantree priority`** command to set the Spanning Tree priority level of a port. This value defines the priority of a port to be blocked in case two ports with the same cost cause a loop.

Syntax

```
set port spantree priority module/port value
```

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		
value	Number representing the priority of the port. 0 is the highest priority. A port with a lower priority will be blocked.	**0-240** (in multiples of 16)	**128**

User level

read-write

Context

general

Example

To set the priority for port 4 of module 3 to 128:

```
G350-147# set port spantree priority 3/4 128
port 3/4 spantree priority is 128
```

set port speed

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 try to set the speed when auto negotiation is enabled

Syntax

set port speed *module/port* 10MB|100MB|1GB

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
10MB	Keyword that sets the specified port to a speed of 10 Mbps		
100MB	Keyword that sets the specified port to a speed of 100 Mbps		
1GB	Keyword that sets the specified port to a speed of 1 Gbps		

User level

read-write

Context

general

Example

To configure port 1 on module 4 to 100 Mbps

```
G350-147# set port speed 4/1 100MB
Port 4/1 speed set to 100 Mbps.
```

set port static-vlan

Use the **set port static-vlan** command to assign a static VLAN to a port.

Syntax

set port static-vlan *module/port vlan_num*

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port or range of ports which are being bound		
vlan_num	VLAN to bind to the port		

User level

read-write

Context

general

Example

To bind ports 4 through 6 of module 3 to VLAN 2:

```
G350-147# set port static-vlan 3/4-6 2
```

```
VLAN 2 is bound to port 3/4
VLAN 2 is bound to port 3/5
VLAN 2 is bound to port 3/6
```

set port trap

Use the **set port trap** command to enable or disable generic SNMP uplink or downlink traps from a port.

Syntax

set port trap *module/port* {enable|disable}

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
enable	Enable uplink/downlink traps		
disable	Disable uplink/downlink traps		

User level

read-write

Context

general

Example

To enable uplink and downlink traps for port 2 of module 3:

```
G350-147# set port trap 3/2 enable
Port 3/2 up/down trap enabled.
```

set port vlan

Use the **set port vlan** command to set the port VLAN ID (PVID).

Note:

You need to define a VLAN before setting a port VLAN ID.

Syntax

set port vlan *vlan_num module/port*

Parameters

Parameter	Description	Possible Values	Default Value
vlan_num	Number identifying the VLAN		
module	The module number		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-write

Context

general

Example

To set the VLAN ID for port 3/5 to 2:

```
G350-147# set port vlan 2 3/5
VLAN 2 modified.
VLAN Mod/Ports
---- --------------------------
   2 3/5
```

set port vlan-binding-mode

Use the **set port vlan-binding-mode** command to define which VLANs will be bound to the specified port.

Syntax

set port vlan-binding-mode ***module/port_list value***

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port_list	The port to bind to VLANs. A list of ports can be entered using the form **n-m**. For example, specify **5/4-8** to indicate module 5, ports 4 through 8.		
value	The type of VLAN binding	**static** - the port supports only the VLANs that are manually configured for this port **bind-to-configured** - the port supports all the VLANs configured on the device	

User level

read-write

Context

general

Example

To specify that ports 5 through 9 on module 5 will only support the VLANs manually configured for those ports:

```
G350-147# set port vlan-binding-mode 5/5-9 static

Set Port vlan binding method:5/5

Set Port vlan binding method:5/6

Set Port vlan binding method:5/7

Set Port vlan binding method:5/8

Set Port vlan binding method:5/9
```

set powerinline trap disable

Use the **set powerinline trap disable** command to disable PoE trap generation.

Syntax

set port powerinline trap disable *module*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module.		

User level

admin

Example

```
Console> set powerinline trap disable 6
```

set powerinline trap enable

Use the **set powerinline trap enable** command to enable the generation of PoE traps and configure the Usage Threshold value.

Syntax

set port powerinline trap enable *module [threshold]*

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module.		
threshold	(Optional) Power consumption usage for generating traps, in percent.	**1-99**	99

User level

admin

Context

general

Example

```
Console> set powerinline trap enable 6 70
```

set qos bearer

Use the **set qos bearer** command to permit the setting of VoIP QoS-bearer related parameters for the Media Gateway Processor and VoIP engines. Since Media Gateway Controller and VoIP engines share the same setup, local values are not set to entered values unless **set qos control local** has been executed (refer to set qos control on page 337).

Syntax

set qos bearer {bbedscp | efdscp | 802p | rtpmin | rtpmax} ***value***

Parameters

Parameter	Description	Possible Values	Default Value
bbedscp	Keyword specifying that the following value is the BBE differentiated services code point	**0-63**	**43**
efdscp	Keyword specifying that the following value is the EF differentiated services code point	**0-63**	**46**
802p	Keyword specifying that the following value is the 802 priority value	**0-7**	**6**
rtpmin	Keyword specifying that the following value is the RTP port min value. The rtpmin value must be an even number, and the difference between rtpmin and rtpmax must be at least 129.	**2048-65406**	**2048**
rtpmax	Keyword specifying that the following value is the RTP port max value. The rtpmax value must be an odd number and the difference between rtpmax and rtpmin must be at least 129.	**2177-65535**	**65535**
value	A value for the specified keyword		

User level

read-write

Context

general

Example

To set the BBE differentiated services code point to 43:

```
G350-001# set qos bearer bbedscp 43
```

set qos control

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 via the CLI, or **remote** in which case the values are obtained from the Media Gateway Controller. The default value is **remote**.

Syntax

`set qos control {local | remote}`

Parameters

Parameter	Description	Possible Values	Default Value
`local`	Keyword that specifies to configure QoS values via the CLI		
`remote`	Keyword that specifies to obtain QoS values from the media gateway controller		

User level

read-write

Context

general

Example

To specify that QoS values are configured locally via the CLI:

```
G350-001# set qos control local
```

set qos rsvp

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 or disabled, refresh rate in seconds, failure retry yes or no, and service profile, guaranteed-service or controlled load service.

Note:

> The **`set qos rsvp command`** *will not* take effect unless QoS source setup is **local**.

Syntax

```
set qos rsvp {enable | disable} | {refresh secs} | {failure {retry |
noretry}} | {profile {guaranteed | controlled}}
```

Parameters

Parameter	Description	Possible Values	Default Value
`enable`			
`disable`			
`refresh`			
`secs`	The refresh time in seconds	**1-99**	**15**
`retry`			
`noretry`			
`guaranteed`			
`controlled`			

User level

read-write

Context

general

Example

To set the refresh rate to 15 seconds:

```
G350-001# set qos rsvp refresh 15
```

To specify no retry upon failure:

```
G350-001# set qos rsvp failure noretry
```

To specify controlled load service:

```
G350-001# set qos rsvp profile controlled
```

To enable RSVP:

```
G350-001# set qos rsvp enable
```

set qos 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, and defining the listening port number.

Syntax

`set qos rtcp {{enable|disable} | monIP` ***`ip address`*** **`| reportper`** ***`seconds`*** **`| listenport`** ***`portno`*** **`}`**

Parameters

Parameter	Description	Possible Values	Default Value
`enable`	Keyword that specifies to enable RTCP reporting capability		
`disable`	Keyword that specifies to disable RTCP reporting capability		
`ip address`	The IP address of the monitor		
`seconds`	The reporting period in seconds	**5-30**	**5**
`portno`	The listening port number	**1-65535**	**5005**

User level

read-write

Context

general

Example

To set the monitoring IP address to 132.123.23.12:

```
G350-001# set qos rtcp monip 132.123.23.12
```

To set the reporting period to 10 seconds:

```
G350-001# set qos rtcp reportper 10
```

To set the listening port number to 5000:

```
G350-001# set qos rtcp listenport 5000
```

To enable reporting capability:

```
G350-001# set qos rtcp enable
```

set qos signal

Use the **`set qos signal`** command to provide the means to set up QoS signaling parameters, DSCP or 802.1Q, for the Media Gateway Processor.

Syntax

`set qos signal {dscp | 802p}` ***`value`***

Parameters

Parameter	Description	Possible Values	Default Value
`dscp`	Keyword that specifies to setup DSCP parameters		
`802p`	Keyword that specifies to setup 802.1Q parameters		
`value`	Parameter value	For dscp: **0-63** For 802p**: 0-7**	For dscp: **34** For 802p: **7**

User level

read-write

Context

general

Example

To set up DSCP parameter 43:

```
G350-001# set qos signal dscp 43
```

set radius authentication

Use the **`set radius authentication`** command to enable or disable RADIUS authentication.

Syntax

```
set radius authentication {enable | disable}
```

Parameters

Parameter	Description	Possible Values	Default Value
`enable`	Keyword specifying to enable RADIUS authentication		
`disable`	Keyword specifying to disable RADIUS authentication (default)		

User level

read-write

Context

general

Example

To enable RADIUS authentication:

```
G350-001# set radius authentication enable
```

set radius authentication retry-number

Use the **`set radius authentication retry-number`** command to set the number of times to resend an access request when there is **no** response.

Syntax

`set radius authentication retry-number` ***`number`***

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of times to resend an access request if there is no response	**1–65535**	

User level

read-write

Context

general

Example

To set the number of retries for RADIUS authentication to 3:

```
G350-147# set radius authentication retry-number 3
```

set radius authentication retry-time

Use the **`set radius authentication retry-time`** command to set the time to wait before resending an access request.

Syntax

`set radius authentication retry-time` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The time in seconds to wait before resending an access request	**1–65535**	

User level

read-write

Context

general

Example

To specify to wait 5 seconds before retrying an access request:

```
G350-147# set radius authentication retry-time 5
```

set radius authentication secret

Use the **`set radius authentication secret`** command to enable secret authentication.

Syntax

`set radius authentication secret` ***`string`***

Parameters

Parameter	Description	Possible Values	Default Value
`string`	The text password		

User level

admin

Context

general

Example

To set the RADIUS authentication password to **hush**:

```
G350-147# set radius authentication secret hush
```

set radius authentication server

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

Syntax

`set radius authentication server` ***`ip_addr`*** **`{primary | secondary}`**

Parameters

Parameter	Description	Possible Values	Default Value
ip_addr	IP address of RADIUS authentication server		
primary	Keyword that specifies to set the primary authentication server (default)		
secondary	Keyword that specifies to set the secondary authentication server		

User level

read-write

Context

general

Example

To set the primary RADIUS authentication server IP address to be 192.40.12.36:

```
G350-147# set radius authentication server 192.40.12.36 primary
```

set radius authentication udp-port

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.

Syntax

`set radius authentication udp-port` ***`number`***

Parameters

Parameter	Description	Possible Values	Default Value
number	The UDP port number		**1812**

User level

read-write

Context

general

Example

To set the UDP port number to 1645:

```
G350-147# set radius authentication udp-port number 1645
```

set reset-times

Use the **`set reset-times`** command to set reset times.

Syntax

```
set reset-times { {total-search | primary-search} minutes |
transition-point value }
```

Parameters

Parameter	Description	Possible Values	Default Value
`total-search`	Set the total search timer		
`primary-search`	Set the primary search timer		
`minutes`	Number of minutes	**1–60**	total-search: **30** primary-search: **1**
`transition-point`	Set the entry point		
`value`		**1–4**	1

User level

read-write

Context

general

Example

To set the primary search timer to 20 minutes:

```
G350-011# set reset-times primary-search 20
```

set security-association lifetime

Use the **`set security-association lifetime`** command to set the IKE phase 2 (IPSec) SA (security-association) lifetime. Use the **no** form of the command to disable the SA lifetime.

Syntax

`[no] set security-association lifetime { seconds` ***`seconds`*** **`| kilobytes {`*****`kilobytes`*****` | disable} }`**

Parameters

Parameter	Description	Possible Values	Default Value
`seconds`	Specify the lifetime in seconds		
`seconds`	The lifetime, in seconds	**120-86,400**	
`kilobytes`	Specify the lifetime by the amount of traffic that should pass through the IPSec tunnel before the security association should time out.		
`kilobytes`	The amount of traffic, in kilobytes	**2,560-536,870,912**	
`disable`	Unlimited lifetime		

User level

read-write

Context

crypto ipsec transform-set

Example

```
G350-001(config-transform:ts1)# set security-association lifetime
seconds 300
```

```
Done!
```

set snmp community

Use the **`set snmp community`** command to set or modify the media gateway's SNMP community strings.

Syntax

`set snmp community read-only | read-write | trap [`*`community_string`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`read-only`	Keyword specifying the read-only access level		
`read-write`	Keyword specifying the read-write access level		
`trap`	Keyword specifying an snmp trap		
`community_string`	Specifies the name of the SNMP community. If no community string is specified, the community string configured for that access type is cleared.		

User level

read-write

Context

general

Example

To set the read-only community string to 'read':

```
G350-001# set snmp community read-only read
SNMP read-only community string set
```

set snmp retries

Use the **`set snmp retries`** command to set the number of times to attempt to communicate with a particular node.

Syntax

```
set snmp retries number
```

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of retry attempts to make	**1 – 100000**	

User level

read-write

Context

general

Example

To set the system to make 100 retry attempts:

```
G350-001# set snmp retries 100
```

set snmp timeout

Use the **set snmp timeout** command to specify the time to wait for a response before retrying the communication.

Syntax

```
set snmp timeout time
```

Parameters

Parameter	Description	Possible Values	Default Value
time	The number of seconds to wait	**1 – 100000**	

User level

read-write

Context

general

Example

To set the system to wait 60 seconds before retrying communications:

```
G350-001# set snmp timeout 60
```

set snmp trap

Use the **`set snmp trap`** command to define an SNMPv1 trap receiver, or configure its settings.

Syntax

```
set snmp trap receiver {enable|disable} [categorylist]
```

Parameters

Parameter	Description	Possible Values	Default Value
`receiver`	The IP address of the trap receiver		
`enable`	Keyword specifying that the trap receiver is enabled		
`disable`	Keyword specifying that the trap receiver is disabled (this is the default		
			1 of 2

Parameter	Description	Possible Values	Default Value
`category list`	List of trap categories to be enabled or disabled for the specified trap receiver.	All— all traps affected by enable/disable config fault, trafic_treshold, module_De-Enrollment, module_Enrollment, delete_SW_redundancy_entry, create_SW_redundancy_entry, temperature_warninggeneral_threshold, cam_change, duplicate_ip, ip_vlan_violation, link_aggregation_connection_fault, link_aggregation_connection_return,link_aggregation_partial_fault, link_aggregation_partial_return,delete_lagcreate_new_lag, active_policy_list_change, policy_access_control_violation,BUPS_module_fault, BUPS_module_fault_return, BUPS_fans_module_fault, BUPS_fans_module_fault_return, fans_module_fault, fans_module_fault_returncascade_up_connection_fault, cascade_up_connection_fault_return,cascade_down_connection_fault_return, cascade_down_connection_fault	
			2 of 2

User level

admin

Context

general

set spantree default-path-cost

Use the **`set spantree default-path-cost`** command to set the version of the spanning tree default path cost used by this bridge.

Syntax

```
set spantree default-path-cost pathcost
```

Parameters

Parameter	Description	Possible Values	Default Value
pathcost	The version of the spanning tree default path cost	**common-spanning-tree** - compatible with IEEE802.1D standard **rapid-spanning-tree** - compatible with IEEE802.1W standard	

User level

read-write

Context

general

Example

To use the rapid-spanning-tree default path cost:

```
G350-011# set spantree default-path-cost rapid-spanning-tree
Spanning tree default path costs is set to rapid spanning tree.
```

set spantree enable/disable

Use the **set spantree** command to enable or disable the spanning-tree algorithm for the media gateway.

Note:

> When you disable spanning tree, blocking ports are disabled in order to prevent loops in the network. As a result, you need to wait 30 seconds before disabling spanning tree if you reset the media gateway, enable spanning tree, or insert a new station.

Syntax

```
set spantree {enable|disable}
```

Parameters

Parameter	Description	Possible Values	Default Value
`enable`	Keyword specifying to enable the spanning-tree algorithm		
`disable`	Keyword specifying to disable the spanning-tree algorithm		

User level

read-write

Context

general

Example

To enable spanning tree:

```
G350-147# set spantree enable
bridge spanning tree enabled.
```

To disable spanning tree:

```
G350-147# set spantree disable
bridge spanning tree disabled.
```

set spantree forward-delay

Use the **`set spantree forward-delay`** command to specify the time used when transferring the state of a port to the forwarding state.

Syntax

`set spantree forward-delay` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The value must exceed (Bridge Max Age / 2). The recommended value is **15**	**4-30**	

User level

read-write

Context

general

Example

To specify a forward delay of 25 seconds:

```
G350-001# set spantree forward-delay 25
bridge forward delay is set to 25.
```

set spantree hello-time

Use the **`set spantree hello-time`** command to specify the time interval between the generation of configuration BPDU’s by the root.

Syntax

`set spantree hello-time` ***`seconds`***

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The value must not exceed (Bridge Max Age / 2) - 1. The recommended value is **2**	**1-10**	

User level

read-write

Context

general

Example

To specify spanning tree hello time is 2 seconds:

```
G350-401# set spantree hello-time 2
bridge hello time is set to 2.
```

set spantree max-age

Use the **`set spantree max-age`** command to specify the time to keep an information message before it is discarded.

Syntax

```
set spantree hello-time seconds
```

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The value must be between 2 * (Bridge-hello-time + 1) and 2 * (Bridge-forward-delay - 1). The recommended value is **20**	**6-40**	

User level

read-write

Context

general

Example

To keep information messages for 20 seconds before discarding:

```
G350-011# set spantree max-age 20
bridge max age is set to 20.
```

set spantree priority

Use the **`set spantree priority`** command to set the bridge priority for the spanning tree.

Syntax

```
set spantree priority bridge_priority
```

Parameters

Parameter	Description	Possible Values	Default Value
bridge_ priority	The number representing the priority of the bridge	**0** (high) **- 65535** (low) in increments of 4096	

User level

read-write

Context

general

Example

To set the bridge priority to 4096:

```
G350-001# set spantree priority 4096
Bridge priority set to 4096.
```

set spantree tx-hold-count

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 BPDU’s transmitted during a hello-time period.

Syntax

```
set spantree tx-hold-count rate
```

Parameters

Parameter	Description	Possible Values	Default Value
rate	Recommended value is **3**	**1-10**	

User level

read-write

Context

general

Example

To limit the number of hello packets to 2:

```
G350-011# set spantree tx-hold-count 2
tx hold count is set to 2.
```

set spantree version

Use the **`set spantree version`** command to set the version of the spanning tree protocol used by the device.

Syntax

`set spantree version` ***`version`***

Parameters

Parameter	Description	Possible Values	Default Value
version	Version of the spanning tree protocol	**common-spanning-tree** — compatible with IEEE802.1D standard **rapid-spanning-tree** — compatible with IEEE802.1W standard	

User level

read-write

Context

general

Example

To use the rapid-spanning-tree version of spanning tree:

```
G350-101# set spantree version rapid-spanning-tree
Spanning tree version is set to rapid spanning tree.
```

set sync interface

Use the **`set sync interface`** command to define the specified module and port as a potential source for clock synchronization for the media gateway.

Syntax

`set sync interface {primary | secondary}` ***`mmID`*** **`[`*`portID`*`]`**

Parameters

Parameter	Description	Possible Values	Default Value
`primary`	Keyword that specifies normal failover		
`secondary`	Keyword that specifies to override normal failover, generate a trap, and assert a fault		
`mmID`	The Media Module ID number of a stratum clock source, of the form “vn” where “n” is the slot number		
`portID`	Port or port range for an ISDN clock source candidate		

User level

read-write

Context

general

Example

To specify that ports 1, 3, 5, 6, 7, and 8 of Media Module 2 are used for normal failover:

```
G350-001# set sync interface primary v2 1,3,5-8
```

set sync source

Use the **`set sync source`** command to specify which clock source is the active clock source. The identity of the current synchronization source is not stored in persistent storage.

Syntax

`set sync source {primary | secondary | local}`

Parameters

Parameter	Description	Possible Values	Default Value
`primary`	Keyword specifying to set the primary clock source to be active		
`secondary`	Keyword specifying to set the secondary clock source to be active, and the primary clock source on standby		
`local`	Keyword specifying to set the local clock to be active		

User level

read-write

Context

general

Example

To set the primary clock as the clock source:

```
G350-001# set sync source primary
```

If the secondary interface is not configured, the sync source set operation will fail.

```
G350-001# set sync source secondary
Operation Failed
Cannot set the secondary clock source to be the active clock source
```

set sync switching

Use the **set sync switching** command to toggle automatic sync source switching.

Syntax

set sync switching {enable | disable}

Parameters

Parameter	Description	Possible Values	Default Value
enable	Enable automatic sync source switching		
disable	Disable automatic sync source switching		

User level

read-write

Context

general

Example

To enable sync source switching:

```
G350-001# set sync switching enable
```

set system contact

Use the **set system contact** command to set the contact information for this media gateway system.

Syntax

set system contact [*string*]

Parameters

Parameter	Description	Possible Values	Default Value
string	The contact name string should be typed inside double quotes. The name is cleared if you leave this field blank.		

User level

read-write

Context

general

Example

To set the descriptive contact of the system to “Larry Williams”

```
G350-147# set system contact “Larry Williams”
*** Set system contact ***
system contact set
```

set system location

Use the **set system location** command to set the location information for this media gateway system.

Syntax

```
set system location [string]
```

Parameters

Parameter	Description	Possible Values	Default Value
string	The location name string should be typed inside double quotes. The location is cleared if you leave this field blank.		

User level

read-write

Context

general

Example

To set the descriptive location of the system to “tech-support”:

```
G350-147# set system location “tech-support”
*** Set system location ***
system location set
```

set system name

Use the **`set system name`** command to specify the name of this media gateway system.

Syntax

`set system name [`*`string`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
string	The system name string should be typed inside quotes. The name is cleared if you leave this field blank.		

User level

read-write

Context

general

Examples

To set the descriptive name of the system to “G350-HQ”:

```
G350-001# set system name “G350-HQ”
*** Set system name ***
system name set
```

set terminal recovery password

Use the **`set terminal recovery password`** command to enable or disable the recovery password.

Note:

This command can only be issued via the console port (not via a modem port).

Syntax

`set terminal recovery password` ***`action`***

Parameters

Parameter	Description	Possible Values	Default Value
action	The state of the recovery password	**enable, disable**	

User level

admin

Context

general

Example

To disable the recovery password:

```
G350-001(super)# set terminal recovery password disable
```

set transform-set

A crypto map object points to a single transform-set object, which contains the parameters required for IKE Phase 2 negotiation.

Use the **`set transform-set`** command to configure the transform-set. Use the **no** form of the command to remove the transform-set from the crypto map.

Note:

You cannot remove a transform-set from a crypto map that is being used by an active crypto-list. You must first de-activate the crypto-list, using the **no** form of the **`ip crypto-group`** command. See ip crypto-group on page 171.

Syntax

```
[no] set transform-set name
```

Parameters

Parameter	Description	Possible Values	Default Value
name	The name of the transfer set	1-32 characters	

User level

read-write

Context

crypto map

Example

```
G350-001(config-crypto:10)# set transform-set ts1
Done!
```

set trunk

Use the **set trunk** command to configure the VLAN tagging mode of a port.

Syntax

```
set trunk module/port {off|dot1q}
```

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		
			1 of 2

Parameter	Description	Possible Values	Default Value
`off`	Keyword that specifies to force the port to become a non-tagging port and persuade the neighboring port to become a non-tagging port. The port becomes a non-tagging port even if the neighbor port does not agree to become a non-tagging port.		
`dot1q`	Keyword that specifies IEEE 802.1q tagging on a Fast Ethernet or Gigabit Ethernet port		
			2 of 2

User level

read-write

Context

general

Example

To configure 802.1q VLAN tagging for port 3 of module 3:

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

set utilization cpu

Use the **`set utilization cpu`** command to enable CPU utilization measurements.

Syntax

`set utilization cpu` ***`module`***

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		

User level

read-write

Context

general

Example

To enable CPU utilization measurements on module 10:

```
G350-100# set utilization cpu 10
CPU utilization is set on module 10
```

set vlan

Use the **set vlan** command to create or modify a VLAN.

Syntax

set vlan *vlan_id* [name *vlan_name*]

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	The VLAN number	**1 – 3071**	
name	Keyword that allows naming or renaming the VLAN		
vlan_name	The VLAN name	string from 1 – 32 characters	

User level

read-write

Context

general

Example

To create VLAN number 3, named “gregory”:

```
G350-147# set vlan 3 name gregory
VLAN id 3, vlan-name gregory created.
```

Note:

If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

set web aux-files-url

Use the **`set web aux-files-url`** command to specify the URL of the Web server containing the online help files and Java plug-in.

Syntax

`set web aux-files-url` ***`url`***

Parameters

Parameter	Description	Possible Values	Default Value
`url`	The IP address and directory name of the Web server		

User level

read-write

Context

general

Example

To set the URL of the Web server to 176.2.3.66/DMweb:

```
G350-001# set web aux-files-url http://176.2.3.66/DMweb
```

show application-memory

Use the **`show application-memory`** CLI command to show the configured and allocated application memory.

Syntax

`show application-memory`

User level

Read only

Context

general

Example

```
interface# > show application-memory
Application                                      Memory(KB)
                                          Allocated  Configured
----------------------------------------  ---------------------
Sniffer (capture buffer-size)                   1024       1024
TFTP (ip tftp-server file-system-size)         18560      18560
----------------------------------------  ---------------------
Total used memory                              19584      19584
Total free memory                                896        896
Total memory (fixed)                           20480
```

show banner login

Use the **`show banner login`** command to display the banner that is displayed before the login prompt.

Syntax

`show banner login`

User level

admin

Context

general

Example

To display the banner that will be displayed before the login prompt:

```
G350-001(super)# show banner login
```

```
Welcome to G350 Media Gateway
```

```
FW version 0.11.0
```

show banner post-login

Use the **show banner post-login** command to display the banner displayed after a user logs in successfully.

Syntax

show banner post-login

User level

admin

Context

general

Example

To display the banner that will be shown after a successful login:

```
G350-001(super)# show banner post-login
```

```
*** Welcome to the G350 Media Gateway CLI Interface ***
For questions, please refer to the CLI Reference Guide
```

show boot bank

Use the **show boot bank** command to display the software bank from which the device boots at the next boot process.

Syntax

show boot bank

User level

read-only

Context

general

Example

To display the bank from which booting currently takes place:

```
G350-001> show boot bank
Boot bank set to bank-a
```

show cam

Use the **show cam** command to display the CAM table entries for a specific module and port. If **no** module or port is specified, the system displays all CAM table entries.

Note:

MACs associated with LAGs appear under the LAG ID, not under the LAG port.

Syntax

show cam [*module*[/*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module		

User level

read-only

Context

general

Example

```
G350-001> show cam 3/33

Total Matching CAM Entries Displayed = 128

Dest MAC/Route Dest vlan Destination Ports
------------------- ---- -----------------
08:00:20:c6:98:5f    1     3/33
08:00:20:c4:c8:51    1     3/33
00:00:5e:00:01:02    1     3/33
00:01:02:de:96:2f    1     3/33
00:02:2d:47:18:67    1     3/33
00:02:2d:48:18:29    1     3/33
00:04:0d:01:b0:00    1     3/33
...
```

show cam mac

Use the **show cam mac** command to display a specific mac entry in the CAM table for a specific VLAN or for all VLANs.

Syntax

show cam mac *mac_address* [*vlan_number*]

Parameters

Parameter	Description	Possible Values	Default Value
mac_address	The MAC entry to display		
vlan_number	The VLAN to display		

User level

read-only

Context

general

Example

To display all entries in VLAN 1 that match the MAC address 00:40:c2:00:66:b0:

```
G350-001> show cam mac 00:40:c2:00:66:b0 1
```

show cam vlan

Use the **`show cam vlan`** command to display all MAC entries in the CAM table for a specific VLAN.

Syntax

```
show cam vlan vlan_number
```

Parameters

Parameter	Description	Possible Values	Default Value
vlan_number	VLAN for which to display the CAM table		

User level

read-only

Context

general

show capture

Use the **`show capture`** command to display information about the currently configured settings for the packet sniffing service.

Note:

Timestamps in the capture file are based on the capture start time that is displayed in the output of the show capture command.

Syntax

```
show capture
```

User level

read-only

Context

general

Example

```
G350-001>show capture
The sniffing service is enabled
Capturing started at:
21:22:01, February 21, 2003 / 7,9:55:55 (uptime)
stopped at: not-stopped
Buffer size: 1000 KB
Buffer mode is cyclic
Maximum number of bytes captured from
each frame: 128
Packet filter: Capture List 503
Number of frames in buffer: 200
Size of capture file: 50 KB (5%)
```

show capture-buffer hex

Use the **`show capture-buffer hex`** command to display the contents of the packet sniffing buffer as a hex dump.

Syntax

`show capture-buffer hex [frame_id]`

Parameters

Parameter	Description	Possible Values	Default Value
`frame_id`	The ID of the first packet to display in the output		

User level

read-only

Context

general

Example

```
G350-001> show capture-buffer hex 5
Frame number: 5
Frame time: 01/01/1970-23:45:09.10001
Time relative to first frame: 0, 0:0:3.021141
Frame Length: 68 bytes (0x44)
Capture Length: 68 bytes (0x44)

00000: d4c3 b2a1 0200 0400 0000 0000 0000 0000 ................
00010: ffff 0000 0100 0000 348c 913e e5df 0e00 ........4..>....
00020: 2800 0000 2800 0000 2053 454e 4401 2053 (...(... SEND. S
00030: 454e 4401 c021 0100 001a 0506 0b87 16c2 END..!..........
00040: 0d03 0611 ....

Frame number: 6
Frame time: 01/01/1970-23:45:09.100012
Time relative to first frame: 0, 0:0:3.021142
Frame Length: 256 bytes (0x44)
Capture Length: 128 bytes (0x80)

0000000: d4c3 b2a1 0200 0400 0000 0000 0000 0000 ................
0000010: ffff 0000 0100 0000 ea71 8e3e e6ed 0b00 .........q.>....
0000020: e300 0000 e300 0000 ffff ffff ffff 0010 ................
0000030: a498 97ab 0800 4500 00d5 3a7d 0000 8011 ......E...:}....
0000040: ea9a 0a00 0002 0a00 00ff 008a 008a 00c1 ................

--type q to quit or space key to continue--
```

Note:

The right side of the hex dump is the octets converted to characters using ascii code. Octets smaller than 32 or greater than 126 are displayed as a dot (.).

show composite-operation

Use the **show composite-operation** command to display information about a specific composite-operation. Use the command without a parameter to display information about all composite-operations.

Syntax

show composite-operation [*composite_operation_index*]

Parameters

Parameter	Description	Possible Values	Default Value
composite_operation_ index	The composite-operation to display	**0 – 19**	

User level

read-write

Context

ip access-control-list, ip access-control-list ip-rule, ip qos-list, ip qos-list ip-rule, ip qos-list composite-operation

Example

To display information about composite-operation 13:

```
G350-001(QoS 440)# show composite-operation 13
```

```
Index Name                 CoS       DSCP      Trust
----- -------------------- --------- --------- ------------
13    HSPackets            cos3      1         No
```

show contact-closure

Use the **show contact-closure** command to view the status of a contact closure relay. If no relay is specified, the status of all relays is displayed.

Syntax

show contact-closure [module/port:*relay*]

Parameters

Parameter	Description	Possible Values	Default Value
module/port	Contact closure module/port to display	**7/20**	
relay	Relay number	**1,2**	

User level

read-only

Context

general

Example

To display information about all contact closure relays:

```
G350-001> show contact-closure
Module port relay admin           pulse-duration   status
------ ---- ----- --------------- ---------------  ------
7       20    1   call-controller 3 seconds        triggered
7       20    2   manual           toggle           off
```

To display information about contact closure relay 2:

```
G350-001> show contact-closure 7/20:2
Module port relay admin           pulse-duration   status
------ ---- ----- --------------- ---------------  ------
7       20    2   manual           toggle           off
```

show controllers

Use the **`show controllers`** command to display status information about a controller interface.

Syntax

`show controllers` ***`module/port`***

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		

User level

read-write

Context

general

Example

To display controller status information:

```
G350-001# show controllers
```

```
T1 5/1 is down.
Cablelength is long gain26 0db.
Transmitter is sending remote alarm.
Receiver has loss of signal.
Framing is SF, Line Code is AMI, Clock Source is Line.
Data in current interval (802 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 802 Unavail
Secs
Total Data (last 4 15 minute intervals):
10 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 3600 Unavail
Secs
```

show controllers remote

Use the **`show controllers remote`** command to display controller statistics from a peer station. If the Facility Data Link (FDL) for this controller is set to **att**, the system displays the status (up or down) of the line. Otherwise, the system displays statistics for the controller. To set the Facility Data Link, refer to fdl on page 142.

Syntax

`show controllers remote` ***`module/port fdl_data_type`***

Parameters

Parameter	Description	Possible Values	Default Value
`module`	The module number		
			1 of 2

Parameter	Description	Possible Values	Default Value
port	The port number		
fdl_data_type	The type of statistics to display	**1h-data, errored-esf-data, enhanced-1h, enhanced-c1-configuration**	
			2 of 2

User level

read-write

Context

general

Example

To display 1h-data statistics for the T1 controller on port 1 of module 5:

```
G350-001# show controllers remote 5/1 1h-data
```

show copy status

Use the **show copy status** command to display the status of the **copy running-config startup-config** operation.

Syntax

```
show copy status
```

User level

read-write

Context

general

Example

To display the status of the current copy operation:

```
G350-001# show copy status
```

```
Module #10
===========
Module           : 10
Source file      : startup-config
Destination file : running-config
Host             : -
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

show crypto ipsec sa

Use the **show crypto ipsec sa** command to display the IPSec SA database status.

Syntax

show crypto ipsec sa [list *crypto-list-id* [rule *rule-id*] | address] [detail]

Parameters

Parameter	Description	Possible Values	Default Value
list			
crypto-list-id	The crypto-list whose SA configuration should be displayed		
rule			
rule-id	The ip-rule in the crypto-list whose SA configuration should be displayed		
address	Show SA configuration by peer IP address		
detail	Display detailed output		

User level

read-only

Context

general

Example

```
G350-001> show crypto ipsec sa detail

Inbound pkts errors (global):
  Invalid spi                 0
  Invalid interface           0

interface: Serial 5/1
           FastEthernet 10/1 (down)
  Crypto list id: 910, Local address: 1.0.0.1

   Rule: 15, Crypto map: 5, "Lincroft VPN"
     Local address: 1.0.0.1, Remote address: 1.0.0.2
     Local  identity: 30.0.0.10/255.255.255.255
     Remote identity: 40.0.0.10/255.255.255.255
     Path mtu 1500, media mtu 1500
     Current outbound spi: 0x12345678

   SA Type      SPI         Transform     PFS Secs left  KB left   Mode
   ------------ ----------- ------------- --- --------- ---------- ----
   Outound ESP   0x12345678  esp-md5-hmac  #2 14560     89630   Tunnel
                              esp-3des

   Inbound ESP   0x87654321   esp-md5-hmac  #2 60000     1569000 Tunnel
                              esp-3des


    Inbound packets                       Outbound packets
     --------------------------------- --------------------------------
     Total                          0    Total                        0
       Total OK                     0      Total OK                   0
         Decrypt                    0        Encrypt                  0
         Verify                     0        Digest                   0
         Decaps                     0        Encaps                   0
       Total discards               0      Total discards             0
         Invalid len                0        No sa                    0
         Replay failed              0        Seq rollover             0
         Sa expired                 0        Sa expired               0
         Auth failed                 0
         Bad padding                 0
         Invalid idenitity           0
         Unprotected                 0
        Other discards              0        Other discards           0
```

```
SA Type      SPI        Transform     PFS Secs left  KB left   Mode
------------ ----------- ------------ --- --------- ---------- ----
Outound ESP  0x12345678  esp-md5-hmac  No 1456      96530   Tunnel
                          esp-3des

Inbound ESP   0x87654321  esp-md5-hmac  No 26964    102044 Tunnel
                          esp-3des


 Inbound packets                       Outbound packets
  ---------------------------------   ------------------------------
  Total                          0    Total                        0
    Total OK                     0      Total OK                   0
      Decrypt                    0        Encrypt                  0
      Verify                     0        Digest                   0
      Decaps                     0        Encaps                   0
    Total discards               0      Total discards             0
      Invalid len                0        No sa                    0
      Replay failed              0        Seq rollover             0
      Sa expired                 0        Sa expired               0
      Auth failed                 0
      Bad padding                 0
      Invalid idenitity           0
      Unprotected                 0
      Other discards             0        Other discards           0
```

show crypto ipsec transform-set

Use the **show crypto ipsec transform-set** command to display the configuration for the specified transform-set or all transform-sets.

Syntax

show crypto ipsec transform-set [tag *transform-set-name*]

Parameters

Parameter	Description	Possible Values	Default Value
tag transform-set-name	The name of the transform set you wish to display. If you do not enter a value, all transform-sets are displayed.		

User level

read-only

Context

general

Example

```
G350-001> show crypto ipsec transform-set

Name                 ESP Encr   ESP Hash PFS  Life sec Life KB Mode
--------------------- ---------- --------- --- --------- -------- ----
Lincroft-Transform    3des      sha-hmac  #2   25000    3680010  Tunnel
Westminster-Transform aes       sha-hmac  No   86400    5368702  Tunnel
```

show crypto isakmp peer

Use the **show crypto isakmp peer** command to display crypto ISAKMP peer configuration.

Syntax

show crypto isakmp peer

User level

read-only

Context

general

Example

```
G350-001> show crypto isakmp peer

Showing 1 rows

Description       Peer identity      Auth  Plc

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

                  135.64.102.109     psk     1
```

show crypto isakmp policy

Use the **`show crypto isakmp policy`** command to display ISAKMP policy configuration.

Syntax

`show crypto isakmp policy`

User level

read-only

Context

general

Example

```
G350-001> show crypto isakmp policy

Id Description      Encr    Hash    Authentication DH group life sec
-- ---------------- ------- ------- -------------- -------- ----------
 1 lincroft ike      3des    md5     Preshared key        2      60000
```

show crypto isakmp sa

Use the **`show crypto isakmp sa`** command to display the ISAKMP SA database status.

Syntax

`show crypto isakmp sa`

User level

read-only

Context

general

Example

```
G350-001> show crypto isakmp sa
```

```
Showing 2 rows:

C-id Local           Remote          State   Hash Auth DH Sec left
---- --------------- --------------- ------- ---- ---- -- -----
1    123.123.123.123 133.133.133.133 Ready    md5  psk  1   29600
2    222.123.123.123 111.133.133.133 Ready    sha  psk  2   12690
5    1.1.1.1         2.2.2.2         MM Neg
10   1.1.1.1         3.3.3.3         No-Srvc  sha  psk  2   80000
17   123.1.2.1       135.34.3.2      Delete   sha  psk  2   20
```

Output fields

Name	Description
C-id	Connection ID (set using the crypto map command)
Local	IP address of local peer
Remote	IP address of remote peer
State	The state of the ISAKMP SA Ready – ready to pass ISAKMP information MM Neg – Main Mode Negotiation No-Srvc – in Deactivate process Delete – in Delete process
Hash	The hashing algorithm used: md5 or sha
Auth	The authentication type
DH	The Diffie-Hellman group
Sec left	Time left for SA (set using the lifetime command in `crypto isakmp policy` context).

show crypto map

Use the **`show crypto map`** command to display all or specific crypto map configurations.

Syntax

`show crypto map [`*`id`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
id	The ID of the crypto map for which to display configuration information. If you do not enter a value then all crypto map configurations are displayed.		

User level

read-only

Context

general

Example

```
G350-001> show crypto map

Showing 2 rows:

ID   Description        Remote Peer     Transform-set          DSCP
---- ------------------ -------------- --------------------    ----
5    Lincroft VPN       1.0.0.2         Lincroft-Transform     copy
10   Westminster VPN     2.1.1.2         Westminster-Transform  10
```

Output fields

Name	Description
ID	Crypto map ID (set using the crypto map command)
Description	Crypto map description
Remote peer	IP address of remote peer
Transform-set	The name of the transform-set
DSCP	The DSCP configuration

show csu loopbacks

Use the **show csu loopbacks** command to view the state of the server SAT-controlled CSU loopbacks on a media module.

Syntax

```
show csu loopbacks mmID
```

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User level

read-only

Context

general

Example

To view the state of loopbacks on Module v2:

```
G350-001>show csu loopbacks v2

CSU LOOPBACK STATUS
-----------------------------------
Towards DTE Port-
Digital Diagnostics: OFF
Towards Network-
Payload: OFF
Line   : OFF
```

show csu status

Use the **show csu status** command to view the status of the CSU on a media module.

Syntax

```
show csu status mmID
```

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User level

read-only

Context

general

Example

To display the status of the CSU on module 4:

```
G350-001# show csu status v4
```

```
TI version of csu status:
```

```
CSU NETWORK INTERFACE STATUS
------------------------------------------------------------------
LOS:ON00F:OFF
EER:OFFL00PD:OFF
AIS:OFFPDV:OFF
LOF:OFFYEL:ON
```

```
E1 version of csu status:
```

```
CSU NETWORK INTERFACE STATUS
------------------------------------------------------------------
LOS:ON00F:OFF
EER:OFFL00PD:OFF
AIS:OFFPDV:OFF
LOF:OFFLMA:OFF
RMA:OFFLCM:ON
```

Output fields

Name	Description
LOS	Loss of signal
OOF	Out of frame
	1 of 2

Name	Description
EER	Excessive error rate
LOF	Loss of frame
AIS	Alarm indication signal
YEL	Yellow
PDV	Pulse density violation (same as BPV)
LOOPD	Looped
LMA	Local multiframe alignment
RMA	Remote multiframe alignment
LCM	Loss of CRC multiframe
	2 of 2

show dev log file

Use the **`show dev log file`** command to display the encrypted device's log file.

Syntax

```
show dev log file
```

User level

read-write

Context

general

show dot1x

Use the **`show dot1x`** command to display the system dot1x capabilities, protocol version, and timer values.

Syntax

```
show dot1x
```

User level

admin

Context

general

Example

```
Console> show dot1x
PAE Capabilities Authenticator Only
Protocol Version 1
system-auth-control disabled
*** Warning : Authentication server is disabled/not-exist and so, no
authentication can be made
```

show download license-file status

Use the **show download license-file status** command to display the status of the download process of the VPN license to the device.

Syntax

show download license-file status

User level

read-only

Context

general

Example

```
G350-001> show download license-file status

Module #10
===========
Module           : 10
Source file      : /home/llevinsk/EI2/03IS70594996.xml
Destination file : license-file
Host             : 135.64.103.112
Running state    : Idle
Failure display  : (null)
Last warning     : (null)
Bytes Downloaded   : 0
```

show download phone-script-file status

Use the **`show download phone-script-file`** status command to the status of status of download phone-script file.

Syntax

`show download phone-script-file`

User level

Read only

Context

general

Example

```
interface# > show download phone-script-file status
```

- If no download has been performed:

```
Module #10
===========
No dest file for download operation - no download operation was
done.
```

- If a download has been performed:

```
Module #10
===========
Module           : 10
Source file      : /home/p46xx-script
Destination file : phone-ScriptA
Host             : 135.64.103.116
Running state    : Idle
Failure display  : (null)

Last warning     : No-warning
Bytes Downloaded : 27
```

show download software status

Use the **`show download software status`** command to display the status of the current Device Manager software download process as the software is being loaded into the module.

Syntax

`show download software status [`*`module_number`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`module_number`	The number of the module for which to display information	**0 – 10**	

User level

read-only

Context

general

Example

To display the status of a device software download into module #1:

```
G350-001> show download software status 1
```

```
Module #1
===========
Module           : 1
Source file      : d:\p340sw\gt-ml\3.5.18\p340.web
Destination file : EW_Archive
Host             : 149.49.70.61
Running state    : Writing ...
Failure display  : (null)
Last warning     : No-warning
```

show download status

Use the **show download status** command to display the status of the current configuration file download process, as the file is being loaded into the device.

Syntax

```
show download status [module_number]
```

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The number of the module for which to display information	**1 – 10**	

User level

read-only

Context

general

Example

To display the status of a configuration file download for module 10:

```
G350-001> show download status 10
```

show dscp-table

Use the **show dscp-table** command to display a specific entry in the DSCP table. If no DSCP index is specified, the entire DSCP table is displayed.

Syntax

```
show dscp-table [index]
```

Parameters

Parameter	Description	Possible Values	Default Value
index	The DSCP entry		

User level

read-write

Context

ip qos-list, ip qos-list dscp-table, ip qos-list ip-rule

Example

To display the entire DSCP table:

```
G350-011(QoS 444)# show dscp-table
```

```
Trust configuration is trust-cos
```

```
DSCP     Action           Precedence     Name
---- -------------------- ---------- ------------
0    No-Change            mandatory  DSCP#0
1    No-Change            mandatory  DSCP#1
2    No-Change            mandatory  DSCP#2
3    No-Change            mandatory  DSCP#3
4    No-Change            mandatory  DSCP#4
5    No-Change            mandatory  DSCP#5
6    No-Change            mandatory  DSCP#6
7    No-Change            mandatory  DSCP#7
8    No-Change            mandatory  DSCP#8
9    No-Change            mandatory  DSCP#9
10   No-Change            mandatory  DSCP#10
11   No-Change            mandatory  DSCP#11
.
.
.
63   No-Change              mandatory    DSCP#63
```

show ds-mode

Use the **show ds-mode** command to display the current mode of the controller.

Syntax

show ds-mode

User level

read-only

Context

general

Example

To display the ds-mode:

```
G350-001> show ds-mode
```

```
Current ds-mode:    T1
Configured ds-mode: T1
```

show dynamic-cac

Use the **show dynamic-cac** command to display information about the most recent dynamic CAC event.

Syntax

show dynamic-cac

User level

read-only

Context

general

Example

```
G350-001> show dynamic-cac
Current RBBL : 256 kbps
event : 0 Days, 1:21:00
Last event BBL : 256 kbps
```

show erase status

Use the **`show erase status`** command to display the status of the **erase startup-config** operation.

Syntax

`show erase status`

User level

read-write

Context

general

show etr

Use the **`show etr`** command to view the status of Emergency Transfer Relay (ETR) mode.

Note:

In ETR mode, the TRK and LINE 1 ports are connected. All other telephone ports stop operating.

Syntax

`show etr`

User level

read-only

Context

general

Example

To display the ETR status:

```
G350-001> show etr
Module: 7
Admin State: auto
Module status: in service
Trunk line  line status
----- ----  -----------
1     2     off hook
```

show faults

Use the **show faults** command to display the active faults for the media gateway.

Syntax

show faults

User level

read-only

Context

general

Example

To display the current fault list:

```
G350-001> show faults
CURRENTLY ACTIVE FAULTS
-------------------------------------------------------------------
-- Hardware Faults --
        + Multiple fans outage, 01/01-18:26:35.00
        + PSU fan brief outage, 01/01-18:26:35.00
-- MGP Faults --
        + No controller found, 01/01-00:00:01.00
```

show flows

Use the **show flows** command to display information about the real-time status of micro-flows within output queues for the current interface.

Note:

This command is only applicable in fair-voip-queue mode.

Syntax

show flows *type identifier*

Parameters

Parameter	Description	Possible Values	Default Value
type	The type of interface	**Fast Ethernet** **Serial**	
identifier	The identifier depends on the interface type: For Fast Ethernet: ***module/ port*** For Serial: ***module/ port:channel-group***	channel-group: E1: **0-30** T1: **0-23**	

User level

read

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when traffic shaping is configured

Examples

```
G350-001> show flows FastEthernet 10/2
```

```
G350-001> show flows Serial 3/1:2
```

show fragment

Use the **show fragment** command to display information about IP packets that are passing from or to the router.

Note:

No IP reassembly is performed on packets in transit through the router.

Syntax

```
show fragment
```

User level

read-only

Context

general

Example

To display fragmented IP packets information:

```
G350-001> show fragment
```

```
Max number of concurrently reassembled packets is 100
Max number of fragments per packet is 64
Fragment timeout is 10 sec
Number of packets waiting to be reassembled is 0
Number of successfully reassembled packets is 11954
Number of packets which failed to be reassembled is 0
Number of packets which overflowed the database is 0
```

show frame-relay fragment

Use the **`show frame-relay fragment`** command to display frame-relay fragmentation statistics and configuration on all PVCs, all PVCs associated with an interface, or a specific PVC.

Note:

When statistics for multiple PVCs are shown, they are sorted first by interface type and number, and then by DLCI.

Syntax

```
show frame-relay fragment [interface interface_name|dlci_number]
```

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	Type and identifier of the interface enclosed in quotes		
dlci_number	The PVC identifier	**16-1007**	

User level

read-only

Context

general

Example

To show details on configuration and statistics for fragmentation on all PVCs associated with a Serial interface:

```
G350-001> show frame-relay fragment interface “Serial 5/1”
```

show frame-relay lmi

Use the **`show frame-relay lmi`** command to display LMI statistics for a particular interface or for all interfaces. The output displayed differs depending on the type of interface.

Syntax

`show frame-relay lmi [interface` ***`interface_name`*** **`]`**

Parameters

Parameter	Description	Possible Values	Default Value
interface_ name	The name of the interface		

User level

read-only

Context

general

Example

To display LMI statistics for all interfaces:

```
G350-001# show frame-relay lmi

LMI Statistics for interface Serial 1 (Frame Relay DTE)

LMI TYPE = ANSI Annex D  Invalid Unnumbered info       0,     Invalid
Prot Disc              0  Invalid dummy Call Ref        0,     Invalid
Msg Type               0  Invalid Status Message        0,     Invalid
Lock Shift             0  Invalid Information ID        0,     Invalid
Report IE Len          0  Invalid Report Request        0,     Invalid
Keep IE Len          0  Num Status Enq. Sent          0,    Num Status
```

```
msgs Rcvd          0  Num Update Status Rcvd        0,     Num Status
Timeouts           0
LMI Statistics for interface Serial 2 (Frame Relay DTE)
LMI TYPE = Auto Detect Mode  Invalid Unnumbered info       0,
Invalid Prot Disc             0  Invalid dummy Call Ref         0,
Invalid Msg Type              0  Invalid Status Message         0,
Invalid Lock Shift            0  Invalid Information ID         0,
Invalid Report IE Len         0  Invalid Report Request         0,
Invalid Keep IE Len           0  Num Status Enq. Sent           0,
Num Status msgs Rcvd          0  Num Update Status Rcvd         0,
Num Status Timeouts            0
```

Output Fields

Item	Description
LMI Statistics	Signaling or LMI specification: ANSI, or ITU-T.
Invalid Unnumbered info	Number of received LMI messages with invalid unnumbered information field.
Invalid Prot Disc	Number of received LMI messages with invalid protocol discriminator.
Invalid dummy Call Ref	Number of received LMI messages with invalid dummy call references.
Invalid Msg Type	Number of received LMI messages with invalid message type.
Invalid Status Message	Number of received LMI messages with invalid status message.
Invalid Lock Shift	Number of received LMI messages with invalid lock shift type.
Invalid Information ID	Number of received LMI messages with invalid information identifier.
Invalid Report IE Len	Number of received LMI messages with invalid Report IE Length.
Invalid Report Request	Number of received LMI messages with invalid Report Request.
Invalid Keep IE Len	Number of received LMI messages with invalid Keep IE Length.
Num Status Enq. Sent	Number of LMI status inquiry messages sent.
Num Status Msgs Rcvd	Number of LMI status messages received.
Num Update Status Rcvd	Number of LMI asynchronous update status messages received.
	1 of 2

Item	Description
Num Status Timeouts	Number of times the status message was not received within the keepalive time value.
Num Status Enq. Rcvd	Number of LMI status enquiry messages received.
Num Status Msgs Sent	Number of LMI status messages sent.
Num Status Enq. Timeouts	Number of times the status enquiry message was not received within the T392 DCE timer value.
Num Update Status Sent	Number of LMI asynchronous update status messages sent.
	2 of 2

show frame-relay map

Use the **`show frame-relay map`** command to display a summary table of Frame Relay sub-interfaces and DLCIs associated with the sub-interfaces.

Syntax

`show frame-relay map`

User level

read-only

Context

general

Example

To display information about the Frame Relay sub-interfaces:

```
G350-001> show frame-relay map
```

```
Showing 2 frame-relay map entries
Interface StateInterface Type DLCI DLCI Type DLCI State
----------- ------ ------------- ---- --------- ------
Serial 1.1 downpoint-to-point   17 broadcast deleted
Serial 1.1 down point-to-point   18 broadcast deleted
```

show frame-relay pvc

Use the **show frame-relay pvc** command to display detailed PVC information. The information can be shown for all PVCs known to the device, for all PVCs learned on an interface, or for a specific PVC (DLCI). Note that in this case, all PVCs with the same DLCI are displayed. When statistics for multiple PVCs are shown, they are sorted first by interface type and number, and then by DLCI.

Syntax

show frame-relay pvc [interface *interface_name* | *dlci_number*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	Type and identifier of the interface enclosed in quotes		
dlci_number	The PVC identifier	**16-1007**	

User level

read-only

Context

general

Example

To show details on configuration and statistics for all PVCs associated with interface “Serial 1.1":

```
G350-001> show frame-relay pvc interface "Serial 1.1"
```

```
Showing 1 PVCPVC Statistics for interface Serial 1 (Frame Relay DTE)
DLCI =   17, USAGE = LOCAL ,
PVC STATUS = DELETED ,
INTERFACE = Serial 1.1
input pkts          0,
output pkts         0,
dropped pkts        0
in bytes            0,
out bytes           0
in FECN pkts        0
in BECN pkts        0
in DE pkts          0,
out DE pkts         0

pvc create time 00:05:17,
last time pvc status changed 00:05:07  traffic-shaping configured by
map-class foobar
cir             70000,
bc               7000,
be                  0  interval          100,
current bc       7000,
current be          0  pkts                0,
delayed pkts        0,
dropped pkts        0  bytes               0,
delayed byts        0,
dropped byts        0  de pre mark is on,
threshold is 20% of bc  end-to-end fragmentation is on,
fragment size is 88PVC Statistics for interface Serial 2 (Frame Relay
DTE)
```

show frame-relay pvc brief

Use the **show frame-relay pvc brief** command to display information on all PVCs known to the device, in a table form.

Syntax

show frame-relay pvc brief

User level

read-only

Context

general

Example

To show a table of all PVCs known to the device:

```
G350-011> show frame-relay pvc brief
```

show frame-relay traffic

Use the **show frame-relay traffic** command to display frame-relay protocol statistics, including ARP requests and replies sent and received over Frame Relay interfaces.

Syntax

show frame-relay traffic

User level

read-only

Context

general

Example

To display frame-relay statistics:

```
G350-001> show frame-relay traffic
```

```
Frame Relay statistics:
ARP requests sent       0,    ARP replies sent       0
ARP requests recvd      0,    ARP replies recvd      0
```

show icc-monitoring

Use the **show icc-monitoring** command to display the state of the icc-monitoring process.

Syntax

show icc-monitoring

User level

read-only

Context

general

Example

To display ICC monitoring status:

```
G350-001> show icc-monitoring
```

show icc-vlan

Use the **show icc-vlan** command to view the ICC-VLAN.

Syntax

show icc-vlan

User level

read-only

Context

general

Example

To display the ICC VLAN:

```
G350-001> show icc-vlan
VLAN 1
```

show image version

Use the **show image version** command to display the software version of the image on both memory banks of the device.

Syntax

show image version

User level

read-only

Context

general

Example

To display the current software versions:

```
G350-001> show image version

Bank   Version
----   -------
```

```
A       3.9.7
B       3.12.10

Module number: 1
```

show interfaces

Use the **`show interfaces`** command to display interface configuration and statistics for a particular interface or all interfaces. The Frame Relay sub-interface only includes the following counters:

- packets & bytes in
- packets & bytes out
- input errors
- output drops

Syntax

`show interfaces [`*`interface_type interface_identifier`*`]`

Parameters\

Parameter	Description	Possible Values	Default Value
interface_type	The type of interface	**FastEthernet, Serial, Vlan, Loopback, Console, Tunnel, USB-modem**	
interface_ identifier	The interface number. The format varies depending on the value of interface_type: For FastEthernet: **module/port** For Serial: **module/ port:channel-group** For Vlan: **Vlan id** For LoopBack: **Loopback number** For Tunnel: **Tunnel number**	For FastEthernet: **10/2** For Serial(USP): **2/1** For Serial (DS1): module/port: **2/1** channel-group: E1: **0-30** T1: **0-23** For VLAN: **1-3071** For Loopback: **1-99**	

User level

read-write

Context

general

Example

To show information about all the interfaces:

```
G350-011# show interfaces
Vlan 1 is up, line protocol is up
Physical address is 00.04.0d.29.c5.11.
Internet address is 172.16.1.139, mask is 255.255.255.240
Primary management interface
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 00:00:30, Last output 00:00:30
Last clearing of ’show interface’ counters never.
5 minute input rate 144 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
3425 packets input, 323518 bytes
3425 broadcasts received, 0 giants
0 input errors, 0 CRC
32 packets output, 896 bytes
0 output errors, 0 collisions

FastEthernet 10/2 is up, line protocol is down
Physical address is 00.04.0d.29.c5.10.
MTU 1500 bytes. Bandwidth 10000 kbit.
Reliability 1/255 txLoad 255/255 rxLoad 255/255
Encapsulation ARPA
Link status trap disabled
Half-duplex, 10Mb/s, 10BaseTX
ARP type: ARPA, ARP Timeout 04:00:00
Dynamic CAC BBL: 1500 kbps
Dynamic CAC activation priority: 50
Dynamic CAC interface status: active
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

Tunnel 1 is up, line protocol is up
Internet address is 177.0.0.17, mask is 255.0.0.0
MTU 468 bytes. Bandwidth 9 kbit
Reliability 255/255 txLoad 1/255 rxLoad 1/255
Encapsulation GRE
Link status trap enabled
Keepalive set (10 sec), retries 3
Tunnel source 17.0.0.17, destination 12.0.0.3
Tunnel protocol/transport GRE/IP, key 777
Checksumming of packets enabled
Tunnel DSCP 63, Tunnel TTL 255
Path MTU Discovery, ager 10 mins, MTU 976, expires 00:09:33
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

Console asynchronous mode is terminal
Terminal baud rate is 9600
```

show interface usb-modem

Use the **`show interface usb-modem`** command to display the status and settings of the usb-modem.

Syntax

`show interface usb-modem`

User level

read-only

Context

general

Example

```
G350-011# show interface usb-modem

USB modem is present
Admin status is no-shutdown

Internet address is 10.0.1.20 mask is 255.255.0.0

MTU 1500 bytes, PPP baud rate is 38400,
line protocol is up

Modem Type: MT5634ZBA-USB

Init String: AT S7=45 S0=2 L1 V1 X4 &c1 E0 Q0,
Init string Status is OK

PPP authentication is PAP

Session inactivity timeout is 2 minutes
```

show ip access-control-list

Use the **show ip access-control-list** command to display the attributes of a specific access control list on the current interface.

Syntax

show ip access-control-list {*list_number* | all | active-list-in | active-list-out | active-list-in-out} [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The access control list to display		
all	Keyword specifying to display all access control lists		
active-list-in	Keyword specifying to display lists for the in direction		
active-list-out	Keyword specifying to display lists for the out direction		
			1 of 2

Parameter	Description	Possible Values	Default Value
`active-list-in-out`	Keyword specifying to display lists for in and out directions		
`detailed`	Keyword specifying to display detailed information		
			2 of 2

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To display detailed information about all access control lists on the VLAN 1 interface:

```
G350-011(if:Vlan 1)# show ip access-control-list all detailed
```

```
List Number: 300
---------------
List Name: Default ACL List
Default Action: permit
Owner: other

List Number: 320
---------------
List Name: Sync1
Default Action: permit
Owner: x9393

List Number: 330
---------------
List Name: Admin13
Default Action: permit
Owner: Charlie
```

show ip access-control-list

Use the **`show ip access-control-list`** command to display the attributes of a specific access control list or all lists.

Syntax

show ip access-control-list {*list_number* | all} [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_ number	The access control list to display		
all	Keyword specifying to display attributes for all access control lists		
detailed	Keyword specifying to display detailed information		

User level

read-write

Context

general

Example

To display detailed information about all access control lists:

```
G350-011# show ip access-control-list all detailed

List Number: 300
---------------
List Name: Default ACL List
Default Action: permit
Owner: other

List Number: 320
---------------
List Name: Sync1
Default Action: permit
Owner: x9393

List Number: 330
---------------
List Name: Admin13
Default Action: permit
Owner: Charlie
```

To display attributes of access control list 330:

```
G350-001# show ip access-control-list 330

Index Name                            Owner
----- ------------------------------- --------------------------
330   list #330                       other
ip options: Permit
ip fragments : Permit

Index Protocol     IP               Wildcard        Port Operation
----- -------- --- ---------------- --------------- ------------ ---
22     tcp     Src  Any                             Any         Permit
  Dst  Any                              Any
Deflt  Any     Src  Any                             Any         Permit
  Dst Any                           Any
```

show ip active-lists

Use the **show ip active-lists** command to display information about a specific policy list or all lists.

Syntax

show ip active-lists [*list_index* | *list_type*]

Parameters

Parameter	Description	Possible Values	Default Value
list_index	The index of the policy list to view	**300 – 499**	
list_type	The type of list: ACL, Crypto, PBR, QoS		

User level

read-only

Context

general

Example

```
G350-001> show ip active-lists

Interface Name                  Dir. Type     Idx List Name
------------------------------- ---- -------- --- ----------------
FastEthernet 10/2               In   ACL      300 Default ACL List
FastEthernet 10/2               In   QoS      400 Default QoS List
FastEthernet 10/2               Out  ACL      300 Default ACL List
FastEthernet 10/2               Out  QoS      400 Default QoS List
FastEthernet 10/2               ---- Crypto   901 list #901
Vlan 1                          In   ACL      300 Default ACL List
Vlan 1                          In   QoS      400 Default QoS List
Vlan 1                          Out  ACL      300 Default ACL List
Vlan 1                          Out  QoS      400 Default QoS List
```

show ip active-pbr-lists

Use the **`show ip active-pbr-lists`** command to display details about a specific pbr list or all pbr lists.

Syntax

`show ip active-pbr-lists {list_number}`

Parameters

Parameter	Description	Possible Values	Default Value
`list_number`	The pbr list to view.	**800-899**	

User level

read-only

Context

general

Example

To display information about all pbr lists:

```
G350-001> show ip active-pbr-lists
```

```
Interface Name   Index   List Name
----------------------------------------
Vlan 1          801    Voice PBR List
Vlan 2           803     Data PBR List
```

show ip arp

Use the **`show ip arp`** command to display the Address Resolution Protocol (ARP) cache.

Syntax

`show ip arp  [`*`interface`*`|`*`ip_interface`*`|`*`ip_addr`*`[`*`ip_mask`*`] | static]`

Parameters

Parameter	Description	Possible Values	Default Value
`interface`	The interface name, in quotes	string (1-32 chars)	
`ip_interface`	The IP interface name, in quotes	string (1-32 chars)	
`ip_addr`	The IP address of the station(s)		
`ip_mask`	The IP mask of the routes		
`static`	Keyword that specifies to display static IP ARP information		

User level

read-only

Context

general

Example

To display all ARP mappings:

```
G350-001> show ip arp
```

To display one host ARP mapping:

```
G350-001> show ip arp 192.168.49.1
```

To display a range of ARP mappings:

```
G350-001> show ip arp 192.168.49.1 255.255.255.0
```

To display ARP mappings for the VLAN 1 interface:

```
G350-001> show ip arp “Vlan 1”
```

To display static ARP mapping:

```
G350-001> show ip arp static
```

Note:

When specifying an interface name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

show ip capture-list

Use the **show ip capture-list** command to display details about capture lists.

Syntax

show ip capture-list { list-number | all } [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The capture list to view.	**800-899**	

User level

read-only

Context

general

Example

To display information about all capture lists:

```
G350-001> show ip capture-list all

Index   Name                   Owner
-------------------------------------
500     Default Capture List    other
501    list #5021           other
```

show ip crypto-list

Use the **show ip crypto-list** command to display all or specific crypto-list configurations.

Syntax

show ip crypto-list {*list-number* | all} [detail]

Parameters

Parameter	Description	Possible Values	Default Value
list-number	The ID of the crypto-list for which to display configuration information		
all	Show all crypto-lists		
detailed	Display detailed configuration information		

User level

read-only

Context

general

Examples

1. To display the configuration of a specific crypto-list:

```
G350-001> show ip crypto-list 901

Index Description                Status     Owner
----- --------------------------- ---------  --------------------------
901   Gregory                    invalid    other

Local address: 12.12.1.2  [Interface Serial 5/1:1]

Rules:

   Index     IP               Wildcard        Action  Crypto map
   ----- --- ---------------- --------------- ------- ----------
   10    Src  171.121.231.123 255.255.255.255 Protect 5
         Dst  1.1.1.1         0.0.0.255
   19    Src  21.23.12.12     255.255.255.0   Protect 10
         Dst  12.1.1.1        0.0.0.255
   25    Src  3.1.2.2         255.255.255.0   Protect 15
         Dst  2.1.1.1         0.0.0.255
   Deflt Src  Any                             Bypass  -
         Dst  Any

Applicable crypto maps:

   ID   Description       Remote Peer     Transform-set        DSCP
   ---- ----------------- -------------- -------------------- ----
   5    Lincroft VPN      1.0.0.2         Lincroft-Transform   copy
   10   Westminster VPN    2.1.1.2         Westminster-Transform12
  15   *** Crypto map does not exist ***
```

2. To display all crypto-lists:

```
G350-001> show ip crypto-list

Index Description                     Status     Owner
----- ------------------------------- ---------
--------------------------
900   Default Crypto List             valid      other
901   list #901                       valid      other
```

show ip dhcp-pool

Use the show ip dhcp-pool command to display the configuration of a pool.

Syntax

show ip dhcp-pool

User level

read only

Context

dhcp pool

Example

To display the configuration of the current DHCP pool:

```
G350-001(DHCP 5)# show ip dhcp-pool
Index           Name
-------       ------------------
5             DHCP pool #5

Mode:                   Inactive
Start IP Address Range: 1.1.1.1
End IP Address Range:   1.1.1.20
Lease Time:             8 days 0 hours 0 minutes 0 seconds
BootFile:               N/A
Next-Server:            N/A
Client-Identifier:      N/A
Server-Name:            N/A

DHCP options
Option Num               1                Name     subnet-mask
Value                    255.255.255.0

Option Num               3                Name     default-router
Value                    1.1.1.1

Vendor Specific Information
Index                    1                Name     ccp.avaya.com
```

show ip dhcp-pool

Use the **`show ip dhcp-pool`** command to display DHCP pool configurations.

Syntax

`show ip dhcp-pool {`*`pool index`*`|all} [detailed]`

Parameters

Parameter	Description	Possible Values	Default Value
pool index	The index of a specific pool	**1-32**	
all	Displays all DHCP pools		
detailed	Displays detailed configuration information		

User level

read only

Context

general

Example

To display the configuration of DHCP pool 5:

```
Sanity_G350-001# show ip dhcp-pool 5
Index           Name
-------       ------------------
5             DHCP pool #5

Mode:                   Inactive
Start IP Address Range: 1.1.1.1
End IP Address Range:   1.1.1.20
Lease Time:             8 days 0 hours 0 minutes 0 seconds
BootFile:               N/A
Next-Server:            N/A
Client-Identifier:      N/A
Server-Name:            N/A

DHCP options
Option Num               1                Name     subnet-mask
Value                    255.255.255.0

Option Num               3                Name     default-router
```

```
Value                    1.1.1.1

Option Num               176              Name     SSON
Value                    This is an example

Vendor Specific Information
Index                    1                Name     ccp.avaya.com
Class-Identifier         (null)
Value                    This is an example too
```

To display the names and statuses of all configured DHCP pools:

```
Sanity_G350-001# show ip dhcp-pool all
Index   Name                           Mode
------  -------------------------  ------------
5       DHCP pool #5                Inactive
6       DHCP pool #6                Inactive
```

To display configuration information for all configured DHCP pools:

```
Sanity_G350-001# show ip dhcp-pool all detailed
Index           Name
-------       ------------------
5             DHCP pool #5

Mode:                   Inactive
Start IP Address Range: 1.1.1.1
End IP Address Range:   1.1.1.20
Lease Time:             8 days 0 hours 0 minutes 0 seconds
BootFile:               N/A
Next-Server:            N/A
Client-Identifier:      N/A
Server-Name:            N/A

DHCP options
Option Num               1                Name     subnet-mask
```

```
Value                    255.255.255.0

Option Num               3                Name     default-router
Value                    1.1.1.1

Option Num               176              Name     SSON
Value                    This is an example



Vendor Specific Information
Index                    1                Name     ccp.avaya.com
Class-Identifier         (null)
Value                    This is an example too



Index            Name
-------        ------------------
6              DHCP pool #6

Mode:                   Inactive
Start IP Address Range: 2.2.2.2
End IP Address Range:   2.2.2.20
Lease Time:             8 days 0 hours 0 minutes 0 seconds
BootFile:               N/A
Next-Server:            N/A
Client-Identifier:      N/A
Server-Name:            N/A

DHCP options
Option Num               1                Name     subnet-mask
Value                    255.255.255.248

Option Num               6                Name     dns-server
Value                    1.1.1.1 2.2.2.2
```

show ip dhcp-server bindings

A binding is an assignment of an IP address to a client. Use the **`show ip dhcp-server bindings`** command to display bindings.

Syntax

`show ip dhcp-server bindings`

Parameters

User level

read only

Context

general

Example

To display all IP address allocations to clients:

```
G350-001# show ip dhcp-server bindings
IP Address  Lease Expiration (seconds) Type      Client-Identifier
----------     ------------------    --------    ------------------
3.3.3.2       Infinite             Automatic   01:00:11:22:33:44:55:67
3.3.3.3       303244               Manual      01:00:11:22:33:44:55:66
```

show ip dhcp-server statistics

Use the **`show ip dhcp-server statistics`** command to display DHCP server statistics.

Syntax

`show ip dhcp-server statistics`

User level

read only

Context

general

Example

To display DHCP server statistics:

```
G350-001# show ip dhcp-server statistics
Counter                Value
-----------           -------
BOOTP Requests           1
DHCP Discovers           2
DHCP Requests            3
DHCP Declines            4
DHCP Releases            5
DHCP Informs             6
BOOTP Replies            7
DHCP Offers              8
DHCP Acks                9
```

show ip distribution access-lists

Use the **`show ip distribution access-lists`** command to display the contents of all current distribution lists or of a specific list.

Syntax

```
show ip distribution access-lists [distribution_list_number]
```

Parameters

Parameter	Description	Possible Values	Default Value
distribution_list_number	The distribution list number	**1-99**	

User level

read-only

Context

general

Example

To display the content of distribution list number 1:

```
G350-001> show ip distribution access-lists 1
```

To display the content of all current distribution lists:

```
G350-001> show ip distribution access-lists
```

show ip icmp

Use the **`show ip icmp`** command to display the status of ICMP error messages.

Syntax

`show ip icmp`

User level

read-only

Context

general

Example

To display ICMP error message status:

```
G350-555> show ip icmp
ICMP error messages status is ENABLE
```

show ip interface

Use the **`show ip interface`** command to display information about an IP interface.

Syntax

`show ip interface [`*`interface_name`*`|`*`ip_interface`*`|`*`ip_address`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface whose information you want to display		
ip_interface	The name of the IP interface whose information you want to display	string (1-32 chars)	
ip_address	The IP address of the interface whose information you want to display		

Note:

When specifying an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

User level

read-only

Context

general

Example

To display information for the FastEthernet interface:

```
G350-001> show ip interface "FastEthernet 10/2"
```

To display information for the sub-interface 0 of the FastEthernet interface:

```
G350-001> show ip interface "FastEthernet 10/2.0"
```

To display all IP interfaces:

```
G350-001> show ip interface
```

```
Showing 2 Interfaces
Serial 1:1 is down
Internet address is 2.2.2.2        , subnet mask is 255.255.255.0
Advertised IPCP address
Broadcast address is 2.2.2.255
Directed broadcast forwarding is disabled
Proxy ARP is disabled
Primary management IP interface

FastEthernet 10/2 is up
Internet address is 149.49.75.71   , subnet mask is 255.255.255.0
```

```
Broadcast address is 149.49.75.255
Directed broadcast forwarding is disabled
Proxy ARP is disabled
```

show ip interface brief

Use the **`show ip interface brief`** command to display a summary of the information for a specific interface or for all of the interfaces.

Syntax

`show ip interface brief [`*`interface_name`*`|`*`ip_interface`*`|`*`ip_address`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The name of the interface whose information you want to display		
ip_interface	The name of the IP interface whose information you want to display	string (1-32 chars)	
ip_address	The IP address of the interface whose information you want to display		

Note:

When specifying an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

User level

read-only

Context

general

Example

To display concise information about the FastEthernet interface:

```
G350-001> show ip interface brief “FastEthernet 10/2”
```

```
Showing 1 Interfaces
Interface             Address        Mask   Status
-------------------- -------------- ---- ---------
FastEth  10/2          172.16.1.139      16      up
```

show ip next-hop-list

Use the **`show ip next-hop-list`** command to show the details of the next-hop list.

Syntax

`show ip next-hop-list {next_hop_number | all}`

Parameters

Parameter	Description	Possible Values	Default Value
`next_hop_number`	The index number of the entry in the next-hop list	1-20	

User level

read-only

Context

ip pbr-list ip-rule

Examples

```
G350-001> show ip next-hop-list all
Index Name
----- ---------
1 list #1
3 list #3
```

```
G350-001> show ip next-hop-list 3
next hop list does not exist
```

show ip ospf

Use the **`show ip ospf`** command to display general information about OSPF routing.

Syntax

`show ip ospf`

User level

read-only

Context

general

Example

To display IP OSPF routing information:

```
G350-001> show ip ospf
```

```
Routing Process OSPF with ID 149.49.75.71
Number of areas in this router is 1
Area 0.0.0.0
Number of Interfaces in this area 0
SPF algorithm executed 1 times
SPF hold time is 3 sec
```

show ip ospf database

Use the **show ip ospf database** command to display lists of information related to the OSPF database for a specific router. If no router type is specified, OSPF information is displayed for all routers.

Syntax

```
show ip ospf database
[asbr-summary|router|network|network-summary|external]
```

Parameters

Parameter	Description	Possible Values	Default Value
asbr-summary	Displays information about the autonomous system boundary router summary LSAs		
router	Displays information about the router LSAs		
network	Displays information about the network LSAs		
network-summary	Displays information about the network LSAs summary		
external	Displays information about the external LSAs		

User level

read-only

Context

general

Example

To display OSPF database information for all router types:

```
G350-001> show ip ospf database
```

```
Showing 1 rows
Area      Type   LSA ID        Router ID     Sequence  Age   Cksm
-------  -----  ------------  -------------  -------- ----- ------
0.0.0.0   RTR   149.49.75.71   149.49.75.71  80000001  567   139b
```

show ip ospf interface

Use the **`show ip ospf interface`** command to display OSPF-related interface information. If no interface name is specified, information for all interfaces is displayed.

Syntax

```
show ip ospf interface [interface_name]
```

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The OSPF interface name	string	

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

User level

read-only

Context

general

Example

To display OSPF information for all interfaces:

```
G350-001> show ip ospf interface
```

```
sh ip ospf interface
```

```
Showing 1 OSPF Interfaces
Vlan 1.0 is up
Internet Address 1.1.1.1, Mask 255.255.255.0  , Area 0.0.0.0
AS Router ID 1.1.1.1, COST 1
Transmit Delay 1, State DR,  Priority 1
DRId 1.1.1.1, IpAddress 1.1.1.1
BDRId is 0.0.0.0, IpAddress 0.0.0.0
Timer Intervals Configured:
Hello 10
Dead 40
Retransmit 5
Neighbor count 0
```

show ip ospf neighbor

Use the **`show ip ospf neighbor`** command to display OSPF neighbor information for a specific interface or for all interfaces.

Syntax

show ip ospf neighbor [*interface_name*] [*neighbor_id*]

Parameters

Parameter	Description	Possible Values	Default Value
interface_name	The OSPF interface name	string	
neighbor_id	The OSPF neighbor ID number	an IP address	

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “New York”).

User level

read-only

Context

general

Example

To display neighbor information for all interfaces:

```
G350-001> show ip ospf neighbor
```

```
Nbr-Id           Priority   State      Router ID       Time To Live
--------------- ---------- ---------- --------------- -------------
10.0.17.2            1    2 Way      212.150.244.1        36
10.0.17.3           12    Full       10.0.17.3            38
10.0.17.6           18    Full       10.0.17.6            33
10.0.18.2            1    Full       105.1.12.1           107
10.0.20.2            0    Full       62.56.252.253        40
18.18.18.2           1    Full       62.56.255.254        38
192.168.6.173        0    Full       172.18.21.254         4
```

show ip pbr-list

Use the **ip pbr-list** command to display information about the specified pbr-list.

Syntax

show ip pbr-list {list_number | all} [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The pbr-list number to display	800-899	

User level

read-only

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

```
G350-001> show ip pbr-list 801 detailed
```

show ip protocols

Use the **`show ip protocols`** command to display parameters and statistics of the IP routing protocol process.

Syntax

`show ip protocols [`*`protocol`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`protocol`	The protocol for which to display statistics	**RIP, OSPF**	

User level

read-only

Context

general

Example

To display all running protocol details:

```
G350-011> show ip protocols
```

To display RIP details:

```
G350-011> show ip protocols RIP
```

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 0 seconds
Invalid after 180 seconds, flushed after 300
Redistributing: rip
Default version control: rip version 1
Interface                       Version   Key
Routing for Networks:
Routing Information Sources:
Gateway                 Last Update
```

show ip qos-list

Use the **show ip qos-list** command to display the attributes about a specific QoS list, or all QoS lists, for the current interface.

Syntax

show ip qos-list {*list_number* | all | active-list-in | active-list-out | active-list-in-out} [detailed]

Parameters

Parameter	Description	Possible Values	Default Value
list_number	The QoS list to display		
all	Keyword specifying to display all QoS lists		
active-list-in	Keyword specifying to display lists for the in direction		
active-list-out	Keyword specifying to display lists for the out direction		
active-list-in-out	Keyword specifying to display lists for in and out directions		
detailed	Keyword specifying to display detailed information		

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3), VLAN (L2, L2-L3), Loopback (L2, L2-L3), Tunnel (L2, L2-L3)

Example

To display information about all QoS lists:

```
G350-011(if:Vlan 1)# show ip qos-list all
```

```
List Number: 400
---------------
List Name: Default QoS List
```

```
Default Action: No-Change
Owner: other
List Trust: trust-cos
```

show ip qos-list

Use the **`show ip qos-list`** command to display the attributes about a specific QoS list.

Note:

> To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

Syntax

`show ip qos-list {`*`list_number`*` | all} [detailed]`

Parameters

Parameter	Description	Possible Values	Default Value
list_ number	The QoS list to display		
all	Keyword specifying to display all QoS lists		
detailed	Keyword specifying to display detailed information		

User level

read-write

Context

general

Example

To display detailed information about all the QoS lists on all the interfaces:

```
G350-011# show ip qos-list all detailed

Index Name                           Owner
----- ------------------------------ --------------------------
400   Default QoS List               other

Index Protocol     IP              Wildcard      Port Operation
```

```
----- -------- --- --------------- -------------- --------
----------
Deflt  Any     Src  Any                            Any Trust-DSCP-CoS
  Dst  Any                              Any


Index Name                            Owner
----- ------------------------------ -------------------------
440   list #440                       other

Index Protocol     IP               Wildcard        PortOperation
----- -------- --- --------------- -------------- ------- ----------
Deflt  Any     Src  Any AnyTrust-DSCP-CoS
 Dst  Any                              Any
```

show ip reverse-arp

Use the **show ip reverse-arp** command to display the IP address of a host, based on a known MAC address.

Syntax

show ip reverse-arp *mac_addr* [*match_len*]

Parameters

Parameter	Description	Possible Values	Default Value
mac_addr	The MAC address		
match_len	The number of bytes in the address to match		

User level

read-only

Context

general

Example

To list IPs that match a specific MAC address:

```
G350-001> show ip reverse-arp 00:10:a4:98:97:e0
```

```
Showing 1 rows
Address         MAC Address          I/F        Type     TTL
--------------- ----------------- ----------- ------- --------
149.49.70.68    00:10:a4:98:97:e0   e-70       Dynamic    14355
```

show ip route

Use the **`show ip route`** command to display information about the IP routing table.

Syntax

`show ip route [`*`ip_address`*`[`*`ip_mask`*`]]`

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the routes		
ip_mask	The IP mask of the routes		

User level

read-only

Context

general

Example

To display all routes:

```
G350-011> show ip route
```

To display a single route:

```
G350-011> show ip route 137.32.50.13
```

To display a range of routes:

```
G350-011> show ip route 137.44.50.13 255.255.255.0
```

show ip route best-match

Use the **show ip route best-match** command to display a routing table for a destination address.

Syntax

show ip route best-match *dst_addr*

Parameters

Parameter	Description	Possible Values	Default Value
dst_addr	The destination IP address		

User level

read-only

Context

general

Example

To display the routing table entries for IP address 199.93.0.0:

```
G350-001> show ip route best-match 199.93.0.0
```

```
Searching for: 199.93.0.0
Showing 1 rows
Network      Mask         Interface  Next-Hop       Cost  TTL Source
-----------  -----------  ---------  -------------  ----  --- -------
199.93.0.0   16           e-135new   135.64.76.1       1   n/a STAT-HI
```

show ip route static

Use the **show ip route static** command to display static routes.

Syntax

show ip route static [*ip_addr* [*mask*]]

Parameters

Parameter	Description	Possible Values	Default Value
ip_addr	The IP address of the routes		
mask	The IP mask of the routes		

User level

read-only

Context

general

Example

To display all static routes:

```
G350-001> show ip route static
```

To display a single static route:

```
G350-001> show ip route static 137.32.50.13
```

To display a range of static routes:

```
G350-001> show ip route static 137.44.50.13 255.255.255.0
```

```
G350-001> show ip route static
```

```
Showing 1 rows
Network  Mask Interface   Next-Hop     Cost  Pref  Perm  Active
-------  ---- ----------  -----------  ----  ----  ----  -------
0.0.0.0   0   FastEth 1  149.49.75.1    1   low    No    Yes
```

where `Pref` is the preference, and `Perm` is Permanent.

show ip route summary

Use the **`show ip route summary`** command to display the number of routes known to the device.

Syntax

`show ip route summary`

User level

read-only

Context

general

Example

To display a summary of routes:

```
G350-001> show ip route summary
```

```
Route Source        Networks          Subnets
----------------  ----------------  ------------
Local                  0                1
Static                 0                1
Total                    0                   2
```

show ip rtp header-compression

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.

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

Syntax

`show ip rtp header-compression [`*`interfaceName`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`interfaceName`	The name of the interface		

User level

read-only

Context

general

Example

To display compression statistics for all interfaces:

```
G350-001# show ip rtp header-compression
```

Output Fields

Section	Item	Description	Comment
Received	Full Headers	No. of RTP packets with Full headers received	
Received	Compressed	No. of RTP packets with compressed headers received	
Received	**Errors**	**Packets discarded during de-compression due to errors.**	
Sent	**Full Headers**	**No. of RTP packets with Full headers sent**	
Sent	**Compressed**	**No. of RTP packets with compressed headers sent**	
Sent	**Bytes Saved**	**Total saving in bytes due to compression**	
Sent	**Bytes Sent**	**Total bytes sent after compression**	
Sent	**Efficiency Improvement Factor**		**Rounded to two decimal places**
Connect	**Active/ Inactive**	**Status of RTP header compression on this interface**	
Connect	**Rx Slots**	**Actual no. of RTP sessions to decompress**	**After negotiation (when there is one), or equal to the user's setting.**
Connect	**Tx Slots**	**Actual no. of RTP sessions to compress**	**After negotiation (when there is one), or equal to the user's setting.**
			1 of 2

Section	Item	Description	Comment
Connect	**Max Time**	**Actual RTP Max time parameter**	**After negotiation (when there is one), or equal to the user's setting.**
Connect	**Max Period**	**Actual RTP Max period parameter**	**After negotiation (when there is one), or equal to the user's setting.**
			2 of 2

show ip rtp header-compression brief

Use the **`show ip rtp header-compression brief`** command to display a subset of header compression statistics in the form of a table.

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, "FastEthernet 10/2").

Syntax

```
show ip rtp header-compression brief [interfaceName]
```

Parameters

Parameter	Description	Possible Values	Default Value
`interfaceName`	The name of the interface		

User level

read-only

Context

general

Example

To display concise header compression statistics for all interfaces:

```
G350-001# show ip rtp header-compression brief
```

```
Interface  Active  Slots Max   Max   Packets    Bytes    Improvement
                         Time Period Sent      Saved       Factor
--------- -------- ----- ---- ------ --------- --------- -----------

Serial 1:0   NO      16    5   256      0        0          1.00
```

show ip ssh

Use the **show ip ssh** command to display general SSH information and information on the currently active connections that are using SSH.

Syntax

show ip ssh

User level

admin

Context

general

Example

```
G350-001(super)# show ip ssh
```

```
Max Sessions: 2
Key type: DSA , 512 bit
Listen Port: 22
Ciphers List: 3des-cbc
```

```
Session Version Encryption Username IP/Port
0        1.5  3des-cbc   guest   11.11.11.1/34444
```

show ip tcp header-compression

Use the **`show ip tcp header-compression`** command to display TCP header compression statistics for a specific interface. If no interface is specified, it shows TCP header compression statistics for all interfaces.

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

Syntax

`show ip tcp header-compression [`*`interfaceName`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`interfaceName`	The name of the interface		

User level

read-only

Context

general

Example

To display tcp header compression statistics for all interfaces:

```
G350-001# show ip tcp header-compression
```

Output Fields

Section	Item	Description	Comment
Received	Full Headers	No. of RTP packets with Full headers received	
Received	Compressed	No. of RTP packets with compressed headers received	
			1 of 2

Section	Item	Description	Comment
Received	Errors	Packets discarded during de-compression due to errors.	
Connect	Active/ Inactive	Status of RTP header compression on this interface	
Connect	Rx Slots	Actual no. of TCP sessions to decompress	After negotiation (when there is one), or equal to the user's setting.
Connect	Tx Slots	Actual no. of TCP sessions to compress	always 0
Connect	Max Time	Actual Max time parameter	After negotiation (when there is one), or equal to the user's setting.
Connect	Max Period	Actual Max period parameter	After negotiation (when there is one), or equal to the user's setting.
			2 of 2

show ip tcp header-compression brief

Use the **`show ip tcp header-compression`** command to display a subset of TCP header compression statistics for a specific interface. If no interface is specified, it shows TCP header compression statistics for all interfaces.

Note:

To specify an interface name that includes spaces, enclose the entire name in quotation marks (for example, “FastEthernet 10/2”).

Syntax

```
show ip tcp header-compression brief [interfaceName]
```

Parameters

Parameter	Description	Possible Values	Default Value
interfaceName	The name of the interface		

User level

read-only

Context

general

show ip tftp-server files

Use the **show ip tftp-server files** command to display the phone image and script files.

Syntax

show ip tftp-server files

User level

Read-write

Example

```
interface# > show ip tftp-server files
 File                Bank          Location    Size (bytes)
----------          ------------- ----------  --------------
46xxupgrade.txt     phone-scriptA Nv-Ram      4096
46xxsettings.txt    phone-scriptB Nv-Ram      16384
4602dbte1_8.bin     phone-imageA  Ram         1048576
4602dape1_8.bin     phone-imageD  Ram         2097152

Nv-Ram:
Total bytes used:             20480
Total bytes free:             110592
Total bytes capacity (fixed): 131072

Ram:
Total bytes used:                3166208
Total bytes free:                2076672
Total bytes capacity (Allocated) 3166208
Total bytes capacity (Configured)5242880
```

show ip traffic

Use the **`show ip traffic`** command to display IP counters information.

Syntax

`show ip traffic [`*`protocol_type`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`protocol_type`	The type of IP protocol for which to display information	**arp, bootp-dhcp, icmp, ip, ospf**	

User level

read-only

Context

general

Example

To display traffic information for all protocols:

```
G350-001> show ip traffic
```

```
IP statistics:
Received:
5644 total, 4012 local destination
0 bad hop count, 0 packet header errors
0 unknown protocol, 0 address errors
1632 discarded
Fragments:
0 reassembled, 0 timeouts
0 couldn’t reassemble, 0 fragmented

Sent:
4014 generated, 0 forwarded
0 no route, 0 discarded

ICMP statistics:
Received:
```

```
0 total, 0 ICMP errors
0 unreachables, 0 time exceeded
0 parameter, 0 quench
0 echo, 0 echo reply
0 timestamps request, 0 timestamp reply
0 mask requests, 0 mask replies
0 redirects

Sent:
0 total, 0 ICMP errors
0 unreachables, 0 time exceeded
0 parameter, 0 quench
0 echo, 0 echo reply
0 timestamps request, 0 timestamp reply
0 mask requests, 0 mask replies
0 redirects

OSPF statistics:
Received:
0 total, 0 checksum errors
0 hello, 0 database desc
0 link state req, 0 link state updates
0 link state acks

Sent:
0 total

ARP statistics:
Received:
5394 requests, 2 replies

Sent:
36 requests, 16 replies (0 proxy)
DHCP  statistics:
Requests: 0 , Replies: 0
BOOTP statistics:
Requests: 0 , Replies: 0
```

show ip vrrp

Use the **`show ip vrrp`** command to display VRRP information for a specific VLAN or for all VLANs.

Syntax

show ip vrrp [*vlan* [router-id *vr_id*]] [detail]

Parameters

Parameter	Description	Possible Values	Default Value
vlan	Filter by the specified VLAN	**1 – 4095**	
router_id	Keyword specifying to filter by virtual router ID		
vr_id	The virtual router ID	**1-255**	
detail	Keyword specifying to provide detailed information		

User level

read-only

Context

general

Example

To show VRRP information for all VLANs:

```
G350-001> show ip vrrp
```

```
VRRP is globally enabled
VLAN  VRID  IP Address     Pri   Timer     State     Since
----- ----- -------------  ----  -------  ---------  -----------
1     1    192.168.66.23  255     1       MASTER     00:00:00
1     2    192.168.66.24  100     1       BACKUP     00:00:00
```

To show detailed VRRP information for all VLANs:

```
G350-001# show ip vrrp detail
```

```
VRRP is globally enabled
Virtual Router on VLAN:1
Router-id:1
State:MASTER
Priority:                 255
Advertisement Interval:   1
Last State Change:        00:00:00
Override Address Ownership Rule: No
Authentication Type:      None
Authentication Key:       ""
Master IP Address         192.168.66.23
Has 1 IP addresses
IP addresses:
192.168.66.23
Primary IP Address:       192.168.66.23
Primary IP Address was chosen by default
Preemption Mode:          enabled
# of times Master:                                     2
# of received Advertisements:                          0
# of transmitted Advertisements:                       20
# of received Advertisements with Security Violations: 0
Virtual Router on VLAN:       1
Router-id:                2
State:                    BACKUP
Priority:                 100
Advertisement Interval:   1
Last State Change:        00:00:00
Override Address Ownership Rule: No
Authentication Type:      None
Authentication Key:       ""
Master IP Address         0.0.0.0
Has 1 IP addresses
IP addresses:
192.168.66.24
Primary IP Address:       192.168.66.23
Primary IP Address was chosen by default
Preemption Mode:          enabled
# of times Master:                                     1
# of received Advertisements:                          0
# of transmitted Advertisements:                       13
# of received Advertisements with Security Violations: 0
```

show ip-rule

Use the **show ip-rule** command to display the attributes of a specific rule. Leave the ***rule_number*** parameter blank to display all rules.

Syntax

show ip-rule [*rule_number*]

Parameters

Parameter	Description	Possible Values	Default Value
rule_number	The specific rule for which attributes are displayed		

User level

read-write

Context

ip access-control-list, ip access-control-list/ip-rule, ip qos-list, ip qos-list/ip-rule, ip capture-list, ip capture-list/ip-rule, ip pbr-list, ip pbr-list/ip-rule

Example

To display information about ip rule 22 in access-control-list 320:

```
G350-001(ACL 320/ip rule 22)# show ip-rule 22

I.D.  Protocol  IP Wildcard         Port      Operation
----- -------- --- ---------------- --------- ----------
22     Ip       Src  Any                      permit

                Dst  Any
```

show isdn bri link

Use the **show isdn bri link** command to view the status of all BRI links on a media module.

Syntax

show isdn bri link *mmID*

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User level

read-only

Context

general

Example

To display the status of all BRI links on media module 1:

```
G350-011> show isdn bri link 1
```

```
LOCATION  TYPE    LINK ID    DLCI       SIDE  STATE
--------- ------- ---------- ---------- ----- ------------
v1        NO LINK N/A        N/A        N/A   N/A
```

show isdn link summary

Use the **show isdn link summary** command to view a summary of all ISDN links.

Syntax

show isdn link summary

User level

read-only

Context

general

Example

To display information about all ISDN links:

```
G350-001> show isdn link summary
```

```
LOCATION      TYPE         NO. OF LINKS UP
---------     --------     ---------------
MG            NO LINK      N/A
```

show isdn pri link

Use the **`show isdn pri link`** command to view the status of all PRI links on a media module.

Syntax

`show isdn pri link` ***`mmID`***

Parameters

Parameter	Description	Possible Values	Default Value
`mmID`	The Media Module ID		

User level

read-only

Context

general

Example

To display PRI link information for media module 1:

```
G350-001> show isdn pri link 1
```

```
LOCATION  TYPE    LINK ID    DLCI       SIDE  STATE
--------- ------- ---------- ---------- ----- ------------
v1        NO LINK N/A        N/A        N/A   N/A
```

show keepalive

Use the **`show keepalive`** command to display information about the extended keepalive settings.

Syntax

`show keepalive`

User level

read-only

Context

Interface: FastEthernet (L2, L2-L3)

Example

To display extended keepalive information for the FastEthernet interface:

```
G350-001(if:FastEthernet 10/2)# show keepalive
```

```
Mode:                     Disable
Status:                   Disable
Destination IP:           172.16.1.228
Next-Hop MAC:             00:40:0d:b9:3e:45
Source IP:                0.0.0.0
Timeout:                  1 Sec
Interval:                 20 Sec
Success Retries:          1
Failure Retries:          4
Success Retries Counter:  0
Failure Retries Counter:0
```

show license status

Use the **show license status** command to display the status of the VPN license.

Syntax

show license status

User level

read-only

Context

general

Example

```
G350-001> show license status
```

```
License was installed.
```

show list

Use the **show list** command to display information about the specified list.

Syntax

show list

User level

read-write

Context

ip access-control-list, ip qos-list, ip capture-list, ip pbr-list

Example

To show detailed information about access control list 330:

```
G350-011(ACL 330)# show list

Index Name           Owner
----- -------------- ------------
330   SplitPriority     Admin

ip options: Permit
ip fragments : Permit


Index  Protocol    IP   Wildcard    Port    Operation-
-----  --------    --- ----------- -----    ----------
22     tcp         Src  Any         Any     Permit
                   Dst  Any         Any
Deflt  Any         Src  Any         Any     Permit
                   Dst  Any         Any
```

show logging file condition

Use the **show logging file condition** command to display all conditions that have been defined for the file output sink.

Syntax

show logging file condition

User level

read-only

Context

general

Example

To show information about conditions that are defined for the file output:

```
G350-011> show logging file condition
******************************************************
*** Message logging configuration of FILE     sink ***

Sink Is Enabled
Sink default severity: Informational

Facility             ! Severity Override
-------------------------------------------
FAN                  ! Error
VLAN                 ! Critical
```

show logging file content

Use the **show logging file content** command to output the messages in the log file to the CLI console. The output is arranged with the most recent event first. The content of the file is output according to the current filter settings and user access.

Syntax

show logging file content [*severity*] [all|*Msgfacility*] [*number*]

Parameters

Parameter	Description	Possible Values	Default Value
severity	Minimal severity of messages to be displayed		
all	Keyword specifying to display messages from all facilities		
Msgfacility	Display messages from this facility only		
number	Maximum number of messages to display		

User level

read-only

Context

general

Example

To display contents of the message file for all message facilities and severities:

```
G350-011> show logging file content
```

```
CLI-Notification: root: exit
CLI-Notification: root: exit
CLI-Notification: root:      ip
SECURITY-Warning: Unauthorized Access from IP address = 0.0.0.0, User
= super, Protocol = 23
CLI-Notification: root: exit
```

show logging server condition

Use the **show logging server condition** command to display the filter conditions that have been defined for the Syslog output sink. If an IP address or hostname is not specified, the configuration of all of the Syslog servers is displayed.

Syntax

show logging server condition [*ip_address* | *hostname*]

Parameters

Parameter	Description	Possible Values	Default Value
ip_address	The IP address of the Syslog server		
hostname	The name of the Syslog server host		

User level

read-only

Context

general

Example

To display filter conditions defined for the Syslog server at IP address 172.16.1.139:

```
G350-011> show logging server condition 172.16.1.139

Logging: enabled
Logging severity: warning

Facility            Severity Override
-------------       -----------------------
System              Critical

Syslog server 222.222.222.222
Logging: enabled
Logging severity: Debug

Facility            Severity Override
-------------       -----------------------
Kernel              Critical
```

show logging session condition

Use the **show logging session condition** command to display the filter conditions defined for message logging to the current console session.

Syntax

show logging session condition

User level

read-only

Context

general

Example

To display filter conditions defined for console messaging:

```
G350-011> show logging session condition

Logging console: enabled
Logging session severity: warning

Facility            Severity Override
-------------       -----------------------
System              Critical
```

show logout

Use the **show logout** command to display the amount of time in minutes the terminal remains idle before timing out. If the logout value is 0, there is no timeout limit. The default logout value is 15 minutes.

Syntax

show logout

User level

read-only

Context

general

Example

To display the timeout value:

```
G350-001> show logout
CLI timeout is 15 minutes
```

show map-class frame-relay

Use the **show map-class frame-relay** command to display the map-class Frame Relay table.

Syntax

show map-class frame-relay

User level

read-only

Context

general

Example

To display the map class Frame Relay table:

```
G350-001> show map-class frame-relay

Showing 1 frame-relay map-class entry
Map Class Name      CIR       BC        BE      De Pre-Mark Fragment
--------------- --------- --------- --------- ----------- ---------
default           56000     7000        0        100%        0
```

show mediaserver

Use the **show mediaserver** command to show media server configuration information.

Syntax

show mediaserver

User level

read-only

Context

general

Example

To display media server configuration information:

```
G350-001# show mediaserver


MGC IP ADDRESS   SAT IP ADDRESS   SAT PORT  SERVER IP ADDRESS  SERVER
PORT
---------------  ---------------  --------  -----------------
-----------
135.8.65.107     135.8.65.107     5023      135.8.65.107       23
```

show mg list_config

Use the **show mg list_config** command to show the installed media gateway equipment. It displays the current hardware and firmware configurations of the media gateway.

The **show mg list_config** command is an alias for show module on page 462.

Syntax

`show mg list_config`

User level

read-only

Context

general

Example

To display the list of installed equipment:

```
G350-001# show mg list_config

SLOT  TYPE   CODE    SUFFIX  HW VINTAGE  FW VINTAGE
----  ------ ------  ------  ----------  -----------
v0    G350   PC1053  B       00          0.0.15(B)
v1     -- Not Installed --
v2     -- Not Installed --
v3     -- Not Installed --
v4     -- Not Installed --
v5     -- Not Installed --
v6     -- Not Installed --
v7     -- Initilalizing --
```

show mgc

Use the **`show mgc`** command to display the currently active Media Gateway Controller state and setup parameters.

Syntax

`show mgc`

User level

read-only

Context

general

Example

To display media gateway controller information:

```
G350-001# show mgc

CALL CONTROLLER STATUS

-------------------------------------------
Registered          : NO
Active Controller   : 255.255.255.255
H248 Link Status    : DOWN
H248 Link Error Code: 0x0

CONFIGURED MGC HOST
---------------------
-- Not Available --
-- Not Available --
-- Not Available --
-- Not Available --
```

show mgc list

Use the **`show mgc list`** command to display the list of available Media Gateway Controllers and their IP addresses.

Syntax

`show mgc list`

User level

read-only

Context

general

Example

To display the list of media gateway controllers:

```
G350-001> show mgc list

CONFIGURED MGC HOST

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

135.8.48.220

-- Not Available --
-- Not Available --
-- Not Available --
```

show mm

Use the **`show mm`** command to show the media gateway Media Module information. It displays the types and serial numbers of Media Modules installed on the media gateway.

If no Media Module ID is specified, information for all Media Modules is displayed.

Syntax

`show mm [`*`mmID`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID number		

User level

read-only

Context

general

Example

To display information about media module 7:

```
G350-001> show mm 7

MEDIA MODULE DESCRIPTION: v7

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

Uptime(d,h:m:s): 0, 00:23:19
Type           : Voice (Initializing)
Description    : N/A
Serial Number  : N/A
HW Vintage     : N/A
HW Suffix      : N/A
FW Version     : N/A
No. of ports   : 0
Faults         : No Fault Messages
```

show module

Use the **`show module`** command to view information about a Media Module. To view information about all Media Modules, do not specify a Media Module.

Syntax

`show module [`*`mmID`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
mmID	The Media Module ID		

User level

read-only

Context

general

Example

To show information about media module 3:

```
G350-001> show module v3
SLOT TYPE       CODE     SUFFIX  HW VINTAGE  FW VINTAGE
---- ---------  ----     ------  ----------  ----------
v3   DS1        MM710    A       4           5
```

To show information about all media modules:

```
G350-001> show module
SLOT TYPE       CODE     SUFFIX  HW VINTAGE  FW VINTAGE
---- ---------  ----     ------  ----------  ----------
v0   G350       DAF1     A       00          10(B)
v1   ICC        S8300    A       4           6
v2   DCP        MM712    A       3           3
v3   DS1        MM710    A       4           5
v4   -- Not Installed -
v5   -- Not Installed -
v6   PoE        MM314
v7   Analog     (on-board)
```

show next-hop

Use the **`show next-hop`** command to show the next-hop entries in the current list.

Syntax

`show next-hop`

User level

read-only

Context

ip next-hop-list

Example

```
G350-001> show next-hop

Index Name

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

3 list #3

Index Next Hop IP/Interface Status
------- ------------------------- -------
1 149.49.200.3 Down
4 Serial5/1:0 Up
```

show pmi

Use the **show pmi** command to view the current Primary Management Interface.

Syntax

show pmi

User level

read-only

Context

general

Example

To view information about the current PMI:

```
G350-001> show pmi
Active PMI     : interface Vlan 1 (172.16.1.139)
Configured PMI : interface Vlan 1 (172.16.1.139)
```

show port

Use the **show port** command to display port status on I/O modules. If no port is specified, information for all ports is displayed.

Syntax

show port [*module*[/*port*]]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To display the status for port 4 on module 3:

```
G350-001> show port 3/4
```

```
Port Name    Status  Vlan Level  Neg    Dup. Spd. Type
---- ------- ------- ---- ----- ------- ---- ---- -------------
3/4 NO NAME no link   1    0   enable  half 10M  10/100BaseTx Port
```

Output fields

Name	Description
Port	Module and port number
Name	Name of port
Status	Status of the port — **connected, faulty, disabled, no link**
Vlan	VLAN ID of the port
Level	Priority level of the port — **0-7**
Neg	Autonegotiation status of the port — **enabled, disabled**
Dup	Duplex setting for the port — **full, half**
Speed	Speed setting for the port — **10, 100, 1000**
Type	Port type, for example: **10/100BASE-TX, GBIC_SX, GBIC_LX, GBIC_not present, GBIC_unknown**

show port auto-negotiation-flowcontrol-advertisement

Use the **`show port auto-negotiation-flowcontrol-advertisement`** command to display the flowcontrol advertisement for a Gigabit port used to perform auto-negotiation. If no port is specified, information for all ports is displayed.

Syntax

`set auto-negotiation-flowcontrol-advertisement [`*`module/port`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
module	The module number		
port	The port number		

User level

read-only

Context

general

Example

To display the flowcontrol advertisement for all ports:

```
G350-001> show port auto-negotiation-flowcontrol-advertisement
asym-tx-only 4/49
Port 4/49 pause capabilities was set
```

show port classification

Use the **`show port classification`** command to display a port’s classification. If no port is specified, information for all ports is displayed.

Syntax

`show port classification [module/[port]]`

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To display information for port 8 of module 4:

```
G350-001> show port classification 4/8
```

```
Port   Port Classification
------ --------------------
4/8    regular
```

show port dot1x

Use the **show port dot1x** command to display the configurable values associated with the authenticator Port Access Entity (PAE) and backend authenticator.

Syntax

show port dot1x ***[mod[/port]]***

Parameters

Parameter	Description	Possible Values	Default Value
mod	(Optional) Number of the module.		
port	(Optional) Number of the port on the module.		

User level

admin

Context

general

Example

```
Console> show port dot1x 3/3
Port   Auth  BEnd  Port    Port   Re   Quiet ReAuth Server Supp   Tx    Max
Number State State Control Status Auth Priod Priod  Tmeout Tmeout Priod Req
------ ----- ----- ------- ------ ---- ----- ------ ------ ------ ----- ---
1/3    Init  Init   Auto   Unauth Disa   60   3600     30     30     30   2
```

show port dot1x statistics

Use the **`show port dot1x statistics`** command to display all the port dot1x statistics.

Syntax

`show port dot1x statistics` ***`[mod[/port]]`***

Parameters

Parameter	Description	Possible Values	Default Value
mod	(Optional) Number of the module.		
port	(Optional) Number of the port on the module.		

User level

admin

Context

general

Example

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

show port edge state

Use the **show port edge state** command to display the edge state of the specified port. If no port is specified, information for all ports is displayed.

Syntax

```
show port edge state [module/[port]]
```

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To show edge state for all ports:

```
G350-001> show port edge state
```

show port flowcontrol

Use the **show port flowcontrol** command to display port flow control information. If no port is specified, information for all ports is displayed.

Syntax

show port flowcontrol [*module*[/*port*]

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module		

User level

read-only

Context

general

Example

To display flowcontrol information for port 4 of module 3:

```
G350-101> show port flowcontrol 3/4
```

```
Port   Send-Flowcontrol Receive-Flowcontrol
Admin Oper       Admin Oper
------ ----- ----       ----- ----
3/4   off   off        off   off
```

Output fields

Field	Description
Port	Module and port number
Send-Flowcontrol-Admin	Send flow-control administration. Possible settings: ON — indicates that the local port is allowed to send flow control frames to the far end. OFF — indicates that the local port is *not* allowed to send flow control frames to the far end.
Send-Flowcontrol-Oper	Send flow-control operation mode. Possible modes: ON — indicates that the local port will send flow control frames to the far end. OFF — indicates that the local port will *not* send flow control frames to the far end.
Receive-Flowcontrol-Admin	Receive flow-control administration. Possible settings: ON — indicates that the local port will act upon flow control indications if received from the far end. OFF — indicates that the local port will discard flow control frames if received from the far end.
Receive-Flowcontrol-Oper	Receive flow-control operation mode. Possible modes: ON — indicates that the local port will act upon flow control indications received from the far end. OFF — indicates that the local port will discard flow control frames received from the far end.

show port mirror

Use the **`show port mirror`** command to display mirroring information for the specified port. If no port is specified, information for all ports is displayed.

Syntax

`show port mirror [`*`module/port`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module		

User level

read-only

Context

general

Example

To display port mirroring information for all ports:

```
G350-011> show port mirror
```

show port point-to-point status

Use the **`show port point-to-point status`** command to display the point-to-point status of the specified port. If no port is specified, information for all ports is displayed.

Syntax

`show port point-to-point status [module/port]`

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module		

User level

read-only

Context

general

Example

To display point-to-point information for all ports:

```
G350-011> show port point-to-point status
```

show port redundancy

Use the **`show port redundancy`** command to display information about software port redundancy pairs defined on the media gateway.

Syntax

`show port redundancy`

User level

read-only

Context

general

Example

To display port redundancy information:

```
G350-001> show port redundancy

Redundancy Name     Primary Port        Secondary Port      Status
-----------------   --------------      ----------------    --------
bud3/48                   3/47   secondary
jack3/46                   3/45  secondary
tony3/1                    3/2   primary
wayne3/34                   3/33  secondary
Minimum Time between Switchovers: 1

Switchback interval: 3
```

show port trap

Use the **`show port trap`** command to display information on SNMP generic link up/down traps sent for a specific port. If no port is specified, information for all ports is displayed.

Syntax

`show port trap [`*`module`*`[/`*`port`*`]]`

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module. You can also specify a range of ports separated by a dash, for example, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To display trap information for port 1 of module 4:

```
G350-455> show port trap 4/1
Port 4/1 up/down trap is disabled
```

show port vlan-binding-mode

Use the **`show port-vlan-binding`** command to display port VLAN binding mode information. If no module number is specified, 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.

Syntax

`show port vlan-binding-mode [`*`module`*`[/`*`port`*`]]`

Parameters

Parameter	Description	Possible Values	Default Value
module	The number of the module		
port	The number of the port on the module. You can also specify a range of ports, for example, 4/5-13 for ports 5 to 13 on module 4.		

User level

read-only

Context

general

Example

To display VLAN binding information for all ports:

```
G350-001> show port vlan-binding-mode
```

```
port 2/1 is statically bound
port 2/2 is statically bound
port 2/3 is statically bound
port 2/4 is statically bound
port 2/5 is statically bound
port 2/6 is statically bound
port 2/7 is statically bound
port 2/8 is statically bound
port 2/9 is statically bound
port 2/10 is statically bound
```

show powerinline

Use the **show powerinline** command to display the current inline power status of the specified module or port. If no port is specified, information for all ports is displayed.

Syntax

show powerinline [*module_number/port_number*]

Parameters

Parameter	Description	Possible Values	Default Value
module_number	The module number		
port_number	The port number		

User level

read-only

Context

general

Example

To display power information for ports on module 6:

```
G350-001> show powerinline 6
Actual powerinline power consumption is 30W.
Powerinline power consumption trap threshold is 207 (99%) Watts.
Powerinline traps are enabled
Port  Inline Operational Status  Powering Priority  PD Type
----  -------------------------  -----------------  --------
6/1   Fault                      Low                telephone
6/2   Searching                  Low                telephone
```

show ppp authentication

Use the **show ppp authentication** command to show the PPP authentication status.

Syntax

show ppp authentication

User level

Read only

Context

Ethernet interface

Example

```
interface# > show ppp authentication
PAP sent-username: configured
CHAP refuseCHAP hostname: G350
CHAP password: not configured
```

show protocol

Use the **`show protocol`** command to display the status of a specific management protocol, or all protocols.

Syntax

`show protocol [ssh|telnet-client|ssh-client|https|snmp|telnet|http|scp |icmp|recovery-password|ftp-client|tftp|dhcp]`

Parameters

Parameter	Description	Possible Values	Default Value
`ssh`	Keyword indicating to display the status of the ssh protocol		
`telnet-client`	Keyword indicating to display the status of the telnet-client protocol		
`ssh-client`	Keyword indicating to display the status of the ssh-client protocol		
`https`	Keyword indicating to display the status of the https protocol		
`SNMP`	Keyword indicating to display the status of the SNMP protocol		
`telnet`	Keyword indicating to display the status of the telnet protocol		
`http`	Keyword indicating to display the status of the http protocol		
`scp`	Keyword indicating to display the status of the scp protocol		
			1 of 2

Parameter	Description	Possible Values	Default Value
icmp	Keyword indicating to display the status of the icmp protocol		
recovery-password	Keyword indicating to display the status of the recovery-password protocol		
ftp-client	Keyword indicating to display the status of the ftp-client protocol		
tftp	Keyword indicating to display the status of the tftp protocol		
dhcp	Keyword indicating to display the status of the DHCP protocol		
			2 of 2

User level

admin

Context

general

Example

To display information about all protocols:

```
G350-011(super)# show protocol
Protocols                          Status
------------                       --------
SSH-CLIENT                          ON
TELNET-CLIENT                       OFF
SNMPv1                              ON
SNMPv3                              ON
TELNET                              ON
HTTP                                ON
RECOVERY-PASSWORD                   ON
FTP-CLIENT                          ON
TFTP                                OFF
DHCP                                ON
```

show qos-rtcp

Use the **show qos-rtcp** command to display QoS and RTCP parameters.

Syntax

show qos-rtcp

User level

admin

Context

general

Example

To display QoS and RTCP information:

```
G350-001(super)# show qos-rtcp

PARAMETERS IN EFFECT: -- Downloaded --

QOS PARAMETERS          LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
Signal 802 Priority:    7                  0
Signal DSCP        :    34                 0
Bearer 802 Priority:    6                  6
Bearer BBE DSCP    :    43                 43
Bearer EF DSCP     :    46                 46
Minimum RTP Port   :    3                  2048
Maximum RTP Port   :    65535              65535

RSVP PARAMETERS         LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
State              :    Enabled            Disabled
Retry on Failure   :    Yes                Yes
Retry Delay(secs)  :    15                 15
Service Profile    :    Guaranteed         Guaranteed

RTCP MON  PARAMETERS    LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
State              :    Enabled            Disabled
IP Address         :    0.0.0.0            0.0.0.0
Listening Port     :    5005               5005
Report Period(secs):    5                  5
```

show queue

Use the **show queue** command to display information about the real-time status of output queues for the current interface.

Note:

This command is only applicable in fair-voip-queue mode.

Syntax

show queue *type identifier*

Parameters

Parameter	Description	Possible Values	Default Value
type	The type of interface	**Fast Ethernet** **Serial**	
identifier	The identifier depends on the interface type: For Fast Ethernet: ***module/port*** For Serial: ***module/port:channel-group***	channel-group: E1: **0-30** T1: **0-23**	

User level

read-only

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3) - when traffic shaping is configured

Examples

```
G350-001> show queue FastEthernet 10/2
```

```
G350-001> show queue Serial 3/1:2
```

show queueing

Use the **`show queueing`** command to display the priority queue size, in packets.

Syntax

`show queueing [`*`interface_type if_number`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`interface_type`	The type of interface	**Serial,** **Fast-Ethernet**	
`if_number`	The port number of this interface in the form: <port>[:<channel_group>]	port: **1, 2** channel_group: E1: **0-30** T1: **0-23**	

User level

read

Context

general

> **Note:**
>
> This command is also used for the FastEthernet interface when traffic shaping has been configured.

Example

```
G350-001> show queueing

Current priority queue configuration:


Interface     VOIP  Est. Delay    Q.1(High)  Q.2  Q.3  Q.4(Low)  DE
Name                [ms]                                         Buf

Serial 2/1    OFF   OFF           524        524  524  524       -

Serial 5/1:1  OFF   OFF           507        507  507  507       507
```

```
Current voip fair queue configuration:

  Interface      Total        Flow         Dynamic   Max voip    Priority
  Name           discard      discard      Queue     delay (ms)  queues
                 threshold    threshold

  Serial 3/1:1   256          64           16        20          1
```

Output fields

Field	Description
Total discard threshold	The total buffer credits limit for WFQ, configurable through **`fair-queue-limit`** command.
Flow discard threshold	Per subqueue buffer credits. Not configurable.
Dynamic queues	The total number of subqueues. Not configurable.
Max voip delay [ms]	Maximum delay for voip bearer. Configurable through the **`voip-queue-delay`** command.
Priority queues	The number of priority queues in the system. Not configurable. From the user's point of view control and bearer queues are the same queue.

show radius authentication

Use the **`show radius authentication`** command to display all RADIUS authentication configurations. Shared secrets are not displayed.

Syntax

`show radius authentication`

User level

read-only

Context

general

Example

To show RADIUS authentication information:

```
G350-001> show radius authentication
```

```
Mode:                  Disable
Primary-server:        0.0.0.0
Secondary-server:      0.0.0.0
Retry-number:          4
Retry-time:            5
UDP-port:              1812
```

show recovery

Use the **`show recovery`** command to show the media gateway monitoring and recovery setup.

Syntax

`show recovery`

User level

read-only

Context

general

Example

To show recovery information:

```
G350-011> show recovery
```

```
RECOVERY TIMES
--------------------------------
Primary Search  : 1
Total Search    : 30
Transition Point: 1
```

show restart-log

Use the **`show restart-log`** command to retrieve restart data that is stored in a log in flash memory.

Syntax

`show restart-log`

User level

read-only

Context

general

Example

To display restart information:

```
G350-011> show restart-log

RESET ID  MM/DD-hh:mm:ss.hs STR
---------- ------------------ ------------------------------------
0000000000 01/01-02:54:17.00 MgFw#:48.46.48 REBOOT
0000000000 01/01-02:54:12.00 MgFw#:48.46.48 WWD-STYCRINO-XXXXX REBOOT
from RecoveryEngineUti
EOF
```

show rmon alarm

Use the **`show rmon alarm`** command to display information about existing alarm entries. If no alarm index is specified, information for all alarms is displayed.

Syntax

`show rmon alarm [`*`alarm_index`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
alarm_index	The alarm about which to display information		

User level

read-only

Context

general

Example

To show information for all existing RMON alarms:

```
G350-001> show rmon alarm

alarm 1 is active, owned by billp
Monitors ifEntry.1.218106371 every 20 seconds
Taking delta samples, last value was 0
Rising threshold is 500, assigned to event # 1
Falling threshold is 100, assigned to event # 2
On startup enable rising or_falling alarms
```

show rmon event

Use the **show rmon event** command to display information about existing event entries. If no index is specified, information for all events is displayed.

Syntax

show rmon event [*event_index*]

Parameters

Parameter	Description	Possible Values	Default Value
event_index	The index of the event about which to display information		

User level

read-only

Context

general

Example

To display RMON event information for all events:

```
G350-001> show rmon event
```

```
Event 32 is active, owned by config
Description is resetTrap
Event firing causes trap to community public, last fired 0:0:0
```

show rmon history

Use the **show rmon history** command to display information about existing history entries. If no index is specified, information for all history entries is displayed.

Syntax

show rmon history [*history_index*]

Parameters

Parameter	Description	Possible Values	Default Value
history_index	The history entry about which to display information		

User level

read-only

Context

general

Example

To display RMON history information for entry 32:

```
G350-001> show rmon history 32
```

```
history
```

```
Entry 32 is active, owned by config
Monitors the port 10/2 every 20 seconds
Requested # of time intervals, ie buckets, is 100
Granted # of time intervals, ie buckets, is 100
Sample # 47 began measuring at 8:32:17
Received 664636 octets, 1912 packets,
2 broadcast and 0 multicast packets,
0 undersize and 0 oversize packets,
22 fragments and 0 jabbers,
0 CRC alignment errors and 3 collisions,
# of dropped packet events (due to a lack of resources): 0
Network utilization is estimated at 0
```

show rmon statistics

Use the **`show rmon statistics`** command to display traffic statistics for an interface. If no module is specified, information for all modules and ports is displayed.

Syntax

`show rmon statistics [`*`module/port`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`module`	The module number of the interface		
`port`	The port or range of ports of the interface		

User level

read-only

Context

general

Example

To display traffic statistics for all modules and ports:

```
G350-001> show rmon statistics
```

```
Statistics for switch is active, owned by Monitor
Received 1150436284 octets, 1344680977 packets,
3301887234 broadcast and 3286425893 multicast packets,
3088727251 undersize and 3613263278 oversize packets,
1062765319 fragments and 3882972139 jabbers,
1956639312 CRC alignment errors and 725598320 collisions,
# of dropped packet events (due to a lack of resources): 181377479
# of packets received of length (in octets):
64:1508486650, 65-127:3587014782, 128-255:1989866214,
256-511:378421598, 512-1023:2746475436, 1024-1518:3976219609,
```

show rtp-stat config

Use the **show rtp-stat config** command to display the RTP statistics application configuration.

Syntax

show rtp-stat config

User level

read only

Context

General

Example

To display the current configuration of the RTP statistics application:

```
G350-001(super)# show rtp-stat config

RTP Statistic: Enabled
QoS Trap: Enabled
QoS Fault Trap: Enabled
    Fault: 1
    Clear: 0
QoS Trap Rate Limiter:
    Token Interval: 10.00 seconds
    Bucket Size: 5
Session Table:
    Size: 128
    Reserved: 64
Min Stat Win: 50
```

Output Fields

Name	Description
RTP Statistic	Status of the RTP Statistics application. Possible values: ● Enabled. The application is enabled. ● Disabled. The application is disabled.
QoS Trap	QoS trap status. Possible values: ● Enabled. The RTP statistics application is configured to generate QoS traps when one or more QoS indicators were over their event thresholds in a terminated RTP stream. ● Disabled. The RTP statistics application is not configured to generate QoS traps.
QoS Fault Trap	QoS fault trap status. Possible values: ● Enabled. The RTP statistics application is configured to generate QoS fault traps when a specified number of active RTP sessions have QoS indicators over the configured thresholds and to send a QoS clear trap after a QoS fault trap when the number of active RTP sessions with QoS indicators over the configured thresholds reduces to a specified number. ● Disabled. The RTP statistics application is not configured to generate QoS fault and clear traps.
Fault	The configured minimum number of sessions suffering bad QoS to trigger the generation of a QoS fault trap
Clear	The configured maximum number of sessions that suffer from bad QoS to trigger the generation of a QoS clear trap
QoS Trap Rate Limiter:	
Token Interval	The configured interval, in hundredths of seconds, between additions of a token to the token bucket of the trap rate limiter. The trap rate limiter limits the rate at which QoS traps are sent to the SNMP trap manager on the media server. The trap rate limiter uses a token bucket scheme, in which the maximum number of QoS traps that can be sent is stored as a number of tokens in a virtual bucket. The number increments by one at a specified interval and is limited to a maximum by a specified bucket size.
Bucket Size	The maximum number of tokens stored in the token bucket of the trap rate limiter.
Session Table:	
Size	The maximum capacity of RTP session entries in the G350 history.
	1 of 2

Name	Description
Reserved	
Min Stat Win	The minimum statistic window configured for the RTP statistics application. That is, the minimum number of observed RTP sequence increments for which the application evaluates packet loss. Use the **no** form of this command to reset the minimum statistic window.
	2 of 2

show rtp-stat detailed

Use the **`show rtp-stat detailed`** command to display a detailed QoS log for a specific RTP session.

Note:

Use the **`show rtp-stat sessions`** command to view a list of all RTP sessions.

Syntax

```
show rtp-stat detailed session-id
```

Parameters

Parameter	Description	Possible Values	Default Value
session-id	The index of a specific RTP session		

User level

read only

Context

General

Example

To display RTP statistics for RTP session 35:

```
G350-001(super)#  show rtp-stat detailed 35

Session-ID: 35
Status: Active, QOS: Faulted, EngineId: 0
Start-Time: 2004-10-20,11:09:07, End-Time: -
Duration: 00:03:11
CName: gwp@135.8.118.252
Phone:
Local-Address: 135.8.118.252:2045 SSRC 154611212
Remote-Address: 135.8.76.107:2061 SSRC 2989801899 (0)
Samples: 38 (5 sec)

Codec:
G723 62B 30mS Off, Silence-suppression(Tx/Rx) Disabled/Not-Supported,
Play-Time
186.690sec, Loss 0.0% #1, Avg-Loss 0.1%, RTT 816mS #18, Avg-RTT 463mS,
JBuf-unde
r/overruns 0.2%/0.0%, Jbuf-Delay 60mS, Max-Jbuf-Delay 60mS

Received-RTP:
Packets 6372, Loss 0.0% #0, Avg-Loss 0.0%, RTT 603mS #18, Avg-RTT
267mS, Jitter
0mS #0, Avg-Jitter 0mS, TTL(last/min/max) 63/63/63, Duplicates 0,
Seq-Fall 0, DS
CP 46, L2Pri 12, RTCP 37

Transmitted-RTP:
VLAN 1, DSCP 184, L2Pri 6, RTCP 43

Remote-Statistics:
Loss 0.0% #0, Avg-Loss 0.0%, Jitter 0mS #0, Avg-Jitter 0mS
```

```
Echo-Cancellation:
Loss 45dB #1, Len 32mS

RSVP:
Status Disabled, Failures 0
```

Output Fields

Name	Description
Session-ID	The RTP Session ID
Status	The current session status. Possible values: ● Active ● Terminated
QoS status	The QoS status. Possible values: ● OK ● Faulted. One or more QoS event counters are over their thresholds.
EngineId	The VoIP engine used for the RTP session.
Start-Time	The start time of the RTP session
End-Time	The end time of the RTP session (empty for active calls)
Duration	The total duration of the RTP session
CName	Equals gwt@<MGP-address>
	1 of 5

Name	Description
Phone	The local extension number and conference ID. Format: *<ConferenceID>:<extensionID>* Format for N-parties conference call: *<ConferenceID>:<ExtensionId1><extensionId2>:... extensionIdN>* **Note:** This item is received from the CM if VMON is configured. **Note:** If VMON (RTCP server) is not present, the administrator can still cause the CM to send the “Phone” data by configuring a dummy RTCP server for the region (e.g., with a localhost IP address such as 127.x.x.x).
Local-Address	The local address for the RTP session. Format: *local gateway PMI or VoIP engine address*:*local UDP port*, SSRC *RTP SSRC field*
Remote-Address	The local address for the RTP session. Format: *remote VoIP engine address, gateway PMI, or IP phone address*:*remote UDP port*, SSRC *RTP SSRC field* (*number of observed SSRC changes(optional)*)
Samples	The number of times the application has sampled the VoIP engine (RTP receiver) statistics. The number in parentheses is the sample interval.
Codec:	
Codec	The codec used for the RTP session (for example, G.711, G.729), the codec packet size, in bytes (for example, 122B), the codec packet interval, in milliseconds (for example, 20ms), and the encryption method
Silence suppression (Tx/ Rx)	The transmitted silence suppression method/the received silence suppression method
Play-Time	The overall time the codec played valid received frames. This timer is not incremented when the codec plays fill frames (for example, during silence suppression conditions)
	2 of 5

Name	Description
Loss *codec-loss*% *#codec-loss-events*	The codec loss is the percentage of time the codec had to play a fill frames due to lack of valid RTP frames. Possible causes include jitter and packet loss. *codec-loss* is the last codec loss sample. *codec-loss-events* is the number of samples that were over the codec-loss threshold.
Avg-Loss	The average codec loss sample
RTT *rtt* ms *#rtt-events*	*rtt*: The last sample of the codec Round Trip Time (in milliseconds). Round Trip Time is the time taken for a message to get to the remote peer and back to the local receiver. In order to reflect the round-trip-delay experienced by the user, this metric includes the internal delay inside the G350 and the IP phone and an estimation of the remote internal delay. *rtt-events*: the number of samples that were over the RTT threshold.
Avg-RTT	The average Round Trip time
Jbuf-under/ overruns	The contribution of jitter-buffer underruns to the average codec loss/ the contribution of jitter-buffer overruns to the average codec loss
Jbuf-delay	The current/last jitter buffer delay, in milliseconds
Max-Jbuf-Delay	The maximum jitter buffer delay during the session
Received RTP:	
Packets	The total number of received RTP packets
Loss *loss*% *#loss-events*	*loss*: The last sample network RTP packet loss *loss-events*: the number of samples that were over the loss threshold The G350 VoIP engine evaluates the current received packet loss in fixed intervals of 6 to 12 seconds. The G350 VoIP engine postpones loss estimation until the next interval if the number of packets received is less than the minimum statistic window. The minimum statistic window is configured with the CLI command **`rtp-stat min-stat-win`**.
Avg-Loss	The average packet loss during the session
RTT *rtt* ms *#rtt-events*	*rtt*: The last network RTP packet round-trip-time sample. The system calculates RTT each time an RTCP packet is received. *rtt-events*: the number of samples that were over the RTT threshold
Avg-RTT	The average Round Trip Time during the session
Jitter *jitter* ms *#jitter-event*	*jitter*: The last sample of network jitter (at the RTP receiver) *jitter-event*: the number of samples that were over the network jitter threshold
	3 of 5

Name	Description
Avg-Jitter	The average network jitter during the session
TTL(last/min/max)	The last, minimum and maximum values of the TTL field of received RTP packets. TTL changes during the session may indicate IP routing instability.
Duplicates	This counter increments each time two consecutive RTP packets with the sample RTP sequence number are received.
Seq-Fall	This counter increments each time an RTP packet with a sequence number less than the last known sequence is received.
DSCP	The last received DSCP value of an RTP packet
L2Pri	The last received L2 priority (usually IEEE802.1p) value of an RTP packet
RTCP	The total number of received RTCP packets
Transmitted-RTP:	
VLAN	The VLAN-ID on which the RTP packets are transmitted
DSCP	The DSCP (diff-serve code point) of RTP packets
L2Pri	The Layer 2 priority (usually 802.1p) of transmitted RTP packets.
RTCP	The total number of transmitted RTCP packets
Remote-Statistics:	
Loss *rem-loss%* *#rem-loss-ev*	*rem-loss*: the network loss experienced by the remote RTP receiver. The local RTP receiver learns about its remote peer statistics from RTCP packets. *rem-loss*-ev: the number of samples that were over the rem-loss threshold.
Avg-Loss	The average network loss experienced by the remote RTP receiver.
Jitter *rem-jitter* *#rem-jitter-ev*	*rem-jitter*: the network jitter experienced by the remote RTP receiver. *rem-jitter-ev*: the number of samples that were over the remote jitter threshold.
Avg-jitter	The average remote jitter
Echo cancellation:	
Loss *loss* dbm *#loss-ev*	*loss*: the echo cancellation loss on the TDM bus. A high value may indicate impairment of DCP terminals. *loss-ev*: a counter that increments each time the Echo-cancellation loss is sampled below its threshold
	4 of 5

Name	Description
Len	The last echo-cancellation tail length used for this session
RSVP:	
Status	The current RSVP reservation state
Failures	The total number of reservation failures during the session
	5 of 5

show rtp-stat sessions

Use the **`show rtp-stat sessions`** command to display RTP sessions QoS statistics.

Syntax

```
show rtp-stat sessions [active|active-events|history|events]
[destination-ip {remote-subnet remote-subnet-mask}|{host rem-addr}]
[last last-N]
```

Parameters

Parameter	Description	Possible Values	Default Value
`active`	Displays only active sessions		
`active-events`	Displays only active sessions experiencing bad QoS conditions		
`history`	Displays only terminated sessions		
`events`	Displays only terminated sessions that experienced bad QoS conditions		
`destination-ip`	Displays only sessions to this destination subnet		
`remote-subnet`	The destination subnet		
			1 of 2

Parameter	Description	Possible Values	Default Value
remote-subnet-mask	The destination subnet mask		
host	Displays only sessions to this specific address		
rem-addr	The specific IP address		
last	Displays only the last *N* entries in the history		
last-N	The number of entries in the history to display		
			2 of 2

User level

read only

Context

General

Example

To display all RTP sessions:

```
G350-001(super)# show rtp-stat sessions
```

```
ID    QoS Start date and time End Time  Type      Destination
----- --- ------------------- --------  -------- ---------------
00001  *  2004-10-15,16:57:48 17:00:15   G729     135.8.76.64
00002     2004-10-15,16:59:06 17:00:15   G729     135.8.76.62
00003  *  2004-10-15,17:00:41 17:01:40   G723     135.8.76.107
00004  *  2004-10-18,10:28:33 10:30:29   G729     135.8.76.64
00005  *  2004-10-18,10:39:03 10:42:15   G723     135.8.76.107
00006  *  2004-10-18,10:52:26 10:53:15   G729     135.8.76.64
00007  *  2004-10-18,10:53:42 10:54:29   G723     135.8.76.107
00008  *  2004-10-18,10:56:31 10:57:34   G729     135.8.76.64
00009     2004-10-18,10:57:39 11:02:38   G729     135.8.76.64
```

```
00010     2004-10-18,11:03:13 11:06:07   G723     135.8.76.13
00011     2004-10-18,11:13:56 11:16:46   G723     135.8.76.35
00012     2004-10-18,11:13:58 11:16:46   G723     135.8.76.14
00013  *  2004-10-18,11:18:47 11:19:32   G723     135.8.76.107
00014  *  2004-10-18,11:18:50 11:19:59   G723     135.8.76.107
00015  *  2004-10-18,11:20:23 11:20:53   G723     135.8.76.107
00016  *  2004-10-18,11:21:04 11:21:55   G723     135.8.76.107
00017  *  2004-10-18,11:22:11 11:23:02   G729     135.8.76.64
00018     2004-10-18,11:22:42 11:23:02   G729     135.8.76.62
00019  *  2004-10-18,11:40:12 11:42:10   G723     135.8.76.107
00020  *  2004-10-18,11:46:43 11:50:33   G723     135.8.76.107
00021  *  2004-10-18,11:47:07 11:50:33   G723     135.8.76.107
00022  *  2004-10-18,11:47:27 11:50:31   G723     135.8.76.107
00023     2004-10-18,11:48:34 11:50:43   G723     135.8.76.35
00024     2004-10-18,11:48:34 11:50:43   G723     135.8.76.14
00025  *  2004-10-18,11:54:01 11:55:27   G723     135.8.76.13
00026  *  2004-10-18,11:54:02 11:55:27   G729     135.8.76.62
00027  *  2004-10-18,13:43:18 13:54:53   G723     135.8.76.107
00028  *  2004-10-18,13:56:57 08:40:39   G723     135.8.76.107
00029     2004-10-19,17:24:00 17:28:10   G711A    135.8.76.107
00030  *  2004-10-19,17:29:06 09:04:04   G723     135.8.76.107
00031     2004-10-20,10:51:36 10:59:07   G729     135.8.76.64
00032  *  2004-10-20,10:53:42 10:57:36   G723     135.8.76.107
00033  *  2004-10-20,10:58:21 10:59:06   G723     135.8.76.107
00034     2004-10-20,11:08:40        -   G729     135.8.76.64
00035     2004-10-20,11:09:07        -   G723     135.8.76.107
```

Note:

An asterisk (*) in the QoS column indicates that the session suffered from QoS problems.

To display the last five sessions:

```
G350-001(super)# show rtp-stat sessions last 5

ID    QoS Start date and time End Time Type    Destination
----- --- ------------------- -------- ------- ---------------
00031     2004-10-20,10:51:36 10:59:07 G729    135.8.76.64
00032  *  2004-10-20,10:53:42 10:57:36 G723    135.8.76.107
00033  *  2004-10-20,10:58:21 10:59:06 G723    135.8.76.107
00034     2004-10-20,11:08:40        - G729    135.8.76.64
00035  *  2004-10-20,11:09:07        - G723    135.8.76.107
```

show rtp-stat summary

Use the **show rtp-stat summary** command to display a summary of the RTP statistics.

Syntax

show rtp-stat summary

User Level

read-write

Context

General

Example

The following summary shows two active sessions, one with QoS problems (35):

```
G350-001(super)# show rtp-stat summary

Total QoS traps: 23
QoS traps Drop : 0
Qos Fault
Engine                            Active   Total    Mean      Tx
ID   Description     Uptime       Session  Session  Duration  TTL
---  --------------  -----------  -------  -------  --------  ----
000        internal  04,18:15:15    2/1     35/24   01:04:44   64
```

Output fields

Name	Description
ID	Number of the trap
Description	Description of the VoIP engine
Uptime	The uptime of the RTP statistics application. This is the time since the last boot or since the last use of the **`rtp-stat clear`** command.
Active Session	The number of active sessions / number of active sessions with QoS problems
Total Session	The total number of sessions / number of sessions that had QoS problems
Mean Duration	The mean RTP session duration
Tx TTL	The TTL field for transmitted RTP packets

show rtp-stat thresholds

Use the **`show rtp-stat thresholds`** command to display the configured thresholds and event-thresholds for QoS metrics sampled by the RTP statistics application during RTP streams. For a description of the thresholds, see rtp-stat threshold on page 281.

Syntax

`show rtp-stat thresholds`

User level

read only

Context

General

Example

To display the configured RTP statistics application thresholds:

```
G350-001(super)# show rtp-stat thresholds


Item                   Threshold      Event Threshold
--------------------  -------------  -----------------
```

```
Codec Loss            6.0%           1
Average Codec Loss    3.0%           N/A
Codec RTT             700mS          1
Echo Return Loss      0dB            1
Loss                  6.0%           1
Average Loss          3.0%           N/A
Remote Loss           6.0%           1
Average Remote Loss   3.0%           N/A
RTT                   500mS          1
Local Jitter          50mS           1
Remote Jitter         50mS           1
SSRC Changes          N/A            1
```

show running-config

Use the **`show running-config`** command to display the media gateway's current configuration.

Syntax

`show running-config`

User level

read-only

Context

general

Example

To display the current configuration:

```
G350-011> show running-config
```

```
G350-011>
! version 0.0.13
!
!
!
ds-mode t1
```

```
!
interface Vlan 1
icc-vlan
ip address 172.16.1.139    255.255.255.240
pmi
!
interface FastEthernet 10/2
!
interface Console
ip address  10.3.0.1  255.255.255.0
!
```

show snmp

Use the **show snmp** command to display SNMP configuration information.

Syntax

show snmp

User level

read-only

Context

general

Example

To display SNMP information:

```
G350-001> show snmp


 Community-Access  Community-String
 read-only         public
 read-write        private
 trap              secret


 Trap-Rec-Addr         Status    Traps configured
```

```
SNMPv3 Notifications Status
Traps: Disabled
Informs: Disabled      Retries: 3   Timeout: 3 seconds

SNMP Rec-Addr     Model  Level   Notification   Trap/    User
                                                Inform   Name
129.22.22.22      v1     noauth  all            trap     ReadCommN
UDP port: 162 DM
129.11.33.44      v2c    noauth  all            inform   WriteCommN
UDP port: 162
```

show snmp engineID

Use the **`show snmp engineID`** command to display the SNMP engine ID for the G350.

Syntax

`show snmp endingid`

User level

admin

Context

general

Example

To display the SNMP engine ID:

```
G350-001(super)# show snmp engineid
EngineId: 00:00:00:09:00:d0:00:4c:18:00
Engine Boots: 1234455
```

show snmp group

Use the **`show snmp group`** command to display configuration information about the SNMP groups.

Syntax

`show snmp group`

User level

admin

Context

general

Example

```
G350-001(super)# show snmp group
```

```
Group Name: defaultROgroup Context:
Security Model: v1
Security Level: noauth
Context Match: exact
Read View: defaultUserView
Write View:
Notify View: defaultUserView
Group Name: defaultROgroup Context:
Security Model: v2c
Security Level: noauth
Context Match: exact
Read View: defaultUserView
Write View:
Notify View: defaultUserView
```

show snmp retries

Use the **`show snmp retries`** command to display the number of retry attempts to make when attempting to communicate with a node.

Syntax

`show snmp retries`

User level

read-only

Context

general

Example

To display the number of retry attempts:

```
G350-001> show snmp retries
the SNMP Retries Number is 100
```

show snmp timeout

Use the **`show snmp timeout`** command to display the time to wait before resending a communication.

Syntax

`show snmp timeout`

User level

read-only

Context

general

Example

To display the timeout value:

```
G350-001> show snmp timeout
the SNMP Timeout is 60
```

show snmp user

Use the **show snmp user** command to display configuration information for the specified SNMP user.

Syntax

show snmp user *username* [*remote EngineID*]

Parameters

Parameter	Description	Possible Values	Default Value
username	The username of the user whose information you wish to display		
remote EngineID	The EngineID of the remote user		

User level

admin

Context

general

Example

```
G350-001(super)# show snmp user <john>
```

```
EngineId: 00:11:22:33:44
User Name: john
Authentication Protocol: md5
Privacy Protocol: des56
Group for Security Model v1:  RestrictedGroup
Group for Security Model v2:  RestrictedGroup
Group for Security Model v3:  RestrictedGroup
Storage Type: volatile
Row status: active
```

show snmp usertogroup

Use the **`show snmp usertogroup`** command to show the mapping table between SNMPv3 users and groups.

Syntax

`show snmp usertogroup [`*`username`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
username			

User level

admin

Context

general

Example

```
G350-001(super)# show snmp usertogroup

Security Model: v1
Security Name: WriteCommN
Group Name: WriteCommG

Security Model: v2c
Security Name: ReadCommN
Group Name: ReadCommG

Security Model: v2c
Security Name: WriteCommN
Group Name: WriteCommG
```

show snmp user summary

Use the **show snmp user summary** command to display configuration information for all SNMP users.

Syntax

show snmp user summary

User level

admin

Context

general

show snmp view

Use the **show snmp view** command to display configuration information for all SNMP views.

Syntax

show snmp view

User level

admin

Context

general

Example

```
G350-001(super)# show snmp view
```

```
View Name: iso
Subtree Oid: 1
Subtree Mask:
View Type: include
Storage Type: nonVolatile
Status: active
```

show spantree

Use the **`show spantree`** command to display spanning-tree information. If no port is specified, information for all ports is displayed.

Syntax

`show spantree [`*`module`*`[/`*`port`*`]``]`

Parameters

Parameter	Description	Possible Values	Default Value
`module`	Number of the module		
`port`	Number of the port on the module		

User level

read-only

Context

general

Example

To display spanning tree information for all ports:

```
G350-001> show spantree
```

```
Spanning tree enabled
Designated Root:  00-40-0d-88-06-c8
Designated Root Priority: 32768
Designated Root Cost: 20
Designated Root Port: 1/1
Root Max Age: 20   Hello Time: 2

Bridge ID MAC ADDR: 00-40-0d-92-04-b4
Bridge ID priority: 32768

Port   State         Cost       Priority
------ ------------- ---------- ------------
4 /1   Forwarding    20         128
4 /2   not-connected 20         128
4 /3   LAG-member    20         128
4 /4   LAG-member    20         128
4 /5   not-connected 20         128
4 /6   not-connected 20         128 ...
```

Output fields:

Field	Description
`Spanning tree`	Spanning-Tree Protocol status (enabled or disabled)
`Designated root`	MAC address of the designated spanning-tree root bridge
`Designated Root Priority`	Priority of the designated root bridge
`Designated Root Cost`	Total path cost to reach the root
`Designated Root Port`	Port through which the root bridge can be reached (shown only on non root bridges)
`Root Max Age`	Amount of time a BPDU packet should be considered valid
`Hello Time`	Number of times the root bridge sends BPDUs
`Bridge ID MAC ADDR`	Bridge MAC address used in the sent BPDUs
`Bridge ID Priority`	Bridge Priority
`Port`	Port number
`Port-State`	Spanning-tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent)
`Cost`	Cost associated with the port
`Priority`	Priority associated with the port

show startup-config

Use the **`show startup-config`** command to show the NVRAM based configuration loaded automatically at startup.

Syntax

```
show startup-config
```

User level

read-only

Context

general

Example

To display the startup configuration:

```
G350-011> show startup-config
```

```
G350-011>
! version 0.0.13
ds-mode t1
interface Vlan 1
icc-vlan
ip address 172.16.1.139    255.255.255.240
pmi
interface FastEthernet 10/2
interface Console
ip address  10.3.0.1  255.255.255.0
```

show status

Use the **show status** command to display the status of the current file copy process to or from the device.

Syntax

show {download | upload} {software [*mmID*] | config} status

Parameters

Parameter	Description	Possible Values	Default Value
download	Keyword specifying that the download status is displayed		
upload	Keyword specifying that the upload status is displayed		
software	Keyword specifying that software download or upload information is displayed		
mmId	The Media Module ID number		
config	Keyword specifying that configuration download or upload information is displayed		

User level

read-only

Context

general

Example

To display the status of software downloads for all media modules:

```
G350-001# show download software status
```

```
TFTP STATUS
---------------------------------------------
Module: MGP
Source File: mg01_3.com
Destination File: BANK B
Host: 0.0.0.0
Running State: idle
Last Failure: No Error
Last Warning: (null)
Progress: [0/0]0%
```

show sync timing

Use the **`show sync timing`** command to display the status of the primary, secondary, and local clock sources.

Syntax

`show sync timing`

User level

read-only

Context

general

Example

To display clock source information:

```
G350-001# show sync timing
```

```
SOURCE     MM                   STATUS                   FAILURE
---------  -------------------  -----------------------  -----------
Primary                         Not Configured
Secondary                       Not Configured
Local      v0                   Active                   None

Active Source: v0               Sync Source Switching: Enabled
```

show system

Use the **show system** command to display information about the device.

Syntax

show system

User level

read-only

Context

general

Example

To display device information:

```
G350-001# show system
System Name         :
System Location     :
System Contact      :
Uptime (d,h:m:s)    : 0,7:36:43
MV Time             : N/A
MAC Address         : 00:04:0d:29:c5:11
WAN MAC address     : 00:04:0d:29:c5:10
Serial No           : 03IS12345678
Model No            : G350 Chassis
HW Vintage          : 00
HW Suffix           : B
FW Vintage          : 0.0.15
```

show temp

Use the **show temp** command to view the device temperature.

Syntax

show temp

User level

read-only

Context

general

Example:

To display temperature information:

```
G350-011> show temp
```

```
Ambient
-------
Temperature : 40C
High Warning: 45C
Low Warning : -5C
```

show timeout

Use the **`show timeout`** command to display the amount of time in minutes the terminal remains idle before timing out. If the timeout value is 0, there is no timeout limit. The default timeout value is 15 minutes.

Syntax

`show timeout`

User level

read-only

Context

general

Example

To display the timeout value:

```
G350-001> show timeout
```

```
CLI timeout is 15 minutes
```

show trunk

Use the **`show trunk`** command to display VLAN tagging information for the media gateway. If no port is specified, information for all ports is displayed.

Syntax

`show trunk [`*`module`*`[/`*`port`*`[-`*`port`*`]]]`

Parameters

Parameter	Description	Possible Values	Default Value
module	Number of the module		
port	Number of the port on the module. You can specify a range of ports. For example, use the syntax 4/1-3 to specify ports 1 through 3 on module 4.		

User level

read-only

Context

general

Example

To display binding information for ports 1-3 of module 4:

```
G350-001# show trunk 4/1-3
```

```
Port   Mode  Binding mode Native vlan Vlans allowed on trunk
------ ----- --------------- ----------- ----------------
Port   Mode  Binding mode Native vlan Vlans allowed on trunk
------ ----- --------------- ----------- ----------------------
Port   Mode  Binding mode Native vlan Vlans allowed on trunk
------ ----- --------------- ----------- ----------------------
4/3   off   statically bound 1       1
```

Output fields:

Field	Description
Port	Module and port numbers
Mode	VLAN tagging status of the port. Possible values: ● **dot1q** - the port uses dot1Q tagging mode ● **off** - the port uses clear tagging mode
Binding mode	Binding mode of the port. Possible values: ● **statically bound** ● **bound-to-configured**
Native vlan	Number of the Port VLAN ID. This is the VLAN to which received untagged traffic is assigned.

show upload dhcp-binding-file status

Use the **`show upload dhcp-binding status`** command to display the upload status of a DHCP binding file.

Syntax

```
show upload dhcp-binding-file status
```

User level

read only

Context

configure

Example

If no download was done:

```
G350-001# show upload dhcp-binding-file status
Module #10
===========
No dest file for download operation - no download operation was done.
```

If download was done:

```
G350-001# show upload dhcp-binding-file status
```

```
Module #10

===========

Module : 10
Source file : dhcp-binding
Destination file : bbbb
Host : 135.64.102.64
Running state : Idle
Failure display : (null)
Last warning : No-warning
```

show upload phone-script-file status

Use the **show upload phone-script-file status** command to display the upload phone-script file.

Syntax

show upload phone-script-file status

User level

Read only

Context

general

Example

```
interface# > show upload phone-script-file status
```

- If no upload has been performed

  ```
  Module #10

  ===========

  No source file for upload operation - no upload operation was done.

  =============================
  ```

- If an upload has been performed

```
Module #10
===========
Module           : 10
Source file      : phone-scriptA
Destination file : d:\lou\run.cfg
Host             : 135.64.102.39
Running state    : Idle
Failure display  : SCP - Permission denied
Last warning     : No-warning
==============================
```

show upload status

Use the **`show upload status`** command to display status information regarding the upload of a configuration file for a specific module or for all modules.

Syntax

`show upload status [`*`module_number`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`module_number`	The module number for which to display upload information	**0 – 10**	

User level

read-only

Context

general

Example

To display upload status information for module 10:

```
G350-001> show upload status 10
```

```
Module #10
===========
No source file for upload operation - no upload operation was done.
```

show username

Use the **`show username`** command to display local user accounts.

Syntax

`show username`

User level

admin

Context

general

Example

To display all the defined user accounts:

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

```
User account   password   access-type

-----------  --------  ------------
root          *****     admin
gkohll        *****     read-only
readwrite      *****      read-write
```

show utilization

Use the **`show utilization`** command to display information about CPU usage. If no module is specified, information for all modules is displayed.

Syntax

`show utilization [`*`module`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
module	Module to display		

User level

read-write

Context

general

Example

To display utilization information for all modules:

```
G350-011# show utilization
Mod   CPU      CPU     RAM      RAM

      5sec     60sec   used(%)  Total(Kb)
---   ------   -----  -------  ----------
10       4%       4%    21%     105313 Kb
```

show vlan

Use the **show vlan** command to display the VLANs configured in the media gateway. If no VLAN is specified, information for all VLANs is displayed.

Syntax

show vlan [*vlan_id* | name *vlan_name*]

Parameters

Parameter	Description	Possible Values	Default Value
vlan_id	VLAN number to display	**1 – 3071**	
name	Keyword indicating to specify the VLAN by name		
vlan_name	VLAN name to display		

User level

read-only

Context

general

Example

To display information for all VLANs:

```
G350-001> show vlan

VLAN ID Vlan-name
------- --------------------------------
1       v1
5       V5
10      V10
15      V15
20      V20
25      V25
```

To display information for VLAN 1:

```
G350-001# show vlan 1

VLAN ID Vlan-name
------- --------------------------------
1       V1

Switch Ports currently bound to this vlan:
In module 10: 3
Switch Ports statically bound to this vlan:
None
```

show voip-parameters

Use the **show voip-parameters** command to display information about the current VoIP engine.

Syntax

show voip-parameters

User level

read-only

Context

general

Example

To display VoIP information:

```
G350-001> show voip-parameters
```

```
VOIP ENGINE PARAMETERS
---------------------------------------------------------
IP (PMI)            : 172.16.1.139
DSP Firmware Version: 200
Fault Status        : No Fault Messages
Additional Status   : No Status Messages

CURRENT STATE
---------------------------------------------------------
In Use     : 0 channels, 0 of 32 resources
DSPs State : Idle
Admin State: Release
```

show voltages

Use the **show voltages** command to view power supply voltages.

Syntax

show voltages

User level

read-only

Context

general

Example

To display voltage information:

```
G350-011> show voltages
Voltage Actual  Status  Usage
------- ------  ------  -----
-48.0   -48.761 OK     5V DC2DC, Analog/DCP ports, Fans
5.0     4.947  OK      3.3V DC2DC,1.8V DC-to-DC,Modules logic,
TDM buses TSI
```

```
3.3     3.277  OK      2.5V voltage regulator, Motherboard logic
2.5     2.533  OK      CPU & companion chip I/O
1.8     1.787  OK      1.6V voltage regulator,
CPU & companion chip core
1.6     1.583  OK      VoIP DSP
```

show web aux-files-url

Use the **`show web aux-files-url`** command to display the URL of the Web server containing online help files and the Java plug-in.

Syntax

`show web aux-files-url`

User level

read-only

Context

general

Example

To display the URL of the Web server:

```
G350-001> show web aux-files-url
```

```
the web aux-files-url is http://176.2.3.66/DMweb
```

shutdown

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 for the interface to up.

Syntax

`[no] shutdown`

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, DS1 FR-SUB L2-L3, DS1 FR-SUB L2, USP PPP L2, USP PPP L2-L3, USP FR L2, USP FR-SUB L2, USP FR-SUB L2-L3), FastEthernet (L2, L2-L3), VLAN (L2-L3, L2), Console, Loopback (L2-L3, L2), Controller, Tunnel (L2-L3, L2)

Example

To shutdown the VLAN 2 interface:

```
G350-001(if:Vlan 2)# shutdown
```

```
Interface Vlan 2, changed state to administratively down
Line protocol on Interface Vlan 2, changed state to down
Done!
```

shutdown

Use the **shutdown** command to disable the usb-modem interface. When the interface is disabled, calls to the modem are immediately hung up. No PPP initialization is performed, and there is no access to the device.

Use the **no** form of this command to enable the usb-modem interface. For security reasons, the usb-modem interface is disabled by default. The USB modem can only be connected after the interface is manually brought up using this command.

Syntax

[no] shutdown

User level

For **shutdown**: read-write

For **no shutdown**: admin

Context

interface usb-modem

Example

```
G350-001(super-if:USB-Modem)# shutdown
```

Done!

snmp trap link-status

Use the **`snmp trap link-status`** command to enable Link Up and Link Down traps. Use the **no** form of this command to restore the default value, interface traps deactivated.

Syntax

```
[no] snmp trap link-status
```

User level

read-write

Context

Interface: Serial (DS1 PPP L2, DS1 PPP L2-L3, DS1 FR L2, DS1 FR-SUB L2, DS1 FR-SUB L2-L3, USP PPP L2, USP PPP L2-L3, USP FR L2), FastEthernet (L2, L2-L3), Tunnel (L2, L2-L3)

snmp-server community

Use the **`snmp-server community`** command to enable access to SNMP services via community strings. Use the **no** form of the command to prevent access to SNMP services using community strings. By default, community string access is enabled.

Syntax

```
[no] snmp-server community
```

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server community
Done!
```

snmp-server dynamic-trap-manager

Use the **`snmp-server dynamic-trap-manager`** command to modify the SNMP settings of the dynamic trap manager. Use the **no** form of the command to restore the dynamic trap manager to its default settings, and remove all notification type filters.

Syntax

`snmp-server dynamic-trap-manager {traps | informs} {v1 | v2c` ***`community`*****`}`** **`[udp-port`** ***`port`*****`] [`*****`notification_type_list`*****`]`**

`no snmp-server dynamic-trap-manager` ***`notification_type_list`***

Parameters

Parameter	Description	Possible Values	Default Value
`traps`	Specifies that the dynamic trap manager sends messages without requesting acknowledgement. This is the default.		
`informs`	Specifies that the dynamic trap manager sends messages requiring acknowledgement.		
`v1`	Specifies that the dynamic trap manager uses SNMP v1 functionality. This is the default.		
`v2c`	Specifies that the dynamic trap manager uses SNMP v2c functionality.		
`community`	The community string for accessing SNMP services.		
port	The udp port of the SNMP host.		
`notification_type_list`	The specific types of messages that the dynamic trap manager sends. Use this list to filter the messages controlled by the dynamic trap manager.		All

User Level

admin

Context

general

Example

`G350-001`(super)# snmp-server dynamic-trap-manager 10.1.2.4 traps v2c public all

snmp-server enable notifications

Use the **`snmp-server enable notifications`** command to enable the sending of all traps and informs from the G350. Use the **no** form of the command to disable the sending of all traps and informs from the G350.

Note:
This command overrides the enabling of individual notifications using the **`snmp-server host`** command.

Syntax

```
[no] snmp-server enable notifications
```

User level

admin

Context

general

Example

`G350-001`(super)# snmp-server enable notifications

Done!

snmp-server engineID

Use the **`snmp-server engineID`** command to specify the SNMP Engine ID for the G350. Use the **no** form of the command to return the device to its default Engine ID.

Note:
The SNMP Engine ID must be unique for all devices on the network.

Note:
When you change the SNMP Engine ID, all users other than the default user are invalidated and must be redefined.

Note:

When the IP address of the G350 changes, the SNMP Engine ID is automatically changed.

Syntax

```
snmp-server engineID engineID
```

```
no snmp-server engineID
```

Parameters

Parameter	Description	Possible Values	Default Value
engineID	12 byte hexadecimal string, with each byte separated by a colon. For example, 00:00:00:81:0a:fe:ff:12:97:33:45:12.		

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server engineid 00:02:00:81:00:d0:00:4c:18:00
Done!
```

snmp-server group

Use the `snmp-server group` command to define a new SNMPv3 group, or to configure settings for the group. An SNMP group associates users with views. Use the **no** form of the command to remove the specified group.

Note:

If you use the **no** form of the command with no additional parameters, all instances of the specified group are removed. If you specify a particular security group, only that group instance is removed.

Syntax

```
snmp-server group groupname {v1|v2c|v3 {auth|noauth|priv}} [read
readviewname] [write writeviewname] [notify notifyviewname]
```

```
no snmp-server group groupname [v1|v2c|v3 {noauth|auth|priv}]
```

Parameters

Parameter	Description	Possible Values	Default Value
groupname	A character string of at most 32 characters specifying the group name		
v1	The group is limited to SNMP v1 functionality		
v2c	The group is limited to SNMP v2c functionality		
v3	The group has full SNMP v3 functionality (this is the default)		
auth	The group authenticates packets		
noauth	The group does not authenticate packets (this is the default)		
priv	The group authenticates and encrypts packets		
readviewname	A character string of at most 64 characters specifying the view name for the read view. Users of this group have read access to the set of MIB objects specified in the read view. If no view is specified, the default is an empty view.		
writeviewname	A character string of at most 64 characters specifying the view name for the write view. Users of this group have write access to the set of MIB objects specified in the write view. If no view is specified, the default is an empty view.		
notifyviewname	A character string of at most 64 characters specifying the view name for the notify view. Users of this group have notify access to the set of MIB objects specified in the notify view. If no view is specified, the default is an empty view.		

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server group 12groupRO v3 auth read view1 notify
view2
```

```
Done!
```

snmp-server host

Use the **`snmp-server host`** command to identify an SNMP management server, and specify the kind of messages it receives. Use the **no** form of the command to remove the specified server, or to disable a particular set of notification types.

Note:

If you specify no snmp-server host without a notification type list, all notification types are disabled.

Syntax

```
snmp-server host {host_address | hostname} {traps | informs} {{{v1 |
 v2c} community} | {v3 [auth | noauth | priv] user}} [udp-port port]
 [notification-type-list]
```

```
no snmp-server host host_address [{traps|informs}
 notification-type-list]
```

Parameters

Parameter	Description	Possible Values	Default Value
host_address	IP address of the SNMP host		
hostname	A character string no longer than 32 characters, specifying the hostname of the SNMP host		
			1 of 3

Parameter	Description	Possible Values	Default Value
`traps`	Send traps to this host (messages not requiring acknowledgement). This is the default.		
`informs`	Send informs to this host (messages requiring acknowledgement)		
`v1`	Use SNMP v1 functionality with this host		
`v2c`	Use SNMP v2c functionality with this host		
`community`	The community string to use to connect to the specified host (for v1 or v2c)		
`v3`	Use SNMP v3 functionality with this host		
`auth`	Authenticate messages to this host		
`noauth`	Do not authenticate messages to this host (this is the default)		
`priv`	Authenticate and encrypt messages to this host		
`user`	The username to use for authentication on the specified host		
`port`	Which port of the target host to use		**162**
			2 of 3

Parameter	Description	Possible Values	Default Value
notification-type-list	List of notification types that are enabled for this host. Use the no form of the command to disable specific notification types. The default is none.	**all** — all traps **generic** — generic traps **hardware** — hardware faults **rmon** — RMON rising/falling alarm **dhcp server** — DHCP server error **dhcp-clients** — DHCP client error **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 **security** — security traps **config** — configuration change notifications **eth-port-faults** — notifications of Ethernet port faults **sw-redundancy** — software redundancy notifications **temperature** — temperature warning notifications **cam-change** — notifications about changes in CAM **l3-events** — notifications about L3 faults (duplicate IP, VLAN violations) **lag-event** — notifications about link aggregation faults and configuration changes **policy** — notifications about changes in policy (for L3 devices) **link-faults** — link-down notifications **supply** — power supply notifications	**all**
			3 of 3

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server host 10.1.2.4 informs v3 auth John
udp-port 789 config generic
```

```
Done!
```

snmp-server informs

Use the **snmp-server informs** command to configure settings for SNMP inform messages.

Syntax

snmp-server informs [retries *retries*] [timeout *timeout*] [pending *pending*]

Parameters

Parameter	Description	Possible Values	Default Value
retries	The maximum number of times to resend an inform message		3
timeout	The number of seconds to wait for an acknowledgement before resending an inform message		3
pending	The maximum allowable number of inform messages that can be waiting for acknowledgement at any given time. When the maximum is reached, the oldest pending inform messages are discarded.		25

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server informs retries 5 timeout 3
Done!
```

snmp-server remote-user

Use the **`snmp-server remote-user`** command to configure settings for a remote SNMPv3 user. If the user does not exist, it is created. Use the **no** form of the command to remove the user from specific groups. If no groups are specified, the user is removed from all groups.

Syntax

`snmp-server remote-user` ***`username SNMPEngineID groupname`*** **`{v1|v2c|v3} [auth {md5|sha}`** ***`auth-password`*** **`[`*****`priv des56 priv-password`*****`]]`**

`no snmp-server remote-user` ***`username`*** **`[`*****`groupname`*** **`{v1|v2c|v3}]`**

Parameters

Parameter	Description	Possible Values	Default Value
username	A character string no longer than 32 characters, specifying the username of this user		
SNMPEngineID	The remote device Engine ID for this user		
groupname	A character string no longer than 32 characters, specifying the groupname this user is associated with		
v1	The user is authorized for SNMP v1 functionality in the specified group		
v2c	The user is authorized for SNMP v2c functionality in the specified group		
v3	The user is authorized for SNMP v3 functionality in the specified group		
auth			
md5	Use the MAC-MD5-96 authentication protocol		
			1 of 2

Parameter	Description	Possible Values	Default Value
sha	Use the HMAC-SHA-96 authentication protocol		
auth-password	A character string no longer than 64 characters specifying the authentication password. An authentication password is required if the auth keyword is used. The minimum length is 8 characters.		
priv			
des56			
priv-password	A character string no longer than 64 characters specifying the privacy password. The minimum length is 8 characters.		
			2 of 2

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server remote-user john
 00:02:00:81:00:d0:00:4c:18:00 L2Group
```

```
Done!
```

snmp-server user

Use the **snmp-server user** command to configure settings for an SNMPv3 user. If the user does not exist, it is created. Use the **no** form of the command to remove the user from specific groups. If no groups are specified, the user is removed from all groups.

Syntax

```
snmp-server user username groupname {v1|v2c|v3} [auth {md5|sha}
 auth-password [priv des56 priv-password]] [volatile]
```

```
no snmp-server user username [groupname {v1|v2c|v3}]]
```

Parameters

Parameter	Description	Possible Values	Default Value
username	A character string no longer than 32 characters, specifying the username of this user		
groupname	A character string no longer than 32 characters, specifying the groupname this user is associated with		
v1	The user is authorized for SNMP v1 functionality in the specified group		
v2c	The user is authorized for SNMP v2c functionality in the specified group		
v3	The user is authorized for SNMP v3 functionality in the specified group		
md5	Use the MAC-MD5-96 authentication protocol		
sha	Use the HMAC-SHA-96 authentication protocol		
auth-password	A character string between 8 and 64 characters specifying the authentication password. An authentication password is required if the auth keyword is used. The minimum length is 8 characters.		
priv-password	A character string between 8 and 64 characters specifying the privacy password. The minimum length is 8 characters.		
volatile	Specifies that the user configurations are only set temporarily, until the system is reset. After reset, the user settings return to their previous values.		

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server user john L2Group v3 auth md5 katmandu
 priv des56 uktanatan
```

```
Done!
```

snmp-server view

Use the **`snmp-server view`** command to configure settings for an SNMP MIB view. If the view does not exist, it is created. A MIB view specifies a particular section or subsection of the MIB tree. You can create a view that includes a particular subsection, or excludes one.

Syntax

```
snmp-server view viewname oidtree {included|excluded}
```

```
no snmp-server view viewname [oidtree]
```

Parameters

Parameter	Description	Possible Values	Default Value
`viewname`	The name of the view		
`oidtree`	The subtree to be included in or excluded from this view. Oidtree is specified as a series of period-separated numbers. In order to include a subtree family, use an asterisk as a wildcard character. Symbolic MIB object names are not supported.		
`included`	Keyword indicating that the view includes the specified subtree (this is the default).		
`excluded`	Keyword indicating that the view excludes the specified subtree.		

User level

admin

Context

general

Example

```
G350-001(super)# snmp-server view internet 1.3.6.1 included
```

```
Done!
```

source-ip

Use the **`source-ip`** command to indicate that the current rule applies to packets from the specified source IP address. Use the **no** form of the command to indicate that the current rule applies to all packets *except* those coming from the specified IP address.

Syntax

```
[no] source-ip {host ip_address | any | ip_address wildcard}
```

Parameters

Parameter	Description	Possible Values	Default Value
`host`	Keyword that indicates a specific host IP address		
`ip_address`	The IP address of packets to which the rule is applied		
`any`	Keyword that indicates any IP address		
`wildcard`	A range of IP addresses		

User level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule, ip crypto-list ip-rule

Example

To specify that rule 22 of QoS policy list 460 applies to any packet coming from IP address 135.64.104.102:

```
G350-110(QoS 460/rule 22)# source-ip host 135.64.104.102
```

speed

Use the **speed** command to set the PPP baud rate to be used by asynchronous PPP ports.

Note:

The peer baud-rate must be set to the same value.

Syntax

```
speed speed_rate
```

Parameters

Parameter	Description	Possible Values	Default Value
speed_rate	The PPP baud rate	**9600,** **19200,** **38400**	**38400**

User level

read-write

Context

Interface: Console, USB-modem

Example

To set the PPP baud rate to 9600:

```
G350-001(if:CON)# speed 9600
```

speed

Use the **speed** command to control the speed setting for the interface.

Note:

This command functions only in **no autoneg** mode.

Syntax

```
speed speed_rate
```

Parameters

Parameter	Description	Possible Values	Default Value
`speed_rate`	The interface speed	**10MB, 100MB**	

User level

read-write

Context

Interface: FastEthernet (L2, L2-L3)

Example

To set the interface speed to 100MB:

```
G350-001(if:FastEthernet 10/2)# speed 100MB
```

start-ip-addr

Use the **`start-ip-addr`** command to set the start IP address of a DHCP pool. For manual/ reservation leasing, set the start IP address to be identical to the end IP address. Use the **no** form of this command to clear the start IP address of the pool. Since there is a combined limit of 256 IP addresses for all pools, clear both the start and end IP addresses in a pool using the **no** forms of **`start-ip-addr`** and **`end-ip-addr`** before you configure a new range.

Syntax

`[no] start-ip-addr` ***`ip-addr`***

Parameters

Parameter	Description	Possible Values	Default Value
`ip_addr`	The start IP address of the DHCP pool	The start IP address must be smaller than the end IP address. The number of IP addresses in one pool cannot exceed 256.	**0.0.0.0**

User level

read-write

Context

dhcp pool

Example

```
G350-001(DHCP 5)# start-ip-addr 135.64.120.2
```

subnet-mask

Use the **subnet-mask** command to set the subnet mask of a DHCP pool. Use the **no** form of this command to reset the subnet mask of the pool to default.

Syntax

[no] subnet-mask {*mask*|*prefix-length*}

Parameters

Parameter	Description	Possible Values	Default Value
mask	The subnet mask of the DHCP pool	**255.0.0.0 - 255.255.255.0**	**255.255.255.0**
prefix-length	The prefix length of subnet mask	**8-32**	**24**

User level

read-write

Context

dhcp pool

Example

To set the subnet-mask for DHCP pool 5 to 255.255.255.240:

```
G350-001(DHCP 5)# subnet-mask 255.255.255.240
```

To set the subnet-mask for DHCP pool 5 to 255.255.255.240 by stating the subnet mask prefix:

```
G350-001(DHCP 5)# subnet-mask 28
```

tcp destination-port

Use the **`tcp destination-port`** command to define a destination port with the TCP protocol for which to apply the current rule. Use the **`no`** form of the command to specify that the rule applies to all ports other than the defined port.

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

```
tcp destination-port any | {{eq | lt | gt}
{port_name | port_number}} | {range start_port end_port}
```

Parameters

Parameter	Description	Possible Values	Default Value
`any`	Keyword that specifies to apply the rule to a port with any name or number		
`eq`	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
`lt`	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
`gt`	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
`port_name`	The name of the port for which to apply the rule		
`port_number`	The number of the port for which to apply the rule		
`range`	Keyword indicating that a range of ports is specified		
			1 of 2

Parameter	Description	Possible Values	Default Value
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		
			2 of 2

User level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule

Example

To specify that the current rule applies to all packets whose destination port is 300:

```
G350-001(ACL 330/ip rule 22)# tcp destination-port eq 300
```

tcp established

Use the **`tcp established`** command to specify that the current rule applies only to packets that are part of an established TCP session. Use the **no** form of the command to specify that the current rule applies to any TCP packets.

Note:

> The **`tcp established`** and **`no tcp established`** commands also set the IP protocol to TCP.

Syntax

```
[no] tcp established
```

User level

read-write

Context

ip access-control-list ip-rule

Example

To specify that rule 27 applies only to packets from an established TCP session:

```
G350-001(ACL 330/ip rule 27)# tcp established
Rule protocol changed.
```

tcp source-port

Use the **`tcp source-port`** command to define a source port with the TCP protocol for which to apply the current rule. Use the **no** form of the command to specify that the rule applies to all ports other than the defined port.

Note:

Issuing this command also sets the protocol to be TCP, if it is not already.

Syntax

```
[no] tcp source-port any | {{eq | lt | gt} {port_name | port_number}}
| {range start_port end_port}
no tcp source-port
```

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
			1 of 2

Parameter	Description	Possible Values	Default Value
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		
			2 of 2

User level

read-write

Context

ip pbr-list ip-rule, ip capture-list ip-rule, ip qos-list ip-rule, ip access-control-list ip-rule

Example

To specify that rule 22 applies to all packets whose source port is greater than 95:

```
G350-001(ACL 330/ip rule 22)# tcp source-port gt 95
```

tech

Use the **tech** command to enter tech mode, where additional tech-related commands are available.

Note:

This command is reserved for service personnel use only.

Syntax

tech

User level

tech

Context

general

Example

To enter tech mode:

```
G350-001# tech
Password:
G350-001(tech)#
```

telnet

Use the **`telnet`** command to initiate a login session via Telnet to a network host.

Syntax

`telnet ipaddress` [***`port_number`***]

Parameters

Parameter	Description	Possible Values	Default Value
ipaddress	The Telnet IP address		
`port_number`	The Telnet port number		**23**

User level

read-only

Context

general

Example

To initiate a Telnet session to IP address 133.23.6.66:

```
G350-011> telnet 133.23.6.66
```

terminal length

Use the **`terminal length`** command to set the length of the terminal display in characters.

Syntax

`terminal length [`*`lines`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
`lines`	The number of lines in the terminal display	**none** - Displays the current length. **3 – 200** - Sets the new screen length to the value.	

User level

read-only

Context

general

Example

To set the screen to display 24 lines:

```
G350-001> terminal length 24
```

terminal width

Use the **`terminal width`** command to set the width of the terminal display in characters.

Syntax

`terminal width [`*`characters`*`]`

Parameters

Parameter	Description	Possible Values	Default Value
characters	The number of characters in the width of the terminal display	**none** - Displays the current width. **10 – 200** - Sets the new screen width to the value.	

User level

read-only

Context

general

Example

To limit the display to a width of 6 characters:

```
G350-001> terminal width 6
```

test led

Use the **test led** command to run a test of the device’s LED operation.

Syntax

test led

User level

read-only

Context

general

Example

To run a test of the device’s LED operation:

```
G350-001> test led
```

The Box level ALM, CPU and MDM LEDs should be BLINKING for 5 seconds each.

test voip-dsp

Use the **test voip-dsp** command to start a BTR test on the VoIP engine. Also refer to: busyout voip-dsp on page 48, and release voip-dsp on page 268.

Note:

If you do not run the **busyout voip-dsp** command before the **test voip-dsp** command, only non-disruptive tests will run.

Note:

Status changes during the test create SNMP traps.

Note:

To view the results of the most recent BTR test, refer to show mm on page 461.

Syntax

test voip-dsp

User level

read-write

Context

general

Example:

To start a BTR test:

```
G350-001# test voip-dsp

DSP TEST RESULTS
--------------------------
DSP 0                PASS
DSP 1                PASS
```

timeout absolute

Use the **timeout absolute** command to set the number of minutes until the system automatically disconnects an idle PPP incoming session.

Syntax

timeout absolute *time*

Parameters

Parameter	Description	Possible Values	Default Value
time	Interval, in minutes, after which the system automatically disconnects the PPP session. An interval of 0 minutes indicates that no timeout should occur.	**0 – 999**	0

User level

read-write

Context

Interface: Console, USB-modem

Example

To set the PPP timeout to 30 minutes:

```
G350-011(if:Console)# timeout absolute 30
```

```
PPP incoming session will automatically disconnect after 30 minutes of
idle time.
```

timers basic

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.

Syntax

timers basic *update invalid*

no timers basic

Parameters

Parameter	Description	Possible Values	Default Value
update	The RIP update timer, in seconds	**30** or more	
invalid	The RIP invalid route timer, in seconds	**30** or more	

User level

read-write

Context

Router: rip

Example

To set the update timer to 30 seconds, and the invalid route timer to 180 seconds:

```
G350-001(router:rip)# timers basic 30 180
```

timers spf

Use the **`timers spf`** command to configure the delay between SPF calculations when using OSPF. Use the **no** form of this command to restore the default value.

Syntax

`timers spf spf_holdtime`

`no timers spf`

Parameters

Parameter	**Description**	**Possible Values**	**Default Value**
spf_holdtime	The time in seconds of the delay between SPF calculations	**1-3600**	**3**

User level

read-write

Context

Router: ospf

Example

To set the SPF delay time to 5 seconds:

```
G350-001(router:ospf)# timers spf 5
```

traceroute

Use the **`traceroute`** command to trace the network routing path to a destination IP address.

Syntax

```
traceroute ip_address
```

Parameters

Parameter	Description	Possible Values	Default Value
`ip_address`	Destination IP address to which a route is traced		

User level

read-only

Context

general

Example

To trace the route to IP address 172.16.1.47:

```
G350-001# traceroute 172.16.1.47
Press any key to stop traceroute ...
172.16.1.47               10 ms   (ttl = 1)
```

traffic-shape rate

Use the **`traffic-shape rate`** command to configure traffic shaping for outbound traffic on the current interface.

Syntax

```
traffic-shape rate bit_rate
```

Parameters

Parameter	Description	Possible Values	Default Value
bit_rate	The bit-rate that traffic is shaped to, in bits per second	**64000 – 2048000**	

User level

read-write

Context

Interface: FastEthernet(L2, L2-L3)

Example

To set the traffic-shaping rate to 128000:

```
G350-001(if:FastEthernet 10/2)# traffic-shape rate 128000
```

transmitter-delay

Use the **transmitter-delay** command to set the minimum number of flags to be sent between successive packets. Use the **no** form of the command to restore the transmitter-delay value to the default of 0.

Syntax

transmitter-delay ***number***

no transmitter-delay

Parameters

Parameter	Description	Possible Values	Default Value
number	The number of flags	**0 – 15**	

User level

read-write

Context

Interface: Serial (USP FR L2, USP PPP L2, USP PPP L2-L3)

Example

To set the transmitter-delay to send at least 10 flags between packets:

```
G350-001(if:Serial 5/1)# transmitter-delay 10
```

tree

Use the **`tree`** command to display the commands that are available at your current location in the CLI hierarchy. All commands are listed alphabetically.

Syntax

`tree` ***`depth`***

Parameters

Parameter	Description	Possible Values	Default Value
depth	The level of depth at which to display the list of CLI commands		

User level

read-only

Context

general

Example

To display the list of available commands to two levels:

```
G350-001> tree 2
```

```
> arp
> arp timeout
> banner login
  banner login > line
> banner post-login
  banner post-login > line
--type q to quit or space key to continue--
```

tunnel checksum

Use the **`tunnel checksum`** command to specify that the router adds a checksum bit to the outgoing GRE packet, for data verification. Use the **no** form of the command to specify that no checksum bit should be added.

Syntax

```
[no] tunnel checksum
```

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel checksum
```

tunnel destination

Use the **`tunnel destination`** command to specify the destination IP address for the GRE tunnel. The destination is the IP address of the tunnel's endpoint.

Note:

The CLI does not verify that the specified IP address actually exists.

Syntax

```
tunnel destination ip-address
```

Parameters

Parameter	Description	Possible Values	Default Value
ip-address	The destination IP address for the GRE tunnel		

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel destination 168.30.10.2
```

tunnel dscp

By default, the GRE header copies the DSCP value from the header of the original packet. Use the **`tunnel dscp`** command to override the original packet's DSCP with the specified DSCP value. Use the **`no`** form of the command to use the DSCP value of the original packet.

Syntax

`tunnel dscp` ***`dscp`***

no tunnel dscp

Parameters

Parameter	**Description**	**Possible Values**	**Default Value**
`dscp`	The DSCP value to be used instead of the DSCP from the header of the original packet	**0-63**	

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel dscp 0
```

tunnel keepalive

Use the **`tunnel keepalive`** command to specify that the tunnel sends keepalive packets to determine if the tunnel endpoint is up. Packets are sent according to the interval specified in the seconds parameters, and resent according to the number of the retries parameter.

Use the **no** form of the command to disable keepalive packets.

If the tunnel's destination interface fails to respond to a consecutive number of keepalive packets equal to the ***`<retries>`*** parameter, the tunnel informs hosts that send packets to the tunnel that the tunnel is down, although the source interface continues to send keepalive packets.

Syntax

`tunnel keepalive [`*`seconds`*` [`*`retries`*`]]`

`no keepalive`

Parameters

Parameter	Description	Possible Values	Default Value
seconds	The rate at which keepalive packets are sent	**0-32767**	10
retries	The number of times that a device continues to send keepalive packets without a response before the interface becomes inactive	**0-255**	3

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel keepalive 10 3
```

tunnel key

Use the **`tunnel key`** command to instruct the router to send GRE packets with a security key number. The tunnel endpoint must also be configured to use a security key, and the key numbers must be identical. If a security key is not configured on the tunnel endpoint, or a different key number is used, the packets are discarded. Use the **no** form of the command to specify that no security key should be sent.

Syntax

`tunnel key` ***`key_id`***

`no tunnel key`

Parameters

Parameter	Description	Possible Values	Default Value
`key_id`	The ID number of the security key to be sent with GRE packets	**0-2147483647**	

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel key 7
```

tunnel mode

Use the **`tunnel mode`** command to specify the encapsulation method of the tunnel. This command is only included for future development, and for conformity with other systems. Currently, the tunnel can only perform GRE encapsulation.

Syntax

`tunnel mode encapsulation`

no tunnel mode

Parameters

Parameter	Description	Possible Values	Default Value
`encapsulation`	The encapsulation method of the tunnel	**gre**	

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel mode gre
```

tunnel path-mtu-discovery

Use the **`tunnel path-mtu-discovery`** command to specify that the tunnel maintain information on the maximum allowable packet size (smallest MTU) for the entire routing path of the tunnel. Packets entering the tunnel that are larger than the tunnel's MTU are either fragmented, or sent back with a request for fragmentation (depending on the DF bit of the packet).

Use the age-timer parameter to force the tunnel to update the MTU after a specified number of minutes. Specify infinite to make the MTU value permanent (no updating).

Use the **no** form of the command to disable MTU discovery.

Note:

When MTU discovery is disabled, the tunnel's source interface marks all packets *may be fragmented*, even if the packet's original setting is *do not fragment*. It is highly recommended to enable the MTU-discovery feature on a tunnel.

Syntax

```
tunnel path-mtu-discovery [age-timer {minutes | infinite}]
no tunnel path-mtu-discovery
```

Parameters

Parameter	Description	Possible Values	Default Value
`age-timer`	Specifies how often the tunnel must update the MTU		
`minutes`	Number of minutes after which the tunnel is updated	**10-30**	**10**
`infinite`	The tunnel does not update the MTU and its value remains permanent		

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel path-mtu-discovery age-timer 20
```

tunnel source

Use the **`tunnel source`** command to specify the IP address of the source interface for the GRE tunnel. The source interface is the interface used to direct all traffic into the tunnel.

Note:

The CLI does not verify that the specified IP address actually exists.

Syntax

`tunnel source` ***`ip-address`***

Parameters

Parameter	Description	Possible Values	Default Value
`ip-address`	The IP address of the source interface for the GRE tunnel		

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel source 90.0.0.10
```

tunnel ttl

By default, GRE packets are given a ttl value of 255, since there is an unknown number of hops to reach the tunnel endpoint. Use the **`tunnel ttl`** command to override this default. Use the **no** form of the command to use the default ttl value.

Syntax

`tunnel ttl` ***`ttl`***

`no tunnel ttl`

Parameters

Parameter	Description	Possible Values	Default Value
`ttl`	The ttl value to be used instead of the default ttl value of 255	**1-255**	

User level

read-write

Context

Interface: Tunnel (L2, L2-L3)

Example

```
G350-001# tunnel ttl 16
```

udp destination-port

Use the **`udp destination-port`** command to define a destination port with the UDP protocol for which to apply the current rule. Use the **no** form of the command to specify that the rule applies to all ports *other* than the defined port.

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

```
udp destination-port any | {{eq | lt | gt}
{port_name | port_number}} | {range start_port end_port}
```

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
lt	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		

User level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule

Example

To specify that rule 22 applies to all packets whose destination port is 300:

```
G350-001(ACL 330/ip rule 22)# udp destination-port eq 300
```

udp source-port

Use the **`udp source-port`** command to define a source port with the UDP protocol for which to apply the current rule. Use the **no** form of the command to specify that the rule applies to all ports other than the defined port.

Note:

Issuing this command also sets the protocol to be UDP, if it is not already.

Syntax

`udp source-port any | {{eq | lt | gt} {`*`port_name`*` | `*`port_number`*`}} | {range `*`start_port end_port`*`}`

Parameters

Parameter	Description	Possible Values	Default Value
any	Keyword that specifies to apply the rule to a port with any name or number		
eq	Keyword that specifies to apply the rule to a port whose name or number matches exactly to the specified name or number		
`lt`	Keyword that specifies to apply the rule to a port whose name or number is less than the specified name or number		
			1 of 2

Parameter	Description	Possible Values	Default Value
gt	Keyword that specifies to apply the rule to a port whose name or number is greater than the specified name or number		
port_name	The name of the port for which to apply the rule		
port_number	The number of the port for which to apply the rule		
range	Keyword indicating that a range of ports is specified		
start_port	The start of a port range for which to apply the rule		
end_port	The end of a port range for which to apply the rule		
			2 of 2

User level

read-write

Context

ip pbr-list ip-rule, ip qos-list ip-rule, ip capture-list ip-rule, ip access-control-list ip-rule

Example

To specify that rule 22 applies to all packets whose source port is greater than 95:

```
G350-001(ACL 330/ip rule 22)# udp source-port gt 95
```

username

Use the **username** command to add a local user account. Use the **no** form of the command to remove the user account from the system.

By default there is only a single user account, named **root**, with password **root**, which accesses the administrator level. You cannot delete this basic user account, nor modify its access level. But you can modify its basic password.

Note:

For security reasons, you should change the **root** password immediately.

Syntax

username *name* password *passwd* access-type *access_type*

no username *name*

Parameters

Parameter	Description	Possible Values	Default Value
name	New user name	**minimum four character string**	
passwd	User's password	minimum four character string	
access_type	Access type definition	**read-only**, **read-write**, **admin**	

User level

admin

Context

general

Example

To create a new user account with username john, password johnny and access type of read-write:

```
G350-011(super)# username john password johnny access-type read-write
User account added.
```

You cannot change the access type of the root user:

```
G350-011(super)# username root password secret access-type read-write
ERROR: User account root has always an administrator access type.
```

To change the password of the root user:

```
G350-011(super)# username root password secret access-type admin
User account modified.
```

Note:

> If you wish to define a name which includes spaces, you must enclose the entire name in quotation marks, for example “new york”.

value

Use the **`value`** command to set the value of a DHCP option or a vendor-specific option. Use the **no** form of this command to clear the vendor-specific value.

Syntax

```
[no] value  raw  type value
```

Parameters

Parameter	Description	Possible Values	Default Value
`raw`	Non-encapsulated value		
`type`	Type of sub-option	● **ascii** — ASCII ● **hex string** — hexadecimal ● **ip-address** — IP address ● **word** — 16 bit number ● **integer** — 32 bit number	
`value`	The sub-option value		

User level

read-write

Context

dhcp pool vendor specific, dhcp pool option

Example

To specify IP addresses for World Wide Web servers (DHCP option 72):

```
G350-001(dhcp 5/option 72)# value raw ip-address "135.64.102.1,
135.64.102.2"
```

To enable IP forwarding (DHCP option 19 specifies whether the client should configure its IP layer for packet forwarding):

```
G350-001(dhcp 5/option 19)# value raw hex 01
```

To set a non-encapsulated value in ASCII format for vendor-specific option 1:

```
G350-001(DHCP 5/vendor specific 1)# value raw ascii
"MCIPADD=10.10.2.140,MCPORT=1719,TFTPSRVR=10.10.5.188"
```

To set a non-encapsulated value in Hex format for vendor-specific option 1:

```
G350-001(DHCP 5/vendor specific 1)# value raw hex
00:00:11:22:33:44:55:66:77
```

vendor-specific-option

A vendor specific option is an option unique to an individual vendor class. Use the **`vendor-specific-option`** command to set a vendor specific option. Use the **no** form of this command to delete a vendor-specific option.

Syntax

`[no] vendor-specific-option` ***`index-num`***

Parameters

Parameter	Description	Possible Values	Default Value
`index-num`	The index number of the vendor-specific option	1-10	

User level

read-write

Context

dhcp pool

Example

To set:

```
G350-001(DHCP 5)# vendor-specific-option 1
```

voip-queue

Use the **`voip-queue`** command to select custom queueing for VoIP traffic. By default, VoIP queuing is off, and Weighted Fair VoIP Queuing (WFVQ) is enabled on all Serial interfaces and all Fast Ethernet interfaces for which traffic-shaping is enabled. If you disable custom queueing by using the **no** form of the **`voip-queue`** command, WFVQ is re-enabled.

Syntax

`[no] voip-queue`

User level

read-write

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3)

> **Note:**
> This command is also used in FastEthernet context when traffic shaping is configured.

Example

To enable VoIP queuing:

```
G350-001(if:Serial 2/1:1)# voip-queue
```

voip-queue-delay

Use the **voip-queue-delay** command to set the maximum query delay for which to estimate.

Syntax

voip-queue-delay ***queue_delay_ms***

Parameters

Parameter	Description	Possible Values	Default Value
queue_delay_ms	The maximum amount of time that voice traffic is allowed to wait in the queue	**1-1000**	

User level

admin

Context

Interface: Serial (DS1 PPP L2-L3, DS1 PPP L2, DS1 FR L2, USP FR L2, USP PPP L2, USP PPP L2-L3), FastEthernet (L2, L2-L3)

> **Note:**
> This command is also used in Serial and WAN FastEthernet context when traffic shaping is configured.

Example

To set the maximum query delay to 30 milliseconds:

```
G350-001(super)# voip-queue-delay 30
```

Done!

zeroize

Use the **`zeroize`** command to clear all secret parameters and initialize the NVRAM to its factory defaults.

> **CAUTION:**
> This command restores factory defaults and disconnects the current session.

Syntax

`zeroize`

User level

admin

Context

general

Example

To clear all secret parameters and initialize the NVRAM to its factory defaults:

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

```
This command will  restore factory defaults, and disconnect your
existing session.
               *** Zeroize *** - do you want to continue (Y/N)? Y
```