NETGEAR

ProSafe Managed Switch

Command Line Interface (CLI) Reference Manual

9.2.0.5
JGSM7224

350 East Plumeria Drive
San Jose, CA 95134
USA

December 2012
202-10921-02
1.0

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10921-02	1.0	December 2012	Added the following new and revised command groups: ACL, DHCP snooping, DHCP L2 relay, DiffServ, DNS client, dual software image, dynamic ARP inspection, IP source control, and storm control.
202-10921-01	1.0	December 2011	Original publication.

Contents

Chapter 7 DHCP L2 Relay

Chapter 8 DHCP Snooping

Chapter 9 SNTP

Chapter 10 LLDP

Chapter 11 LLDP-MED

Chapter 12 VLAN

Chapter 13 Double VLAN

Chapter 14 Port Security

Chapter 15 Private Group

Chapter 16 Static MAC Filtering

Chapter 17 Voice VLAN

Chapter 18 STP

Chapter 19 PNAC

Chapter 23 IGMP Snooping

Chapter 24 Syslog

Chapter 25 SSH

Chapter 26 SSL

Chapter 27 SNMPv3

Chapter 28 RMON

Chapter 29 IPV4

Chapter 30 IPV6

Chapter 31 Port Protected

Chapter 32 Green Feature

Chapter 33 IP-ARP-INSPECTION

Chapter 34 ACL

Chapter 35 DOS

Chapter 36 Diffserv

Chapter 37 QoS

Chapter 38 IP Source Guard

Chapter 39 DNS Client

Chapter 40 Storm Control

Chapter 41 Dual Image

Chapter 42 Command List

Introduction 1

Purpose

The JGSM7224 performs switching between Ethernet ports at wire speed. It provides basic bridging functionality and also offers advanced features, such as link aggregation, IGMP Snooping, and Network Access Control.

This document describes in detail the CLI commands supported by the JGSM7224 switch. It is a reference manual for users and system administrators who need to configure the switch using the CLI interface.

Scope

The scope of this document is limited to JGSM7224 release 9.2.0.5. This document details all the CLI commands provided by the JGSM7224 software. The commands that are not applicable for a specific hardware platform are indicated wherever necessary.

Document Conventions

- The syntax of the CLI command is shown in Courier New 10-point bold.
- Elements in (< >) indicate the field is required as input along with a CLI command, for example, *<integer* `(100-1000)>`.
- Elements in square brackets (`[ ]`) indicate optional fields for a command.
- Text in {} refers to an “either-or” group for the tokens separated by a | symbol inside the braces.
- CLI commands, output, and messages are shown in Courier font.
- The no form of the command resets a particular configuration to its default value or revokes the effect. This is explained in the description of the commands as needed.
- Any action that can change the switch configuration, any conditionals and requirements for a command, and any information associated with significant details and functionality of a command is listed using the “..” symbol.

Key Conventions

Keyboard Shortcuts

Key Sequence	Description
Up Arrow/Down Arrow	Displays the previously executed command
Backspace / Ctrl + H	Removes a single character
TAB	Completes a command without typing the full word
Left Arrow/Right Arrow	Traverses the current line

Others

- ? - Lists the available commands.
- q - Exits the output display if the display is more than one page and returns to the JGSM7224 prompt.
- `show history` - Displays the command history list.

Command-Line Interface

2

This chapter describes how to configure the JGSM7224 using the Command Line Interface.

Note: The Command Line Interface (CLI) can be used to configure the Intelligent Switch Solution from a console attached to the serial port of the switch or from a remote terminal using TELNET.

The JGSM7224 CLI uses a simple login authentication mechanism. The authentication is based on a user name and password provided by the user during login. The user `admin` is created by default and has a blank password.

Note: When JGSM7224 is started, the user name and password must be given at the login prompt to access the CLI shell:

```
------------------------------------------------
user: admin
password:
(JGSM7224)>
------------------------------------------------
```

The user-exec mode is now available. For a detailed description of the various modes available for the JGSM7224, see *CLI Command Modes* on page 19.

CLI commands need not be fully typed. The abbreviated forms are also accepted by the switch. For example, commands like `show management vlan` can be typed as `show management vl`.

CLI commands are case-insensitive.

CLI commands are successful only if the dependencies are satisfied for the particular command entered. Appropriate error messages are displayed if the dependencies are not satisfied.

Note: The ethernet type of an interface is determined during System Startup. The ethernet type needs to be specified correctly when you configure interface-specific parameters.

A fast ethernet interface cannot be configured as a gigabit-ethernet interface and vice-versa.

CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	This is the initial mode to start a session.	`(JGSM7224)>`	The logout method is used.
Privileged EXEC	The User EXEC mode command `enable` is used to enter the Privileged EXEC mode.	`(JGSM7224)#`	To return from the Privileged EXEC mode to the Privileged EXEC mode, use the `disable` command.
Global Configuration	The Privileged EXEC mode command `configure terminal` is used to enter the Global Configuration mode.	`(JGSM7224)(config)#`	To exit to the Global Configuration mode, use the `exit` command. To exit to the Privileged EXEC mode use the `end` command.
Interface Configuration	The Global Configuration mode command interface `<interface-type> <interface-id>` is used to enter the Interface configuration mode.	`(JGSM7224)(config-if)#`	To exit to the Global Configuration mode, use the `exit` command. To exit to the Privileged EXEC mode use the `end` command.
VLAN Config	The Privileged EXEC mode command `vlan database` is used to enter the VLAN Config mode.	`(JGSM7224)(vlan)#`	To exit to the Privileged EXEC mode, use the `exit` command.

User EXEC Mode

After logging in to the device, the user is automatically in the User EXEC mode. In general, the User EXEC commands are used to temporarily change terminal settings, perform basic tests, and list system information.

Privileged EXEC Mode

Since many of the privileged commands set operating parameters, privileged access is password protected to prevent unauthorized use. The password is not displayed on the screen and is case-sensitive. The Privileged EXEC mode prompt is the device name followed by the pound sign (#).

Global Configuration Mode

Global Configuration commands apply to features that affect the system as a whole, to any specific interface.

Interface Configuration Mode

Physical Interface Mode

The Physical Interface mode is used to perform interface-specific operations. To return to the global configuration mode, use the `exit` command.

Port Channel Interface Mode

The Port Channel Interface mode is used to perform port channel-specific operations. To return to the global configuration mode, use the `exit` command.

Management VLAN Interface Mode

The Management VLAN Interface mode is used to perform L3-IPVLAN-specific operations. To return to the global configuration mode, use the `exit` command.

Tunnel Interface Mode

The Tunnel Interface mode is used to perform Tunnel-specific operations. To return to the global configuration mode, use the `exit` command.

VLAN Config Mode

This mode is used to perform VLAN-specific operations. To return to the global configuration mode, use the `exit` command.

Protocol-Specific Modes

DHCP Pool Configuration Mode

This mode is used to configure the network pool / host configurations of a subnet pool. The Global configuration mode command `ip dhcp pool <integer(1-2147483647)>` creates a DHCP server address pool and places the user in DHCP pool configuration mode. The prompt displayed in this mode is `(JGSM7224)(dhcp-config)#`.

To return to the global configuration mode, use the `exit` command.

ACL MAC Configuration Mode

The MAC access-list global configuration command creates Layer 2 MAC ACLs and returns the MACAccess list configuration mode to the user. The Global configuration mode command `mac access-list extended <(name(1-31))>` is used to enter the ACL MAC Configuration mode and the prompt displayed in this mode is `(JGSM7224)(config-ext-macl)#`.

To return to the global configuration mode, use the `exit` command.

SNTP Configuration Mode

This mode is used to configure the SNTP-specific parameters for the switch. The Global configuration mode command `sntp` is used to enter the SNTP Configuration mode and the prompt displayed in this mode is `(JGSM7224)(config-sntp)#`.

To return to the global configuration mode, use the `exit` command.

System Commands

3

This chapter describes the commands used to manage access permissions, mode access, and terminal configurations on the JGSM7224 switch.

enable

This command turns on privileged commands. When in User EXEC mode, you can use this command to enter Privileged EXEC mode.

Syntax `enable`

Mode User EXEC

Example

```
----------------------------------------------------------------
(JGSM7224)> enable
(JGSM7224)#
----------------------------------------------------------------
```

configure terminal

Use this command to enter the configuration mode.

Syntax `configure terminal`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------
(JGSM7224)# configure terminal
(JGSM7224)(config)#
-------------------------------------------------------------------------
```

Related Command

`exit` - Exits the current configuration mode to the next highest configuration mode.

listuser

This command lists all valid users, along with their permissible mode.

Syntax `listuser`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
listuser
-------------------------------------------------------------------------------
```

Related Command

`show users` - Displays information about terminal lines.

username

This command creates a user and sets the enable password for that user. The `no` form of the command deletes a user and disables the enable password for that user. At the system default state, there is only one user, `admin`, with a blank password.

When you log in with the user name `admin`, you can add or delete a user and change the password of other users in the system. If you log in with another user name, however, you can change only your own password. If you add a new user with this command and do not specify a password, the user you add has a default blank password.

Syntax

```
username <user-name> [password <passwd>]
no username <user-name>
```

Mode Global Configuration

`user-name` - User names can be up to 20 characters in length and are case-sensitive. Only alphanumeric characters, dashes (-), and underscores (_) are accepted.

`password` - Password.

Related Command

`listuser` - lists all valid users

logout

This command exits from Privileged EXEC or User EXEC mode to the JGSM7224 Login Prompt if you are in a console session. If a telnet session is active, this command terminates the session.

Syntax `logout`

Mode Privileged EXEC
User EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)>logout
user:
-------------------------------------------------------------------------------
```

exit

This command exits the current configuration mode to the next highest configuration mode in the CLI. The login name and password must be reentered to gain access to the CLI command shell.

Syntax `exit`

Mode All modes

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if) # exit
(JGSM7224)(config) #
-------------------------------------------------------------------------------
```

show users

This command displays information about login user sessions.

Syntax `show users`

Mode Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show users
ID   Type     User    Peer-Address
c1   console  admin   Local Peer
c2   telnet   admin   192.168.0.10
w1   http     admin   192.168.0.10
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Command

`listuser` - Lists all valid users, along with their permissible mode.

show history

This command displays command history. The commands are listed from the earliest to the latest command. The buffer is unchanged when entering configuration mode and then returning.

Syntax `show history`

Mode Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show history
1 show debug-logging
2 show users
3 listuser
4 show users
5 show history
(JGSM7224)#
-----------------------------------------------------------------------------
```

reload

This command restarts the switch.

Syntax `reload`

Mode Privileged EXEC

show process cpu

This command displays the process CPU utilization.

Syntax `show process cpu`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show process cpu

Memory Utilization Report
status         bytes

free           13135872
alloc          51830784

CPU Utilization:

PID   Name             5 Sec    1 Min   5 Min
1     init             0.0%     0.0%    0.0%
2     kthreadd         0.0%     0.0%    0.0%
3     ksoftirqd/0      0.0%     0.0%    0.0%
4     events/0         0.0%     0.0%    0.0%
5     khelper          0.0%     0.0%    0.0%
15    kblocked/0       0.0%     0.0%    0.0%
31    pdflush          0.0%     0.0%    0.0%
(JGSM7224)#
-------------------------------------------------------------------------------
```

show memory cpu

This command displays the system memory utilization.

Syntax `show memory cpu`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show memory cpu
Total Memory.......................... 63444 KBytes
Available Memory Space................ 12828 KBytes
(JGSM7224)#
-------------------------------------------------------------------------------
```

System Features

4

The JGSM7224 switch offers a rich set of system features, such as login services, copying/writing facilities, duplex/negotiation support, and many others. Some features might have special hardware requirements and others might have special design considerations. The related command sections provide overview descriptions of the features and include specific information to consider when using these features.

CFA (Common Forwarding Agent) is a proprietary module that acts as a common forwarder of packets between the Network Protocol Module(s), the Data-Link Layer Protocol Layer Module(s), and the Device Drivers. CFA provides central management of the generic parameters of all the interfaces in the system.

login authentication

This command sets the authentication method for user logins and the no form of the command sets the authentication method for user logins to default values. Changing login authentication from default to another value might disconnect the telnet session.

TACACS is an authentication program used on UNIX and Linux systems, a few network routers, and other network equipment that allows access to a server or a managing computer to determine if the user attempting to log in has the proper rights or is in the user database.

Syntax `login authentication { local | radius | tacacs }`
`no login authentication`

Mode Global Configuration

`local` - Local username database for authentication.

`radius` - List of all RADIUS servers for authentication.

`tacacs` - List of useful TACACS+ servers for authentication.

Example

```
----------------------------------------------------------------
(JGSM7224)(config)# login authentication radius
(JGSM7224)(config)#
----------------------------------------------------------------
```

Related Commands

`username` - Creates a user and sets the enable password for that user with the privilege level.

`show system information` - Displays system information.

ip http port

This command sets the HTTP port, and the `no` form of the command resets the HTTP port.

Default 80

Syntax
```
ip http port <port-number(1-65535)>
no ip http port
```

Mode Global Configuration

Example

```
--------------------------------------------------------------------------
(JGSM7224)(config)# ip http port 90
(JGSM7224)(config)#
--------------------------------------------------------------------------
```

Related Commands

`ip http server` - Enables access to the switch through the Web interface.
`show ip http` - Displays the HTTP settings for the switch.

ip http server

This command enables access to the switch through the Web interface, and the `no` form of the command disables it. When access is enabled, the user can log in to the switch from the Web interface. When access is disabled, the user cannot log in to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Default Enabled

Syntax
```
ip http server
no ip http server
```

Mode Global Configuration

Example

```
--------------------------------------------------------------------------
(JGSM7224)(config)# no ip http server
(JGSM7224)(config)#
--------------------------------------------------------------------------
```

Related Commands

`ip http port` - Sets the HTTP port.
`show ip http` - Displays the HTTP settings for the switch.

ip http session timeout

This command configures the timeout for unsecure HTTP sessions in minutes. Configuring this value to zero sets an infinite timeout. When the timeout expires the user is forced to re-authenticate. The timer begins on initiation of the Web session and is restarted with each access to the switch. The `no` form of the command resets the timeout to the default value.

Default 30

Syntax
```
ip http session timeout <0-60>
no ip http session timeout
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip http session timeout 10
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip http` - Displays the HTTP settings for the switch.

interface

This command selects an interface to configure, which can be a physical interface, a port-channel interface, or a management vlan interface. On execution of this command, the user enters the interface configuration mode for that interface. Eight port-channels are created by default.

Syntax
```
interface {vlanMgmt | {port-channel | lag}<integer (1-8)> |
<slot/port>}
```

Mode Global Configuration

`vlanMgmt` - The management vlan interface.
`port-channel` - Port Channel Identifier.
`slot/port` - Physical interface ID, including type, slot, and port format.

Example

```
--------------------------------------------------------------------------------
For management VLAN Interface:
(JGSM7224)(config)# interface vlanMgmt
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show interface` - Displays the interface status and configuration.

interface range

This command selects a range of interfaces to configure, which can be physical interfaces or port-channel interfaces.

Syntax `interface range {<iface_list> | port-channel <po_list>}`

Mode Global Configuration

`iface-list` - The physical interface list.
`port-channel` - The port channel identifier.
`po-list` - The port channel interface list.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# interface range 0/1-24
(JGSM7224)(config-if-range)#
--------------------------------------------------------------------------------
```

management vlan-list

This command sets the VLAN list for the L3 VLAN interface. The no form of the command resets the list for the L3 VLAN interface.The VLAN list can be specified as a range of VLAN IDs separated by a hyphen or a series of non-consecutive VLANs separated by a comma. A single VLAN ID can also be substituted instead of a range of VLANs. This command is configured only when the code is compiled with the WorkGroupSwitch enabled, if the L2 Vlan Management support is required.

Default vlan - 1
interface-type - eth0

Syntax `management vlan-list <vlan-list>`
`no management vlan-list <vlan-list>`

Mode Global Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# management vlan-list
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Command

`show management vlan` - Displays the VLANs associated with the management interface.

mtu frame size

This command configures the maximum transmission unit frame size for the interface. The MTU includes the Ethernet header, CRC, and payload. The MTU size is a valid integer between 1518 and 9216 for untagged packets. For tagged packets, the actual MTU is the specified MTU size plus 4. The interface must be brought down administratively prior to changing the MTU.

Default	1518
Syntax	`mtu <frame-size(1518-9216)>`
Mode	Interface Configuration

> **Note:** For IPV6, the minimum valid MTU is 1280.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# mtu 1600
(JGSM7224)(config-if)#
-----------------------------------------------------------------------------
```

Related Commands

`show interfaces` - Displays the interface status and configuration.
`show interface mtu` - Displays the global maximum transmission unit.

snmp trap link-status

This command enables trap generation on either the physical interface or the port-channel interface. The no form of this command disables trap generation on the respective interface.

Default Enabled

Syntax
```
snmp trap link-status
no snmp trap link-status
```

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# snmp trap link-status
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show interfaces` - Displays the interface status and configuration.

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make persist across a reboot. This command is the same as `copy system:running config nvram:startup-config`.

Syntax `write memory`

Mode Privileged EXEC

Related Commands

`copy` - Uploads and downloads the file from the remote.

`save` - Saves the configuration.

`erase` - Erases the specified file.

copy

This command uploads and downloads files to and from the switch. Upload and download files from a server by using TFTP.

Syntax `copy <source> <destination>`

Mode Privileged EXEC

Replace the <source> and <destination> parameters with the options in the following table. For the <tftp_url> source or destination, use the following values:

<tftp_url> tftp://<ipaddr | hostname>/<filename>

For TFTP, the <ipaddr> parameter is the IP address of the server, and <filename> is the name of the file you want to upload or download. Parameters for the copy command are listed in the following table:

Source	Destination	Description
<tftp url>	nvram:sslpem-server	Downloads Secure Server PEM file to the system
<tftp url>	nvram:startup-config	Downloads the startup configuration file to the system
<tftp url>	system:boot	Downloads and updates the boot code
<tftp url>	system:image	Downloads and updates the image
<tftp url>	{image1 | image2}	Download an image from the remote server to either image.
{image1 | image2}	<tftp url>	Upload either image to the remote server.
image1	image2	Copy image1 to image2.
image2	image1	Copy image2 to image1.
nvram:backup-config	<tftp url>	Uploads the backup configuration to the server
nvram:backup-config	nvram:startup-config	Copies the backup config to the startup config
nvram:debug-log	<tftp url>	Uploads the debug log file to the server
nvram:log1	<tftp url>	Uploads the log file 1 to the server
nvram:log2	<tftp url>	Uploads the log file 2 to the server
nvram:log3	<tftp url>	Uploads the log file 3 to the server
nvram:startup-config	<tftp url>	Uploads the startup configuration to the server
nvram:startup-config	nvram:backup-config	Copies the startup config to the backup config
system:running-config	nvram:startup-config	Save the running configuration to nvram

Related Commands

write memory - Create the configuration file.
save - Save the configuration.
erase - Erase the specified file.

save

This command makes the current configuration changes permanent by writing the configuration changes to system NVRAM.

Syntax `save`

Mode Privileged EXEC

Related Commands

`write memory` - Create the configuration file.
`copy` - Uploads and downloads the file from the remote.
`erase` - Erases the specified file.

clock set

This command manages the system clock.The date is configured in the switch in the following format:

- Hours:minutes:Seconds Date Month Year.
- The format for the date is dd(1-31).
- The format for the month is Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.
- The format for the year is yyyy(1970-2035).

Syntax `clock set hh:mm:ss day month year`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# clock set 18:04:10 18 Oct 2005
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show clock` - Displays the system clock.

erase

This command clears the contents of a specified file.

Syntax `erase { startup-config | backup-config | log1 | log2 | log3 }`

Mode Privileged EXEC

`startup-config` - Startup configuration file.
`backup-config` - Backup configuration file.
`log1` - Log file 1.
`log2` - Log file 2.
`log3` - Log file 3.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# erase startup-config
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`write memory` - Create the configuration file.
`copy` - Uploads and downloads the file from the remote.
`save` - Save configuration.

shutdown - physical/vlanMgmt/port-channel Interface

This command disables a physical interface/vlanMgmt interface/port-channel interface. The no form of the command enables a physical interface/vlanMgmt interface/port-channel interface. All functions on the specified interface are disabled by the shutdown command.

Default	Physical Interface enabled Management VLAN interface enabled Port-channel interface enabled
Syntax	`shutdown` `no shutdown`
Mode	Interface Configuration Mode for physical interface/port-channel Interface Management VLAN Interface Mode for vlanMgmt interface

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# shutdown
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`interface` - Configures an interface, which can be a physical interface, a port-channel interface, or a management vlan interface.

`show interfaces` - Displays the interface status and configuration.

debug-logging

This command configures where debug logs are to be displayed and the no form of the command displays debug logs on the console. Debug logs are directed to the console screen or to a buffer file, which can later be uploaded based on the input.

Syntax `debug-logging { console|file }`
`no debug-logging`

Mode Global Configuration

`console` - Debug logs are displayed on the Console.
`file` - Debug logs are displayed in the file.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# debug-logging console
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show debug-logging` - Displays the debug logs stored in file.

show interfaces

This command displays the interface status and configuration.If executed without the optional parameters, this command displays the IP interface statistics and configuration for all available interfaces.

Syntax `show interfaces [{ [<slot/port>] [{ description | rate-limit | flowcontrol | capabilities | status }] | port-channel <port-channel-id (1-8)> }]`

Mode Privileged EXEC

`slot/port` - Physical interface ID, including type, slot, and port format.

`description` - Description of the interface.

`rate-limit` - Rate limit of the interface.

`flowcontrol` - Receive or send flow control value for an interface.

`capabilities` - Capabilities of the interface.

`status` - Status of the interface.

`port-channel` - Port Channel Identifier.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show interfaces 0/2

0/2 up, line protocol is up (connected)

Hardware Address is 00:01:02:03:04:22
RARP Client is enabled
MTU 1500 bytes, Full duplex, 100 Mbps, Auto-Negotiation
HOL Block Prevention enabled.
Flow-control is off

Link Up/Down Trap is enabled

Reception Counters
Octets : 739284
Unicast Packets : 0
Non Unicast Packets : 5963
Discarded Packets : 0
Error Packets : 0
Unknown Protocol : 5963

Transmission Counters
Octets : 741775
Unicast Packets : 0
Non Unicast Packets : 5985
Discarded Packets : 0
Error Packets : 0
(JGSM7224)# show interfaces

Interface   Status   Protocol
---------   ------   --------
0/1         up       up
0/2         up       down
0/3         up       up
(JGSM7224)# show interfaces 0/2 flowcontrol
Port Tx Rx Tx Pause Rx Pause             HC Rx Pause
---- ----- -------- --------             --------
0/2   off  off 0     0    0               0
(JGSM7224)# show interfaces 0/2 capabilities
0/2
Type : 10/100/1000 Base TX
Speed : 10, 100, 1000, Auto
Duplex : Half, Full
FlowControl : Send, Receive
JGSM7224 # show interfaces 0/2 status
Port Status Duplex Speed Negotiation
```

```
---- ------ ------ ----- -----------
0/2  connected Full 100 Mbps Auto
JGSM7224 # show interfaces port-channel
2 po2 up, line protocol is up (connected)
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`interface` - Configures an interface which can be a physical interface or a port-channel interface or management vlan interface.

show interfaces - counters

This command displays the interface statistics for each port.

Syntax `show interfaces counters {<slot/port> | port-channel <integer (1-8)>} [detail]`

Mode Privileged EXEC

`counters` - Various counters for the switch or for the specific interface.

`slot/port` - Physical interface ID, including type, slot, and port format.

`port channel` - Port channel ID.

`detail` - Detailed statistics.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show interfaces counters 0/1 detail Port
.....................................................................
0/1 Packets R1 64 Octets
.......................................... 39 Packets R1 65-127
Octets ..................................... 38 Packets R1
128-255 Octets ..................................... 18 Packets
R1 256-511 Octets ..................................... 1
Packets R1 512-1023 Octets
..................................... 4 Packets R1 1024-1518
Octets ..................................... 0 Packets R1
1519-1522 Octets ..................................... 0 Packets
R1 1522-2047 Octets ..................................... 0
Packets R1 2048-4095 Octets
..................................... 0 Packets R1 4095-9216
Octets ..................................... 0 Multicast Packets
Received ..................................... 5
--------------------------------------------------------------------------------
```

Related Command

`show interfaces` - Displays the interface status and configuration.

show management vlan

This command displays the VLANs associated with the management interface.

Syntax `show management vlan`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show management vlan

Interface Status.............................. UP

IP Address.................................... 192.168.0.239
Subnet Mask................................... 255.255.255.0
Default Gateway............................... No Configurated
Configured IPv4 Protocol...................... NONE

IPv6 Administrative Mode...................... UP
IPv6 Prefix is ............................... fe80::a221:b7ff:fe97:4f93/128
Default IPv6 GateWay is ...................... No Configurated
Configured IPv6 Protocol...................... None

MAC address................................... a0:21:b7:97:4f:93
Management VLAN ID............................ 1

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`management vlan-list` - Sets the VLAN list for the L3 VLAN interface.

show network

This command displays the management interface.

Syntax `show network`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show network

Interface Status.............................. UP

IP Address.................................... 192.168.0.239
Subnet Mask................................... 255.255.255.0
Default Gateway............................... No Configurated
Configured IPv4 Protocol...................... NONE

IPv6 Administrative Mode...................... UP
IPv6 Prefix is ............................... fe80::a221:b7ff:fe97:4f93/128
Default IPv6 GateWay is ...................... No Configurated
Configured IPv6 Protocol...................... None

MAC address................................... a0:21:b7:97:4f:93
Management VLAN ID............................ 1

(JGSM7224)#
--------------------------------------------------------------------------------
```

show interfaces mtu

This command shows the Maximum Transmission Unit (MTU) of ports in the switch.

Syntax `show interfaces mtu [{ port-channel <port-channel-id (1-8)> | <slot/port> }]`

Mode Privileged EXEC

`port-channel` - Port Channel Identifier.

`slot/port` - Physical interface ID including type, slot, and port number.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show interface mtu 0/1
0/1 MTU size is 1500
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`mtu frame size` - Configures the maximum transmission unit frame size for the interface.

show system information

This command displays system information.

Syntax `show system information`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show system information

System Uptime               : 21 hrs, 30 mins, 29 secs

System Description          : JGSM7224 - 24-Port Gigabit Layer 2 Managed Switch
Switch Name                 : JGSM7224
System Contact              : JGSM7224
System Location             : JGSM7224
System Object ID            : 1.3.6.1.4.1.4526.100.2.6

Base Mac Address            : e0:46:9a:47:c2:0a

Logging Option              : Console Logging
Login Authentication Mode   : Local
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`write` - Writes the running-config to a startup-configuration file.

`erase` - Clears the contents of the startup configuration or sets parameters in NVRAM to default values.

`login authentication` - Sets the authentication method for user logins.

show version

This command displays system version information.

Syntax `show version`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show version
System Description.........JGSM7224  -  24-Port Gigabit Layer 2 Managed Switch
Machine Type...............24-Port Gigabit Layer 2 Managed Switch
Machine Model..............JGSM7224
Serial Number..............23H511570074D
Manufacturer...............Netgear
Software Version...........9.2.0.5
(JGSM7224)#
--------------------------------------------------------------------------------
```

show debug-logging

This command displays the debug logs stored in the log file.

Syntax `show debug-logging`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# debug-logging file
(JGSM7224)(config)# exit
(JGSM7224)# debug spanning-tree events
(JGSM7224)# show debug-logging
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
AST: MSG: Timer Expiry Event processed...
AST: MSG: Completed processing the event(s).
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`debug-logging` - Configures where debug logs are to be displayed.

show clock

This command displays the system date and time.

Syntax `show clock`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show clock
Tue Oct 18 18:04:11 2005
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`clock set` - Manages the system clock.

show running-config

This command displays the current operating configuration in the system.

Syntax show running-config
show running-config changed
show running-config interface

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show running-config

Building configuration...
!
!
vlan database
vlan 4-6
!

!

interface 0/1 no shutdown
```

```
!
interface 0/2
no shutdown
!
interface 0/3
no shutdown
!
........
interface vlanMgmt
ip address 192.168.0.2 255.255.255.0
no shutdown
ipv6 enable
!
!
!
!

snmp user initial
snmp user templateMD5 auth md5 AUTH_PASSWD
snmp user templateSHA auth sha AUTH_PASSWD priv DES DES_CBC
!
!
!

end
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

Related commands include the configuration commands of all the modules.

show ip http

This command displays the http settings for the switch.

Syntax	show ip http
Mode	Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip http

HTTP Mode (Unsecure)........................... Enabled
HTTP Port...................................... 80
HTTP Session Timeout........................... 30
```

```
HTTP Mode (Secure)............................ Disabled
Secure Port................................... 443
HTTPS Session Timeout......................... 30
Certificate Present........................... True

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`ip http port` - Sets the HTTP port.

`ip http server` - Enables access to the switch through the Web interface.

`ip http session timeout` - Configures the timeout for unsecure HTTP sessions in minutes.

`ip http secure-server` - Enables the secure socket layer for secure HTTP.

`ip http secure-port` - Set the SSL port, where port can be 1-65535.

`ip http secure-session timeout` - Configures the timeout for secure HTTP sessions in minutes.

`crypto certificate generate` - Generates self-signed certificate for HTTPS.

`show ssl server-cert` - Displays SSL server certificate.

console timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected infinitely. The time range is 0 to 160. The no form of the command sets the console login inactivity timeout value to the default.

Default 30

Syntax
```
console timeout <0-160>
no console timeout
```

Mode Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# console timeout 10
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show console` - Displays console settings for the switch.

ip telnet server enable

This command enables Telnet connections to the system and enables the Telnet Server Admin Mode. This command opens the Telnet listening port. The no form of the command disables Telnet access to the system and disables the Telnet Server Admin Mode. The no form of the command also closes the Telnet listening port and disconnects all open Telnet sessions.

Default Enabled

Syntax
```
ip telnet server enable
no ip telnet server enable
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# no ip telnet server enable
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show telnet` - Displays the current Telnet settings.

telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160. The no form of the command sets the Telnet connection session timeout value to the default.

Default 30

Syntax
```
telnetcon timeout <1-160>
no telnetcon timeout
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# telnetcon timeout 10
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show telnet` - Displays the current Telnet settings.

telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5. The no form of the command sets the maximum number of Telnet connection sessions to the default value.

Default 5

Syntax
```
telnetcon maxsessions <0-5>
no telnetcon maxsessions
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# telnetcon maxsessions 3
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show telnet` - Displays the current Telnet settings.

show console

This command displays console settings for the switch.

Syntax `show console`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# show console
Console Login Timeout (minutes)..... 30
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`console timeout` - Specifies the maximum connect time (in minutes) without console activity.

show telnet

This command displays the current Telnet settings.

Syntax `show telnet`

Mode Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show telnet

Telnet Server Admin Mode..................... Enable
Remote Connection Login Timeout (minutes)..... 30
Maximum Number of Remote Connection Sessions... 5
Telnet Sessions Currently Active.............. 0

(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`ip telnet server enable` - Enables Telnet connections to the system and enables the Telnet Server Admin Mode.

`telnetcon timeout` - Sets the Telnet connection session timeout value, in minutes.

`telnetcon maxsessions` - Specifies the maximum number of Telnet connection sessions that can be established.

restore startup-config

This command sets the startup-config restore flag. If this flag is set, the switch will use startup-config for the next restore.

Syntax `restore startup-config`

Mode Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# restore startup-config
(JGSM7224)#
-----------------------------------------------------------------------------
```

Note: These commands also set the startup-config restore flag: `save`, `write memory`, `copy <tftp_url> nvram:startup-config`, and `copy nvram:backup-connfig nvram:startup-config`.

Related Commands

`write memory` - Creates the config file.

`copy` - Uploads and Downloads the file from the remote.

`save` - Saves the configuration. This command also sets the restore flag.

no restore

This command sets the no restore flag. If this flag is set, the switch will not use the startup-config for the next restore. This flag will also be set if the startup-config does not exist.

Syntax `no restore`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# no restore
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`write memory` - Creates the config file.

`copy` - Uploads and downloads the file from the remote.

`save` - Saves the configuration.

clear interfaces counters

This command clears statistics for the interface.

Syntax `clear interfaces [<slot/port>] counters`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# clear interfaces 0/1 counters
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`slot/port` - Physical interface ID, including type, slot, and port format.

Port Manager 5

The JGSM7224 switch offers a rich set of commands to manage ports, such as port speed, port duplex, auto-negotiation, rate-limit, storm-control, and port-mirroring.

monitor session

This command enables port-mirroring in the switch. The no form of the command disables port mirroring in the switch.

Default Port Mirroring is disabled

Syntax
```
monitor session <session_number:1> { destination interface <slot/port> |
source interface <slot/port>[{ rx | tx }] | mode }
no monitor [session <session_number:1>] [{source interface <slot/port> |
destination interface | mode}]
```

Mode Global Configuration

`session number` - Specifies the session number identified with the session.

`destination interface` - Specifies the destination interface or the mirror-to port. Valid interfaces are physical ports. There can be only one mirror-to port per switch.

`source interface` - Specifies the interface for the traffic that is to be mirrored. Valid interfaces include physical ports, with a maximum of eight physical ports.

`rx` - Received traffic is mirrored.

`tx` - Transmitted traffic is mirrored.

`mode` - Enable or disable mirror.

Example

```
----------------------------------------------------------------------
(JGSM7224)(config)# monitor session 1 source interface 0/2
----------------------------------------------------------------------
```

Related Command

`show monitor session 1` - Displays port-monitoring information.

negotiation

This command enables auto-negotiation on the interface. The no form of the command disables auto- negotiation on the interface. The auto-negotiation doesn't affect flow control status.

Syntax `negotiation`
`no negotiation`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# negotiation
-------------------------------------------------------------------------------
```

speed

This command sets the speed of the interface.

Default 100

Syntax `speed { 10 | 100 }`

Mode Interface Configuration

`10` - Port runs at 10Mbps

`100` - Port runs at 100Mbps

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# speed 100
-------------------------------------------------------------------------------
```

Related Commands

`negotiation` - Enables auto-negotiation

`duplex` - Configures the duplex operation

duplex

This command configures duplex operation.

Default half

Syntax `duplex { full | half }`

Mode Interface configuration

full - Port is in full-duplex mode

half - Port is in half-duplex mode

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# duplex half
--------------------------------------------------------------------------------
```

Related Commands

`negotiation` - Enables auto-negotiation on the interface

`speed` - Sets the speed of the interface

rate-limit

This command enables the rate limiting and burst size rate limiting by configuring the egress and ingress packet rate of an interface. The `no` form of the command disables the rate limiting and burst size rate limiting on an egress or ingress port.

Defaults `rate-value - 0`
`burst-value - 0`

Syntax `rate-limit {output | input }<rate-value> <burst-value>`
`no rate-limit {output | input}`

Mode Interface configuration

`rate-value` - Line rate in kbps

`burst-value` - Burst size value in kbps

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# rate-limit output 64 32
--------------------------------------------------------------------------------
```

show monitor session

This command displays port-monitoring information.

Syntax `show monitor session <session_number : 1>`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show monitor session 1
-------------------------------------------------------------------------------
```

Related Command

`monitor session` - Enables port-mirroring in the switch

DHCP

6

DHCP (Dynamic Host Configuration Protocol) allows dynamic configuration of a host computer. When a DHCP client is booted, it initially does not have an IP address assigned to it. It issues a broadcast message to any DCHP servers that are on the network. An exchange takes place during which the DHCP server assigns an IP address to the client and sends the client certain key network configuration parameters.

Many Internet service providers (ISPs) require that their customers use a DHCP client so the ISP can dynamically assign IP addresses and control other network settings. Another use is for laptop computers, which can be connected to more than one network. For example a laptop can be connected to a network in the office and also at home. This is an ideal use for DHCP since the laptop doesn't need to be manually reconfigured for use in the two different networks. In this case, there needs to be a DHCP server both on the office network and the home network and the laptop needs a DHCP client.

dhcp client release

This command immediately releases the DHCP lease on the interface specified.The VLAN interface must have an IP address assigned by the DHCP server, and it must be in binding state.

Syntax `dhcp client release`

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# dhcp client release
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`show management vlan` - Displays the IP interface statistics and configuration.

`show dhcp client stats` - Displays the DHCP client statistics information.

`dhcp client acquire` - Configures the current VLAN interface to dynamically acquire an IP address from the DHCP server.

dhcp client renew

This command immediately renews the DHCP lease for the interface specified. The VLAN interface must have an IP address assigned by the DHCP server.

Syntax `dhcp client renew`

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# dhcp client renew
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`dhcp client acquire` - Configures the current VLAN interface to dynamically acquire an IP address from the DHCP server.

`show dhcp client stats` - Displays the DHCP client statistics information.

dhcp client acquire

This command immediately acquires the ip address through the DHCP on the interface specified.

Syntax `dhcp client acquire`

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# dhcp client acquire
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`show ip dhcp client stats` - Displays the DHCP client statistics information.

`show management vlan` - Displays the IP interface statistics and configuration.

`dhcp client release` - Releases the address acquired from the dhcp server.

`dhcp client renew` - Renews the address lease.

debug dhcp client

This command sets the debug level for tracing the DHCP client module. The no form of the command disables the debug level for the DHCP client.

Default Disabled

Syntax
```
debug dhcp client { all | event | packets | errors | bind }
no debug dhcp client { all | event | packets | errors | bind }
```

Mode Privileged EXEC

`all` - All trace messages.

`event` - Trace management messages.

`packets` - Packets-related messages.

`errors` - Trace error code debug messages.

`bind` - Trace bind messages.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# debug dhcp client all
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`show dhcp client stats` - Displays the DHCP client statistics information.

show dhcp client stats

This command displays the DHCP client statistics.

Syntax
```
show dhcp client stats
```

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show dhcp client stats
Dhcp Client Statistics
--------------------------
Interface : vlanMgmt
Client IP Address : 0.0.0.0
Client Lease Time :0
Client Remain Lease Time : 0
Message Statistics
```

```
------------------
DHCP DISCOVER : 1
DHCP REQUEST : 0
DHCP DECLINE : 0
DHCP RELEASE : 0
DHCP INFORM : 0
DHCP OFFER : 1
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`dhcp client acquire` - Configures the current VLAN interface to dynamically acquire and IP address from the DHCP server.

`dhcp client release` - Releases the DHCP lease on the interface specified.

`dhcp client renew` - Renews the DHCP lease for the interface specified.

service dhcp

This command enables the DHCP server. The `no` form of this command disables the DHCP server. The DHCP Relay must be disabled before enabling the DHCP server.

Default	Disabled
Syntax	`service dhcp` `no service dhcp`
Mode	Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# service dhcp
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp server information` - Displays the DHCP server information.

ip dhcp pool

This command creates a DHCP server address pool and places the user in the DHCP pool configuration mode. The no form of the command deletes the DHCP server address pool. On execution of this command, the configuration mode changes to DHCP pool configuration mode, identified by the `(config-dhcp)#` prompt. In this mode, the administrator can configure pool parameters.

Default Address pools are not created by default.

Syntax
```
ip dhcp pool <index (1-2147483647)>
no ip dhcp pool <index (1-2147483647)>
```

Mode Global Configuration

`index` - Pool Number.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp pool 1
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`network` - Sets the network number and mask in DHCP server configuration parameters.

`excluded-address` - Creates an excluded pool to prevent the DHCP from assigning certain addresses.

`domain-name` - Sets the domain name in the DHCP server configuration parameters.

`dns-server` - Specifies the IP address of a DNS server.

`netbios-name-server` - Sets the NetBIOS (WINS) name servers in the DHCP server configuration parameters.

`netbios-node-type` - Sets the NetBios node type in the DHCP server configuration parameters.

`default-router` - Sets the default router in the DHCP server configuration parameters.

`option` - Sets the pool specific DHCP server option.

`lease` - Sets the lease period.

`host hardware-type` - Specifies the hardware address of a Dynamic Host Configuration Protocol (DHCP) client.

`show ip dhcp server information` - Displays the DHCP server information.

`show ip dhcp server pools` - Displays the DHCP server pools.

ip dhcp next-server

This command sets the next boot server in the DHCP server configuration parameters. The no form of this command deletes the next boot server from the DHCP server configuration parameters.

Syntax `ip dhcp next-server <ip address>`
`no ip dhcp next-server`

Mode Global Configuration

`ip address` - IP address of the TFTP server.

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp next-server 12.0.0.1
(JGSM7224)(config)#
------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the DHCP server information.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

ip dhcp bootfile

This command sets the boot file name in the DHCP server configuration parameters. The no form of this command deletes the boot file name from the DHCP server configuration parameters.

Syntax `ip dhcp bootfile <bootfile (63)>`
`no ip dhcp bootfile`

Mode Global Configuration

`boot file` - Name of the file that specifies the boot image.

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp bootfile 53
(JGSM7224)(config)#
------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the DHCP server information.

ip dhcp

This command sets the DHCP server parameters such as enabling the ICMP echo mechanism or offer-reuse timeout. The `no` form of this command is used to set the DHCP server parameters, such as disabling the ICMP echo mechanism or server offer-reuse to its default value or removing a bind entry from the server binding table.

The DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client. If the ping is answered, the server will add this address to the excluded address pool.

Default `server-offer-reuse` default is 5

Syntax
```
ip dhcp{ping-packets|server-offer-reuse <timeout(1-120)>}
no ip dhcp{ping-packets|server-offer-reuse|binding <ip address>}
```

Mode Global Configuration

`ping packets` - Enable icmp echo's prior to assigning a pool address. The `no` form of this command option prevents the server from pinging pool addresses.

`server offer reuse` - The amount of time the DHCP server entity would wait for the `DHCP REQUEST` from the client before reusing the offer.

`binding` - The binding option if specified deletes the specified address from binding.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp ping-packets
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the DHCP server information.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

ip dhcp option

This command sets the DHCP server options.

Syntax `ip dhcp option <code (1-255)> {ascii <string> | hex <Hex String> | ip <address>}`

`no ip dhcp option <code(1-255)>`

Mode Global Configuration

`code` - Option Code.

`ascii` - ASCII string.

`hex` - Hexadecimal string.

`ip` - IP address.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp option 19 hex 01
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

The subnet-specific options take precedence over global options and the host-specific options take precedence over global and subnet options.

RFC 2132 provides details about option code to option name mapping and the option length information.

Note: When in HEX format, two HEX chars are regarded as 1 byte. For example, the HEX string ef9a's length is 2, because the "ef" is one octet. The following is the list of supported and configurable DHCP options with their corresponding option length values:

- Options 19, 20, 27, 29, 30, 31, 34, 36, 39, 46 must have a length of 1
- Options 12, 14, 15, 17, 18, 40, 43, 47, 64, 66, 67 must have a length >=1
- Option 16 must have minimum length 4 and the value for this option must be an IP address and Option 25 can have a length of 2 and 2*n
- Option 68 must have length 4 and the value for this option must be an IP address
- Options 2-11, 41, 42, 44, 45, 48, 49, 65, 69, 70-76 must have a length of 4. Value for these options must be an IP address
- Options 21, 33 must have minimum length as 8 and 8*n
- Options 0, 1, 22-24, 26, 28, 32, 35, 37, 38, 50-63, 77-255 are not configurable using this command
- Option 1 is set when configuring the network mask

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server pools` - Displays the DHCP server pools.

`option` - Sets the pool specific DHCP server option.

network

This command sets the network IP address and mask in DHCP server configuration parameters. The no form of the command deletes the network IP address and mask from DHCP server configuration. This command is valid for DHCP sub network address pools only.

Syntax `network <network-IP>{<mask>| / <prefix-length (1-31)> } [start-ip <ucast_addr>] [end-ip <ucast_addr>]`
`no network`

Mode DHCP Pool Configuration

`network-IP` - Network IP address of the DHCP pool.

`mask` - Subnet mask of the DHCP pool.

`prefix-length` - The number of bits that comprise the address prefix. Prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

`start ip` - Start IP address of the pool.

`end ip` - End IP address of the pool.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# network 20.0.0.0 255.0.0.0 start-ip 20.0.0.10
(JGSM7224)(dhcp-config)#
--------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the server information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

excluded-address

This command creates an excluded pool to prevent the DHCP Server from assigning certain addresses. The no form of the command deletes the excluded pool. The DHCP server assumes that all pool addresses can be assigned to clients. This command is used to

exclude a single IP address or a range of IP addresses. If a client sends a DECLINE packet to decline an address, this address will be added to the excluded address pool.

Syntax

```
excluded-address <low-address> <high-address>
no excluded-address <low-address> <high-address>
```

Mode DHCP Pool Configuration

low-address - The excluded IP address, or first IP address in an excluded address range.
high-address - The last IP address in the excluded address range.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# excluded-address 20.0.0.1 20.0.0.30
(JGSM7224)(dhcp-config)#
--------------------------------------------------------------------------------
```

Related Commands

network - Sets the network IP and mask in DHCP server configuration parameters.

service dhcp - Enables the DHCP server.

show ip dhcp server information - Displays the server information.

show ip dhcp server pools - Displays the DHCP server pools.

show ip dhcp server binding - Displays the DHCP server binding information.

show ip dhcp server statistics - Displays the DHCP server statistics.

domain-name

This command sets the domain name in the DHCP server configuration parameters. The no form of the command deletes the domain name from the DHCP server configuration parameters. The configuration of this command takes effect only after configuring the network address pool using the network command.

Syntax

```
domain-name <domain (63)>
no domain-name
```

Mode DHCP Pool Configuration

domain - Client's domain name string.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# domain-name netgear
(JGSM7224)(dhcp-config)#
--------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the server information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

`network` - Configures the network IP address of the DHCP Address Pool.

dns-server

This command is used to specify the IP address of a DNS server available to a DHCP client. The no form of the command deletes the DNS server from the DHCP server configuration parameters. If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses. The configuration of this command takes effect only after configuring the network address pool using network command.

Syntax `dns-server <ip address>`
`no dns-server`

Mode DHCP Pool Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# dns-server 20.0.0.1
(JGSM7224)(dhcp-config)#
--------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the server information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

`network` - Configures the network IP address of the DHCP Address Pool.

netbios-name-server

This command sets the NetBIOS (WINS) name servers in the DHCP server configuration parameters. The no form of the command deletes the NetBIOS name server from the DHCP configuration parameters. The configuration of this command takes effect only after configuring the network address pool using network command.

Syntax `netbios-name-server <ip address>`
`no netbios-name-server`

Mode DHCP Pool Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# netbios-name-server 20.0.0.3
(JGSM7224)(dhcp-config)#
-----------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the server information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

`network` - Configures the network IP address of the DHCP Address Pool.

netbios-node-type

This command is used to set the NetBios node type in the DHCP server configuration parameters. The no form of this command is used to delete the NetBios node type from the DHCP server configuration parameters.

The NetBIOS node type for Microsoft DHCP clients can be one of the four settings: broadcast, peer-to-peer, mixed, or hybrid. The recommended type is hybrid node. The configuration of this command takes effect only after configuring the network address pool using network command.

Syntax `netbios-node-type{ <0-FF> | b-node | h-node | m-node | p-node}`
`no netbios-node-type`

Mode DHCP Pool Configuration

`0-FF` - Node type value.

`b-node` - Broadcast node.

`h-node` - Hybrid node.

`m-node` - Mixed node.

`p-node` - Peer-to-peer node.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# netbios-node-type h-node
(JGSM7224)(dhcp-config)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp-server` - Enables the DHCP server.

`show ip dhcp server information` - Displays the server information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

`network` - Configures the network IP address of the DHCP Address Pool.

default-router

This command sets the default router in the DHCP server configuration parameters. The `no` form of the command deletes the default router from the DHCP server configuration parameters. The configuration of this command takes effect only after configuring the network address pool using network command.

Syntax `default-router <ip address>`
`no default-router`

Mode DHCP Pool Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# default-router 10.23.2.99
(JGSM7224)(dhcp-config)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp-server` - Enables the DHCP server.

`show ip dhcp server information` - Displays the server information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

`network` - Configures the network IP address of the DHCP Address Pool.

option

This command sets the pool-specific DHCP server option. The `no` form of the command deletes the pool-specific DHCP server option.

The subnet-specific options take precedence over global options and the host specific options take precedence over global and subnet options.

RFC 2132 provides details about option code to option name mapping and the option length information.

The following is the list of supported and configurable DHCP options with their corresponding option length values:

- Options 19, 20, 27, 29, 30, 31, 34, 36, 39, 46 must have length 1
- Options 12, 14, 15, 17, 18, 40, 43, 47, 64, 66, 67 must have length>=1
- Option 16 must have minimum length 4 and the value for this option must be an IP address and Option 25 can have a length of 2 and 2*n
- Option 68 must have length 4 and the value for this option must be an IP address
- Options 2-11, 41, 42, 44, 45, 48, 49, 65, 69, 70-76 must have a length of 4. Value for these options must be an IP address
- Options 21, 33 must have minimum length as 8 and 8*n
- Options 0, 1, 22-24, 26, 28, 32, 35, 37, 38, 50-63, 77-255 are not configurable using this command
- Option 1 is set when configuring the network mask

The network pool must be configured prior to the execution of this command. Only then the configured option is visible to the user in the `show` command output. If the network pool is deleted, then the option configured for that network pool will also be deleted.

Syntax `option <code (1-255)> ascii <string> | hex <Hex String> | ip <address>}`
`no option <code (1-255)>`

Mode DHCP Pool Configuration

`code` - Option Code.

`ascii` - ASCII string.

`hex` - Hexadecimal string.

`ip` - IP address.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# option 19 hex f
(JGSM7224)(dhcp-config)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`ip dhcp pool` - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode.

`ip dhcp option` - Sets the DHCP server options.

`network` - Sets the network IP and mask in DHCP server configuration parameters.

`show ip dhcp server pools` - Displays the DHCP server pools.

lease

This command configures the duration of the lease for an IP address that is assigned from JGSM7224 Dynamic Host Configuration Protocol (DHCP) Server to a DHCP client. The no form of this command restores the default value of 3600 seconds.

Default	3600 seconds
Syntax	`lease {<days (0-365)> [<hours (0-23)> [<minutes (0-59)>]] | infinite}` `no lease`
Mode	DHCP Pool Configuration

`days` - Duration of the lease in number of days.

`hours` - Number of hours in lease.

`minutes` - Number of minutes in lease.

`infinite` - Duration of the lease is unlimited.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# lease 1
(JGSM7224)(dhcp-config)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the server information.

`show ip dhcp server pools` - Displays the DHCP server pools.

`show ip dhcp server binding` - Displays the DHCP server binding information.

`show ip dhcp server statistics` - Displays the DHCP server statistics.

utilization threshold

This command sets the pool utilization threshold value in percentage. If the pool utilization reaches this threshold level, a syslog event and an SNMP trap message will be generated. The `no` form of this command sets the pool utilization threshold to its default value.

Default 75

Syntax
```
utilization threshold { <integer (0-100)> }
no utilization threshold
```

Mode DHCP Pool Configuration

`days` - Duration of the lease in number of days.

`hours` - Number of hours in lease.

`minutes` - Number of minutes in lease.

`infinite` - Duration of the lease is unlimited.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# utilization threshold 76
(JGSM7224)(dhcp-config)#
-------------------------------------------------------------------------------
```

Related Commands

`show ip dhcp server pools` - Displays the DHCP server pools.

`logging` - Enables Syslog server and configures the Syslog Server IP address, the log-level and other Syslog related parameters.

host hardware-type

This command specifies the hardware address of a Dynamic Host Configuration Protocol (DHCP) client and host specific DHCP options. The `no` form of the command deletes the host

option. The subnet-specific options take precedence over global options and the host specific options take precedence over global and subnet options.

Syntax `host hardware-type <type (0-1)> client-identifier <mac-address> option <code 1-254)> {ascii <string> | hex <Hex String> | ip <address>}`

`no host hardware-type <host-hardware-type (0-1)> client-identifier <client-mac-address> option <code (1-254)>`

Mode DHCP Pool Configuration

`type` - 0 means an identifier other than a hardware address type, 1 means the hardware address type.

`client identifier` - Host MAC address or an identifier

`option` - The tag octet of the DHCP option.

`ascii` - ASCII String.

`hex` - Hex String.

`ip` - Host IP address.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(dhcp-config)# host hardware-type 1 client-identifier
00:11:22:33:44:55 option 3 ip 10.0.0.1
(JGSM7224)(dhcp-config)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`ip dhcp pool` - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode.

debug ip dhcp server

This command specifies the hardware address of a Dynamic Host Configuration Protocol (DHCP) client and host specific DHCP options. The no form of the command deletes the host option.

Default Disabled

Syntax `debug ip dhcp server {all | events | packets | errors | bind}`

`no debug ip dhcp server {all | events | packets |errors | bind}`

Mode Privileged EXEC

`all` - All trace messages.

`events` - Trace management messages.

`packets` - Packet related messages.

`errors` - Trace error code debug messages.

`bind` - Trace bind messages.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug ip dhcp server all
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`show ip dhcp server information` - Displays the server information.

`show ip dhcp server binding` - Displays the DHCP server binding information.

show ip dhcp server information

This command displays the DHCP server information.

Syntax	`show ip dhcp server information`
Mode	Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip dhcp server information
DHCP server status : Enable
Send Ping Packets : Disable

Debug level: None
Server Address Reuse Timeout : 5 secs

Next Server Address : 0.0.0.0
Boot file name : None
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`ip dhcp next-server` - Sets the next boot server in the DHCP server configuration parameters.

`ip dhcp bootfile` - Sets the boot file name in the DHCP server configuration parameters.

`ip dhcp` - Sets the DHCP server parameters such as enabling the ICMP echo mechanism or offer-reuse timeout.

show ip dhcp server pools

This command displays the DHCP server pools.

Syntax `show ip dhcp server pools`

Mode Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show ip dhcp server pools
Pool Id : 1
-----------------------------------------
Subnet : 12.0.0.0
Subnet Mask : 255.0.0.0
Lease time : 180 secs
Start Ip : 12.0.0.1
End Ip : 12.255.255.254

Exclude Address Start IP : 12.0.0.1
Exclude Address End IP : 12.0.0.10
Pool Id : 2
-----------------------------------------
Subnet : 20.0.0.0
Subnet Mask : 255.0.0.0
Lease time : 7200 secs
Start Ip : 20.0.0.1
End Ip : 20.255.255.254
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`ip dhcp pool` - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode.

`lease` - Configures the duration of the lease for an IP address that is assigned from JGSM7224 Dynamic Host Configuration Protocol (DHCP) Server to a DHCP client.

`network` - Sets the network IP and mask in DHCP server configuration parameters.

show ip dhcp server binding

This command displays the DHCP server binding information. Binding refers to the state of binding. This can be offered, assigned, or probing. In offered state the offer is sent, but no req has been received from the client. In assigned state the address is assigned to the client. In probing state the address is currently being probed by the DHCP server.

Syntax `show ip dhcp server binding`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip dhcp server binding
Ip Hw Hw Alloc Expire Binding
Address Type Address Method Time State

------- ---- ------- ------ ------ -------
12.0.0.11 Ethernet 00:01:02:03:04:41 Dynamic 161 Assigned
20.0.0.1 Ethernet 00:01:02:03:04:31 Dynamic 7152 Assigned

(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp` - Enables the DHCP server.

`host hardware-type` - Specifies the hardware address of a Dynamic Host Configuration Protocol (DHCP) client.

`ip dhcp option` - Sets the DHCP server options.

show ip dhcp server statistics

This command displays the DHCP server statistics.

Syntax `show ip dhcp server statistics`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip dhcp server statistics
Address pools : 2
Message Received
------- --------
DHCPDISCOVER 6
DHCPREQUEST 2
DHCPDECLINE 0
DHCPRELEASE 0

DHCPINFORM 0

Message Sent
------- ----
DHCPOFFER 6
DHCPACK 2
DHCPNAK 0

(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`service dhcp-server` - Enables the DHCP server.

`ip dhcp pool` - Creates a DHCP server address pool and places the user in the DHCP pool configuration mode.

`ip dhcp` - Sets the DHCP server parameters such as enabling the ICMP echo mechanism or offer-reuse timeout.

`show ip dhcp server pools` - Displays the DHCP server pools.

DHCP L2 Relay

7

In some networks, DHCP servers rely on Relay Agent Information option appended by Relay Agents for IP address and other parameter assignment policies. This works fine when end hosts are directly connected to Relay Agents. In some network configurations, one or more Layer 2 devices might reside between DHCP clients and Relay agent. In these network scenarios, it is difficult to use the Relay Agent Information option for IP address and other parameter assignment policies effectively. So there is a need for the device that is closest to the end hosts to append a Relay Agent Information option in DHCP messages. These devices are typically known as Layer 2 Relay Agents.

dhcp l2relay

This command enables or disables the DHCP l2 relay globally or on a specific interface.

Format `dhcp l2relay`
`no dhcp l2relay`

Mode
- Global Configuration Mode
- Interface Configuration Mode

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config)# dhcp l2relay
(JGSM7224)(config)#

(JGSM7224)(config)# interface 0/1
(JGSM7224)(config-if)# dhcp l2relay
------------------------------------------------------------------------------
```

Related Commands

`show dhcp l2relay all` - Displays all configuration of the DHCP l2 Relay

`show dhcp l2relay interface` - Displays the DHCP l2 Relay interface configuration

dhcp l2relay vlan

This command enables or disables the DHCP l2 relay on a specific vlan.

Format `dhcp l2relay vlan <vlan_list>`
`no dhcp l2relay vlan <vlan_list>`

Mode Global Configuration Mode

`<vlan_list>` - Enter VLAN IDs in range <1-4094>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# dhcp l2relay vlan 1-3,4
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`show dhcp l2relay all` - Displays all configuration of the DHCP l2 Relay

`show dhcp l2relay agent-option` - Displays the DHCP l2 Relay agent-option

`show dhcp l2relay vlan` - Displays the DHCP l2 Relay vlan configuration

dhcp l2relay circuit-id

This command enables or disables the DHCP l2 relay circuit-id insertion of option 82 on a specific vlan.

Format `dhcp l2relay circuit-id <vlan_list>`
`no dhcp l2relay circuit-id <vlan_list>`

Mode Global Configuration Mode

`<vlan_list>` - Enter VLAN IDs in range <1-4094>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# dhcp l2relay circuit-id 1-3,4
(JGSM7224)(config)#
The format of the circuit id:
       Length      Length
         |           |
    1   10  0   8   VLAN     SLOT    PORT
```

```
-----------------------------------------
1byte 1byte 1byte 1byte 4 bytes 2bytes 2bytes
----|---------|----------------------------
    |         |
 SubOption  CircuitID
   Type       Type
-------------------------------------------------------------------------------
```

Related Commands

`show dhcp l2relay all` - Displays all configuration of the DHCP l2 Relay

`show dhcp l2relay agent-option` - Displays the DHCP l2 Relay agent-option

`show dhcp l2relay circuit-id` - Displays the DHCP l2 Relay circuit id configuration

dhcp l2relay remote-id

This command enables or disables the DHCP l2 relay remote-id insertion of option 82 on a specific vlan. If it is disabled, the remote-id will not be added.

Format `dhcp l2relay remote-id <string> <vlan_list>`
`no dhcp l2relay remote-id <vlan_list>`

Mode Global Configuration Mode

`<vlan_list>` - Enter VLAN IDs in range <1-4094>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

`<String>` - Remote-id suboption string of n charaters(1-32)

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# dhcp l2relay remote-id netgear 1-3,4
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`show dhcp l2relay all` - Displays all configuration of the DHCP l2 Relay

`show dhcp l2relay agent-option` - Displays the DHCP l2 Relay agent-option

`show dhcp l2relay remote-id` - Displays the DHCP l2 Relay remote ID configuration

dhcp l2relay trust

This command set the interface as trust/untrust.

Format	`dhcp l2relay trust` `no dhcp l2relay trust`
Mode	Interface Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# interface 0/1
(JGSM7224)(config-if)# dhcp l2relay trust
-------------------------------------------------------------------------------
```

Related Commands

`show dhcp l2relay all` - Displays all configuration of the DHCP l2 Relay

`show dhcp l2relay interface` - Displays the DHCP l2 Relay interface configuration

show dhcp l2relay all

This command shows the complete configuration of the DHCP l2 Relay.

Format	show dhcp l2relay all
Mode	Privileged Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show dhcp l2relay all
DHCP L2 Relay is Disabled. DHCP L2 Relay Debug:
Interface    L2RelayMode   TrustMode
0/1          Disabled      Untrusted
0/2          Disabled      Untrusted
0/3          Disabled      Untrusted
0/4          Disabled      Untrusted
0/5          Disabled      Untrusted
0/6          Disabled      Untrusted
0/7          Disabled      Untrusted
0/8          Disabled      Untrusted
0/9          Disabled      Untrusted
0/10         Disabled      Untrusted
0/11         Disabled      Untrusted
```

```
0/12          Disabled      Untrusted
0/13          Disabled      Untrusted
0/14          Disabled      Untrusted
0/15          Disabled      Untrusted
0/16          Disabled      Untrusted
0/17          Disabled      Untrusted
0/18          Disabled      Untrusted
0/19          Disabled      Untrusted
0/20          Disabled      Untrusted
0/21          Disabled      Untrusted
0/22          Disabled      Untrusted
0/23          Disabled      Untrusted
0/24          Disabled      Untrusted

VLAN Id     L2 Relay   CircuitId    RemoteId
-------     --------   ---------    --------
1           Enabled    Disabled
2           Enabled    Enabled      netgear
3           Enabled    Disabled
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`dhcp l2relay` - Configure the dhcp l2 relay globally or on specific interfaces

`dhcp l2relay vlan` - Configure the dhcp l2 relay on specific VLAN

`dhcp l2relay circuit-id` - Configures the dhcp l2 relay circuit id on specific VLAN

`dhcp l2relay remote-id` - Configures the dhcp l2 relay remote ID on specific VLAN

`dhcp l2relay trust` - Configures the dhcp l2 relay trust mode on specific interface

show dhcp l2relay agent-option

This command shows the DHCP l2 Relay agent-option.

Format	`show dhcp l2relay agent-option`
Mode	Privileged Configuration Mode

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show dhcp l2relay agent-option vlan 1-3
DHCP L2 Relay is Disabled.
DHCP L2 Relay Debug:
VLAN Id   L2 Relay   CircuitId   RemoteId
-------   --------   ---------   --------
1         Enabled    Disabled
2         Enabled    Enabled      netgear
3         Enabled    Disabled
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`dhcp l2relay vlan` - Configure the dhcp l2 relay on specific VLAN

`dhcp l2relay circuit-id` - Configures the dhcp l2 relay circuit ID on specific VLAN

`dhcp l2relay remote-id` - Configures the dhcp l2 relay remote ID on specific VLAN

show dhcp l2relay circuit-id

This command shows the DHCP l2 Relay circuit-id enabled on a specific vlan.

Format	`show dhcp l2relay circuit-id vlan <vlan-list>`
Mode	Privileged Configuration Mode

`<vlan_list>` - Enter VLAN IDs in range <1-4094>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show dhcp l2relay circuit-id vlan 1-3
DHCP L2 Relay is Disabled.
DHCP L2 Relay Debug:
DHCP Circuit-Id option is enabled on the following VLANs: 2
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Command

`dhcp l2relay circuit-id` - Configures the dhcp l2 relay circuit ID on a specific VLAN

show dhcp l2relay remote-id

This command shows the DHCP l2 Relay remote-id on a specific vlan.

Format `show dhcp l2relay remote-id vlan <vlan-list>`

Mode Privileged Configuration Mode

`<vlan_list>` - Enter VLAN IDs in range <1-4094>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Example

```
-------------------------------------------------------------------------------
(JGSM7224 # show dhcp l2relay remote-id vlan 1-3
DHCP L2 Relay is Disabled.
DHCP L2 Relay Debug:
VLAN ID      RemoteId
1
2            netgear
3
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`dhcp l2relay remote-id` - Configures the dhcp l2 relay remote ID on a specific VLAN

show dhcp l2relay vlan

This command shows the DHCP l2 Relay enabled on a specific vlan.

Format `show dhcp l2relay vlan <vlan-list>`

Mode Privileged Configuration Mode

`<vlan_list>` - Enter VLAN IDs in range <1-4094>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show dhcp l2relay vlan 1-3
DHCP L2 Relay is Disabled.
DHCP L2 Relay Debug:
DHCP L2 Relay is enabled on the following VLANs: 1-3
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`dhcp l2relay vlan` - Configures the dhcp l2 relay on a specific VLAN

show dhcp l2relay stats

This command shows the DHCP l2 Relay statistics.

Format `show dhcp l2relay stats interface { all | <slot/port> | port-channel <1-8> }`

Mode Privileged Configuration Mode

`<slot/port>` - Enter interface in slot/port format.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show dhcp l2relay stats interface all
Interface  UntrustedServer   UntrustedClient  TrustedServer    TrustedClient
           MsgsWithOpt82     MsgsWithOpt82    MsgsWithoutOpt82 MsgsWithoutOpt82
-------------------------------------------------------------------------------
0/1          0                 0                0                0
0/2          0                 0                0                0
0/3          0                 0                0                0
0/4          0                 0                0                0
0/5          0                 0                0                0
0/6          0                 0                0                0
0/7          0                 0                0                0
0/8          0                 0                0                0
0/9          0                 0                0                0
0/10         0                 0                0                0
0/11         0                 0                0                0
0/12         0                 0                0                0
0/13         0                 0                0                0
0/14         0                 0                0                0
0/15         0                 0                0                0
0/16         0                 0                0                0
0/17         0                 0                0                0
0/18         0                 0                0                0
0/19         0                 0                0                0
0/20         0                 0                0                0
0/21         0                 0                0                0
0/22         0                 0                0                0
0/23         0                 0                0                0
```

```
0/24         0                0               0                0

(JGSM7224)# show dhcp l2relay stats interface 0/1

Interface  UntrustedServer   UntrustedClient  TrustedServer    TrustedClient
           MsgsWithOpt82     MsgsWithOpt82    MsgsWithoutOpt82 MsgsWithoutOpt82
-------------------------------------------------------------------------------
0/1          0                0               0                0
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`clear dhcp l2relay statistics` - Clear the dhcp l2 relay statistics

show dhcp l2relay interface

This command shows the DHCP l2 Relay interface configuration.

Format `show dhcp l2relay interface { all | <slot/port> | port-channel <1-8> }`

Mode Privileged Configuration Mode

`<slot/port>` - Enter interface in slot/port format.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show dhcp l2relay interface all
DHCP L2 Relay is Disabled.
DHCP L2 Relay Debug:
Interface       L2RelayMode       TrustMode
0/1             Disabled          Untrusted
0/2             Disabled          Untrusted
0/3             Disabled          Untrusted
0/4             Disabled          Untrusted
0/5             Disabled          Untrusted
0/6             Disabled          Untrusted
0/7             Disabled          Untrusted
0/8             Disabled          Untrusted
0/9             Disabled          Untrusted
0/10            Disabled          Untrusted
0/11            Disabled          Untrusted
0/12            Disabled          Untrusted
0/13            Disabled          Untrusted
```

```
0/14            Disabled          Untrusted
0/15            Disabled          Untrusted
0/16            Disabled          Untrusted
0/17            Disabled          Untrusted
0/18            Disabled          Untrusted
0/19            Disabled          Untrusted
0/20            Disabled          Untrusted
0/21            Disabled          Untrusted
0/22            Disabled          Untrusted
0/23            Disabled          Untrusted
0/24            Disabled          Untrusted

(JGSM7224)# show dhcp l2relay interface 0/1

DHCP L2 Relay is Disabled.

DHCP L2 Relay Debug:

Interface      L2RelayMode    TrustMode
---------      -----------    ---------
0/1            Disabled       Untrusted
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`dhcp l2relay` - Configures the dhcp l2 relay globally or on specific interfaces

`dhcp l2relay trust` - Configures the dhcp l2 relay trust mode on specific interface

clear dhcp l2relay statistics

This command clears the DHCP l2 Relay interface statistics.

Format	`clear dhcp l2relay statistics`
Mode	Privileged Configuration Mode

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# clear dhcp l2relay statistics
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`show dhcp l2relay stats` - Displays the dhcp l2 relay statistics

debug dhcp l2relay

This command debugs the DHCP l2 Relay process.

Format `debug dhcp l2relay { all | event | fail | packet | trace }`
`no debug dhcp l2relay { all | event | fail | packet | trace }`

Mode Privileged Configuration Mode

`all` - debug all

`event` - debug the event

`fail` - debug the failure

`packet` - debug the packet

`trace` - trace debug

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# debug dhcp l2relay all
(JGSM7224)#
--------------------------------------------------------------------------------
```

DHCP Snooping

8

DHCP snooping is a DHCP security feature that filters untrusted DHCP messages and builds and maintains a DHCP snooping binding table. An untrusted message is one that is received from outside the network or firewall and that can cause traffic attacks within your network.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

ip dhcp snooping

Use this command to enable or disable DHCP snooping globally. DHCP snooping cannot be enabled with the DHCP server at the same time.

Format `ip dhcp snooping`
`no ip dhcp snooping`

Mode Global Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp snooping
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping` - Display the DHCP Snooping global

ip dhcp snooping verify mac-address

Use this command to enable or disable verification of the source MAC address with the client hardware address in the received DHCP message.

Format `ip dhcp snooping verify mac-address`
`no ip dhcp snooping verify mac-address`

Mode Global Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp snooping verify mac-address
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping` - Display the DHCP Snooping global

ip dhcp snooping vlan

Use this command to enable or disable DHCP snooping on a list of comma-separated VLAN ranges.

Format `ip dhcp snooping vlan <vlan_list>`
`no ip dhcp snooping vlan <vlan_list>`

Mode Global Configuration Mode

`<vlan_list>` - Enter VLAN IDs in range <1-4094>. Use '-' to specify a range, or ',' to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp snooping vlan 1-3
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping` - Display the DHCP Snooping global

ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format `ip dhcp snooping binding <ucast_mac> vlan <1-4094> <ucast_addr> interface { <slot/port> | port-channel <1-8> }`

`no ip dhcp snooping binding <ucast_mac>`

Mode Global Configuration Mode

`<ucast_mac>` - Enter the MAC address field of the binding.

`<ucast_addr>` - Enter the IPv4 address field of the binding.

`<slot/port>` - Enter interface in slot/port format.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp snooping binding 00:11:22:33:44:55 vlan 1
192.168.0.10 interface 0/1
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`show ip dhcp snooping binding` - Display the DHCP Snooping binding

`clear ip dhcp snooping binding` - Clear the DHCP Snooping binding

ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local of a remote file on a given IP machine.

Format `ip dhcp snooping database { <tftp_url> | local }`

Mode Global Configuration Mode

`<tftp_url>` - Remote server address and filename in the format `tftp://<ipv4address>/<filename>`

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp snooping database tftp://192.168.0.10/dhsnp.cfg
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping database` - Display the DHCP Snooping configuration related to the database persistency

ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.The `no` command sets the value to the default (300).

Format `ip dhcp snooping database write-delay <15-86400>`
`no ip dhcp snooping database write-delay`

Mode Global Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip dhcp snooping database write-delay 100
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping database` - Display the DHCP Snooping configuration related to the database persistency

ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come. The default rate is 15 pps with a range from 0 to 100 pps. The default burst level is 1 second with a range of 1 to 15 seconds. The limit `none` will disable the control. The `no` form of the command sets the limit to the default.

Format `ip dhcp snooping limit { none | rate <0-100> [ burst interval <1-15> ] }`
`no ip dhcp snooping limit`

Mode Interface Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# interface 0/1
(JGSM7224)(config-if)# ip dhcp snooping limit rate 25 burst interval 6
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping interfaces` - Display the DHCP Snooping per port configurations

ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping. The default is disabled.

Format `ip dhcp snooping log-invalid`
`no ip dhcp snooping log-invalid`

Mode Interface Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# interface 0/1
(JGSM7224)(config-if)# ip dhcp snooping log-invalid
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping interfaces` - Display the DHCP Snooping per port configurations

ip dhcp snooping trust

Use this command to configure the port as trusted or untrusted. The default is untrusted.

Format `ip dhcp snooping trust`
`no ip dhcp snooping trust`

Mode Interface Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# interface 0/1
(JGSM7224)(config-if)# ip dhcp snooping trust
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping interfaces` - Display the DHCP Snooping per port configurations

show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations.

Format `show ip dhcp snooping`

Mode Privileged Configuration Mode

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show ip dhcp snooping
DHCP Snooping Mode:     Disabled
MAC Address Validation: Disabled
DHCP Snooping is configured on the following VLANs: 1-3
DHCP Snooping Debug:  event   bind
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`ip dhcp snooping` - Configure the DHCP Snooping globally

`ip dhcp snooping verify mac-address` - Configure the DHCP Snooping verification

`ip dhcp snooping vlan` - Configure the DHCP Snooping on specific vlan

`debug ip dhcp snooping` - Configure the DHCP Snooping debug

show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries.

Format `show ip dhcp snooping binding`

Mode Privileged Configuration Mode

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show ip dhcp snooping binding
MacAddress      IpAddress     VLAN Interface Type   Lease(sec)
0011.2233.4455  192.168.0.25   1   0/1       Static
Total Number Of Bindings: 1
```

```
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`ip dhcp snooping binding` - Configure the static binding

show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format	`show ip dhcp snooping database`
Mode	Privileged Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip dhcp snooping database

Log File Store Type: remote
Agent IP:            192.168.0.10
Agent File:          dhsnp.cfg
Write-delay:         300 seconds.

(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`ip dhcp snooping database` - Configure the persistent location of the DHCP Snooping database

`ip dhcp snooping database write-delay` - Configure the interval in seconds at which the DHCP Snooping database will be persisted

show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format	`show ip dhcp snooping statistics`
Mode	Privileged Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip dhcp snooping statistics
Interface  MAC Verify   Client Ifc   DHCP Server
           Failures     Mismatch     Msgs Rec'd
0/1        0            0            0
0/2        0            0            0
0/3        0            0            0
0/4        0            0            0
0/5        0            0            0
0/6        0            0            0
0/7        0            0            0
0/8        0            0            0
0/9        0            0            0
0/10       0            0            0
0/11       0            0            0
0/12       0            0            0
0/13       0            0            0
0/14       0            0            0
0/15       0            0            0
0/16       0            0            0
0/17       0            0            0
0/18       0            0            0
0/19       0            0            0
0/20       0            0            0
0/21       0            0            0
0/22       0            0            0
0/23       0            0            0
0/24       0            0            0
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`clear ip dhcp snooping statistics` - Clear the DHCP snooping statistics

show ip dhcp snooping interfaces

Use this command to display the DHCP Snooping per port configurations.

Format	`show ip dhcp snooping interfaces`
Mode	Privileged Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip dhcp snooping interfaces
Interface   Trust State   Logging-Invalid   Rate Limit   Burst Interval
                          Packets           (pps)        (seconds)
0/1         No            Enabled           25           6
0/2         No            Disabled          15           1
0/3         No            Disabled          15           1
0/4         No            Disabled          15           1
0/5         No            Disabled          15           1
0/6         No            Disabled          15           1
0/7         No            Disabled          15           1
0/8         No            Disabled          15           1
0/9         No            Disabled          15           1
0/10        No            Disabled          15           1
0/11        No            Disabled          15           1
0/12        No            Disabled          15           1
0/13        No            Disabled          15           1
0/14        No            Disabled          15           1
0/15        No            Disabled          15           1
0/16        No            Disabled          15           1
0/17        No            Disabled          15           1
0/18        No            Disabled          15           1
0/19        No            Disabled          15           1
0/20        No            Disabled          15           1
0/21        No            Disabled          15           1
0/22        No            Disabled          15           1
0/23        No            Disabled          15           1
0/24        No            Disabled          15           1
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`ip dhcp snooping limit` - Configure the DHCP snooping packet control

`ip dhcp snooping log-valid` - Configure the DHCP snooping logging

`ip dhcp snooping trust` - Configure the DHCP snooping port mode

clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format `clear ip dhcp snooping binding [interface { <slot/port> | port-channel <1-8>}] | [vlan <1-4094>]`

Mode Privileged Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# clear ip dhcp snooping binding vlan 1
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`ip dhcp snooping binding` - Configure the static binding

clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format `clear ip dhcp snooping statistics`

Mode Privileged Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# clear ip dhcp snooping statistics
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping statistics` - Displays the DHCP snooping statistics

debug ip dhcp snooping

Use this command to debug the DHCP Snooping process.

Format `debug dhcp l2relay { all | bind | event | fail | packet | trace }`
`no debug dhcp l2relay { all | bind | event | fail | packet | trace }`

Mode Privileged Configuration Mode

`all` - debug all

`bind` - debug binding

`event` - debug the event

`fail` - debug the failure

`packet` - debug the packet

`trace` - trace debug

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug ip dhcp snooping all
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show ip dhcp snooping` - Displays the DHCP snooping global

SNTP

9

SNTP is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It is a simplified access strategy for servers and clients using NTP as now specified and deployed in the Internet. The access paradigm is identical to the UDP/TIME Protocol and, in fact, it should be easily possible to adapt a UDP/TIME client implementation to operate using SNTP. Moreover, SNTP is also designed to operate in a dedicated server configuration including an integrated radio clock.

sntp

This command enters SNTP configuration mode.

Syntax	`sntp`
Mode	Global configuration

`sntp` - Enter SNTP configuration mode.

Example

```
----------------------------------------------------------------------------
(JGSM7224)(config)# sntp
(JGSM7224)(config-sntp)#
----------------------------------------------------------------------------
```

set sntp client

This command enables or disables SNTP client module.

Default	Disabled
Syntax	`set sntp client { enable | disable }`
Mode	SNTP Configuration

`enable` - Enable the SNTP client module.

`disable` - Disable the SNTP client module.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# set sntp client enable
--------------------------------------------------------------------------------
```

Related Command

`show sntp client` - Displays SNTP configuration information.

sntp client version

This command sets the operation of the SNTP for the client.

Default `v4`

Syntax `sntp client version { v1 | v2 | v3 | v4 }`

Mode SNTP Configuration

`v1` - SNTP Version 1
`v2` - SNTP Version 2
`v3` - SNTP Version 3
`v4` - SNTP Version 4

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)-sntp)# sntp client version v3
--------------------------------------------------------------------------------
```

Related Command

`show sntp client` - Displays SNTP configuration information.

sntp client port

This command sets the listening port for the SNTP client greater than 1024, since below 1024 is reserved. Therefore the configurable listening port for a SNTP client starts at 1025. The no form of command deletes the listening port for the SNTP client and sets the default value. The SNTP client should be enabled.

Default `123`

Syntax `sntp client port <portno(1025-65535)>`
`no sntp client port`

Mode SNTP Configuration

`port no` - Listening port for SNTP client

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-sntp)# sntp client port 1026
-----------------------------------------------------------------------------
```

Related Command

`show sntp client` - Displays SNTP configuration information.

sntp client clock-format

This command sets the system clock format as AM PM format or HOURS format. The SNTP clock format configuration in the switch is as follows:

Date - Hours, Minutes, Seconds, Date Month and Year

Month - Jan, Feb, Mar, and so on.

Year - yyyy

Default `hours`

Syntax `sntp client clock-format { ampm | hours }`

Mode SNTP Configuration

`am-pm` - Sets the system clock to am/pm format

`hours` - Sets the system clock to 24 hours format

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-sntp)# sntp client clock-format ampm
-----------------------------------------------------------------------------
```

Related Command

`show sntp clock` - Displays the current time.

clock timezone

This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT. The SNTP server must be enabled prior to the execution of this command.

Syntax `clock timezone <+/- UTC TimeDiff in Hrs:UTC TimeDiff in Min>`
`no clock timezone`

Mode SNTP Configuration

`+/-` - After or before UTC.

`UTC TimeDiff in Hrs` - UTC Time difference in hours

`UTC TimeDiff in Min` - UTC Time difference in minutes

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-sntp)# clock timezone +05:30
--------------------------------------------------------------------------------
```

Related Command

`show sntp client` - Displays SNTP configuration information.

clock summer-time

This command enables Daylight Saving Time. The no form of the command disables Daylight Saving Time.

Syntax `clock summer-time <week-day-month,hh:mm> <week-day-month,hh,mm>`
`no clock summer-time`

Mode SNTP Configuration

`week` - First, Second, Third, Forth, or Last week of month.

`Day` - Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.

`Month` - January, February, March, April, May, June, July, August, September, October, November, or December.

`hh:mm` - Time in hours and minutes

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-sntp)# clock summer-time First-Sun-Jan,12:12
Second-Sun-Mar,12:12
--------------------------------------------------------------------------------
```

Related Command

`show sntp client` - Displays SNTP configuration information.

set sntp server auto-discovery

This command configures the SNTP client status of auto-discovery of the server. The SNTP client addressing mode should be unicast.

Default Disabled

Syntax `set sntp server auto-discovery { enabled | disabled }`

Mode SNTP Configuration Mode

`enabled` - Enables the auto-discovery of the server.

`disabled` - Disables the auto-discovery of the server

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-sntp)# set sntp server auto-discovery enabled
-------------------------------------------------------------------------------
```

Related Command

`show sntp unicast-mode status` - Displays the SNTP Unicast Mode status

sntp unicast client poll-interval

This command configures the SNTP client poll interval. The SNTP client addressing mode should be unicast.

Default 6

Syntax `sntp unicast client poll-interval <value (4-14)>`

Mode SNTP Configuration

`value` - Poll interval value in seconds to the power of two.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-sntp)# sntp unicast client poll-interval 5
-------------------------------------------------------------------------------
```

Related Command

`show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

sntp unicast client poll-timeout

This command configures SNTP client maximum poll interval timeout. The SNTP client addressing mode should be unicast.

Default 5

Syntax `sntp unicast client poll-timeout <value (1-30) seconds>`

Mode SNTP Configuration

`value` - Maximum poll interval time out value in seconds.

Example

```
---------------------------------------------------------------------------
(JGSM7224)(config-sntp)# sntp unicast client poll-timeout 25
---------------------------------------------------------------------------
```

Related Command

`show sntp unicast-mode status` - Displays the SNTP Unicast Mode status

sntp unicast client poll-retry

This command configures SNTP client maximum retry poll count. The SNTP client addressing mode should be unicast.

Default 3

Syntax `sntp unicast client poll-retry <value (1-10) times>`

Mode SNTP Configuration

`value` - Maximum retry poll count value

Example

```
---------------------------------------------------------------------------
(JGSM7224)(config-sntp)# sntp unicast client poll-retry 10
---------------------------------------------------------------------------
```

Related Command

`show sntp unicast-mode status` - Displays the SNTP Unicast Mode status

sntp server

This command configures SNTP unicast server attributes. The no form of the command deletes the sntp unicast server attributes and sets them to the default. The SNTP client addressing mode should be unicast.

Syntax `sntp server <ipaddress|ipv6address|host-name> [port <integer(1025-36564)>][{primary|secondary}][version { 3 | 4 }]`

`no sntp unicast-server <ipaddress|ipv6address|host-name>`

Mode SNTP Configuration

`ipaddress` - Version 4 IP address

`ipv6address` - Version 6 IP address

`host-name` - dns host name

`primary/secondary` - Primary/Secondary NTP servers

`port` - Port identifier

`version` - version 3/ version 4

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-sntp)# sntp server ipv4 12.0.0.100
-------------------------------------------------------------------------------
```

Related Command

`show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

show sntp client

This command displays the SNTP status.

Syntax `show sntp client`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show sntp client
sntp client is enabled
current sntp client version is v4
current sntp client addressing mode is unicast
sntp client port is 123
sntp client clock format is 24 hours
sntp client authentication key id is 5
```

```
sntp client authentication algorithm is md5
sntp client auth Key is Delta
sntp client time zone is + 05:30
sntp client dst start time is not set
sntp client dst end time is not set
-------------------------------------------------------------------------
```

Related Command

`sntp status unicast-mode status` - Display the SNTP Unicast Mode status.

show sntp unicast-mode status

This command displays the SNTP Unicast Mode status.

Syntax `show sntp unicast-mode status`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------
(JGSM7224)# show sntp unicast-mode status
auto discovery of sntp/ntp servers is disabled
unicast poll interval value is 50
unicast max poll time out value is 25
unicast max retry time value is 10
unicast primary server address is 12.0.0.100
unicast primary server version is 3
unicast primary server port is 1234
-------------------------------------------------------------------------
```

Related Commands

`set sntp server auto-discovery` - Configures the SNTP client status of auto-discovery of server

`sntp unicast client poll-interval` - Configures the SNTP client poll interval

`sntp unicast client poll-timeout` - Configures the SNTP client maximum poll interval timeout

`sntp unicast client poll-retry` - Configures the SNTP client maximum retry poll count

show sntp clock

This command displays the current time.

Syntax `show sntp clock`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show sntp clock
-------------------------------------------------------------------------------
```

Related Command

`show clock` - Displays the system date and time.

debug sntp

This command enables SNTP trace. The `no` form of the command disables the SNTP trace.

Default Disabled

Syntax `debug sntp { all | [all-fail] [buff] [control] [data-path] [init-shut] [mgmt] [pkt-dump] [resource]}`
`no debug sntp { all | [all-fail] [buff] [control] [data-path] [init-shut] [mgmt] [pkt-dump] [resource]}`

Mode Privileged EXEC

`init/shut` - Initialization/Shutdown messages

`mgmt` - Management Messages

`data-path` - Data Path Messages

`control` - Control Messages

`pkt-dump` - Packet Dump Messages

`all-fail` - All failure Messages

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug sntp all
-------------------------------------------------------------------------------
```

LLDP 10

LLDP (Link Layer Discovery Protocol) is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network. Information gathered with LLDP is stored in the device and can be queried using Simple Network Management Protocol. The topology of a LLDP-enabled network can be discovered by crawling the hosts and querying this database. The information available includes:

- System name and description
- Port name and description
- VLAN name
- Port and protocol VLAN
- Port VLAN
- IP management address
- System capabilities (switching, routing, and so on)
- MAC/PHY information
- Link aggregation
- Maximum frame size

shutdown lldp

This command starts lldp capability. The `no` form of the command stops the lldp capability. When shutdown, all resources acquired by the lldp module are released to the system.

Default	no shutdown
Syntax	`shutdown lldp` `no shutdown lldp`
Mode	Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# shutdown lldp
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`set lldp` - Enables or disables lldp on the system.

`show lldp` - Displays LLDP global configuration details.

set lldp

This command enables or disables lldp on the system.

Default	Enabled
Syntax	`set lldp {enable | disable}`
Mode	Global Configuration

`enable` - Enable lldp on the system.

`disable` - Disable lldp on the system.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# set lldp enable
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp` - Displays LLDP global configuration details.

lldp timers interval

This command sets the transmission interval at which LLDPDUs are transmitted. The `no` form of the command sets it to the default value.

Default	30
Syntax	`lldp timers interval <seonds(5-32768)>` `no lldp timers interval`
Mode	Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# lldp timers interval 50
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp` - Displays LLDP global configuration details.

lldp timers hold

This command sets the multiplier value used to calculate the Time-To-Live for the LLDP advertisements. The `no` form of this command sets it to the default value.

Default 4

Syntax
```
lldp timers hold <value(2-10)>
no lldp timers hold
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# lldp timers hold 5
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp` - Displays LLDP global configuration details.

lldp timers reinit

This command sets the re-initialization delay time taken by LLDP to re-initialize on any interface. The `no` form of this command sets it to the default value.

Default 2

Syntax
```
lldp timers reinit <integer(1-10)>
no lldp timers reinit
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# lldp timers reinit 5
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp` - Displays LLDP global configuration details.

lldp timers tx-delay

This command sets the transmit delay-minimum amount of delay between successive LLDP frame transmissions. The no form of this command sets it to the default value.

Default 2

Syntax
```
lldp timers tx-delay <seconds(1-8192)>
no lldp timers tx-delay
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# lldp timers tx-delay 5
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp` - Displays LLDP global configuration details.

lldp notification-interval

This command sets the notification interval at which LLDP notifications are sent to NMS. The no form of this command sets it to the default value.

Default 5

Syntax
```
lldp notification-interval <integer(5-3600)>
no lldp notification-interval
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# lldp notification-interval 10
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp` - Displays LLDP global configuration details.

lldp chassis-id-subtype

This command configures the lldp chassis id subtype and the chassis id value.

Default	MAC address
Syntax	`lldp chassis-id-subtype {chassis-comp <string(255)> | if-alias | port-comp <string(255)> | mac-addr | nw-addr | if-name | local <string(255)> }`
Mode	Global Configuration

`chassis-comp` - Chassis component.

`if-alias` - Interface alias.

`port-comp` - Port component.

`mac-addr` - MAC address.

`nw-addr` - Network address.

`if-name` - Interface name.

`local` - Locally assigned.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# lldp chassis-id-subtype if-alias
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp` - Displays LLDP global configuration details.

clear lldp counters

This command clears the LLDP transmit and receive statistics.

Default	Disabled
Syntax	`clear lldp counters`
Mode	Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# clear lldp counters
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp traffic` - Displays LLDP counters, including the number of frames sent, received, discarded, and so on.

clear lldp table

This command clears LLDP neighbors information.

Default Disabled

Syntax `clear lldp table`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# clear lldp table
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp remote-device` - Displays information about neighbors on an interface or all interfaces.

debug lldp

This command enables debugging of the lldp module. The `no` form of the command disables debugging of the ldp module.

Default Disabled

Syntax

```
debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump]
[resource] [all-fail] [buf] [neigh-add] [neigh-del] [neigh-updt]
[neigh-drop] [neigh-ageout] [critical][tlv {all | [chassis-id]
[port-id] [ttl] [port-descr] [sys-name] [sys-descr] [sys-capab]
[mgmt-addr] [port-vlan] [ppvlan] [vlan-name] [proto-id] [mac-phy]
[pwr-mdi] [lagg] [max-frame]}] [redundancy]}]
no debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl]
[pkt-dump] [resource] [all-fail] [buf] [neigh-add] [neigh-del]
[neigh-updt] [neigh-drop] [neigh-ageout] [critical][tlv {all |
[chassis-id][port-id] [ttl] [port-descr] [sys-name] [sys-descr]
[sys-capab] [mgmt-addr] [port-vlan] [ppvlan] [vlan-name] [proto-id]
[mac-phy] [pwr-mdi] [lagg] [max-frame]}] [redundancy]}]
```

Mode Privileged EXEC

`all` - All lldp debug message.

`init-shut` - Init and Shutdown debug messages.

`mgmt` - Management messages.

`data-path` - Data path messages.

`ctrl` - Control plane messages.

`pkt-dump` - Packet dump messages.

`resource` - System Resources management messages.

`all-fail` - Error code debug messages.

`buf` - Buffer related messages.

`neigh-add` - Neighbor add messages.

`neigh-del` - Neighbor delete messages.

`neigh-updt` - Neighbor update messages.

`neigh-drop` - Neighbor drop messages.

`neigh-ageout` - Neighbor age out messages.

`critical` - Critical messages.

`tlv` - tlv related debug messages.

`all` - All tlv messages.

`chassis-id` - Chassis id messages.

`port-id` - Port id messages.

`ttl` - Time to live messages.

`port-descr` - Port description messages.

`sys-name` - System name messages.

`sys-descr` - System description messages.

`sys-capab` - System capability messages.

`mgmt-addr` - Management address messages.

`port-vlan` - Port vlan messages.

`ppvlan` - Ppvlan messages.

`vlan-name` - Vlan name messages.

`proto-id` - Protocol id messages.

`mac-phy` - Mac phy messages.

`pwr-mdi` - Power MDI messages.

`lagg` - LAGG messages.

`max-frame` - Max Frame messages.

`redundancy` - LLDP Redundancy messages.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# debug lldp all
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp` - Displays LLDP global configuration details.

show lldp

This command displays LLDP global configuration details.

Default	Disabled
Syntax	`show lldp`
Mode	Privileged EXEC

Example

```
--------------------------------------------------------------------------
(JGSM7224)# show lldp

LLDP is disabled
Transmit Interval       : 30
Holdtime Multiplier     : 4
Reinitialization Delay  : 2
Tx Delay                : 2
Notification Interval   : 5
Chassis Id SubType      : Mac Address
Chassis Id              : 00:01:02:03:04:05
(JGSM7224)#
--------------------------------------------------------------------------
```

Related Commands

`set lldp` - Enable or disable lldp on the system.

`lldp timers interval` - Sets the transmission interval at which LLDPDUs are transmitted.

`lldp timers hold` - Sets the multiplier value which is used to calculate the Time-To-Live for the LLDP advertisements.

`lldp timers reinit` - Sets the re-initialization delay time taken by LLDP to re-initialize on any interface.

`lldp timers tx-delay` - Sets the transmit delay-minimum amount of delay between successive LLDP frame transmissions.

`lldp notification-interval` - Sets the notification interval at which LLDP notifications are sent to NMS.

`lldp chassis-id-subtype` - Configures lldp chassis id subtype and chassis id value.

show lldp interface

This command displays LLDP configuration details on a particular interface or all interfaces.

Default	Disabled
Syntax	`show lldp interface [<slot>/<port>]`
Mode	Privileged EXEC

`slot/port` - Interface information.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show lldp interface 0/1
0/1:
Tx State             : Enabled
Rx State             : Enabled
Notification Status  : Disabled
Notification Type    : Mis-configuration
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`lldp` - Enables LLDP packets to be transmitted or received on an interface.

`lldp notification` - Enables LLDP trap notification on an interface.

show lldp remote-device

This command displays information about remote devices learned on an interface or all interfaces.

Syntax `show lldp remote-device [chassis-id <string(255)> port-id <string(255)>] [<slot/port>][detail]`

Mode Privileged EXEC

`chassis-id` - Show lldp neighbors by chassis id.

`port-id` - Show lldp neighbors by port id.

`slot/port` - Interface information.

`detail` - show lldp neighbors' detail information.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show lldp remote-device
Capability Codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis  ID          Local  Intf     Hold-time Capability   Port  Id
----------           ----------     --------------------   -------
00:01:02:03:04:05    0/1            120       B,R          Slot0/19

Total  Entries  Displayed  : 1
JGSM7224  #
--------------------------------------------------------------------------------
(JGSM7224)# show  lldp  remote-device  detail

Capability  Codes:
(R)  Router,  (B)  Bridge,  (T)  Telephone,  (C)  DOCSIS  Cable  Device,
(W)  WLAN  Access  Point,  (P)  Repeater,  (S)  Station,  (O)  Other

Chassis Id SubType      : Mac Address
Chassis Id              :00:01:02:03:04:05
Port Id SubType         : Interface Alias
Port Id                 : Slot0/19
Port Description        : Ethernet Interface
System Name             : linux_ipv6
System Desc             : Linux_ipv6-24 ports with 4
combo,Hardware Version(5.2.4),Firmware Version(5.1.0)
Local Intf              : 0/1
Time Remaining          : 105 Seconds
System Capabilities Supported   : Bridge ; Router ;
System Capabilities Enabled     : Bridge ; Router ;
```

```
Management Addresses            :

IfId  SubType  Address        OID
----  -------  -------        ---
33    IPv4     10.0.0.1        1 3 6 1 2 1 2 2 1 1

Extended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto-Neg Support & Status     : Supported, Enabled
Advertised Capability Bits    : 6c11
10base-T(HD)
10base-T(FD)
100base-TX(HD)
100base-TX(FD)
Asym and Symm PAUSE(FD)
1000base-T(FD)
Operational MAU Type          : 30
-Link Aggregation
Capability & Status           : Not Capable, Not In Aggregation
Aggregated Port Id            : 19
-Maximum Frame Size           : 1500

Extended 802.1 TLV Info
-Port VLAN Id  : 1
-Port & Protocol VLAN Id
Protocol Vlan Id       Support      Status
---------------        -------      ------
0                      Supported    Enabled
-Vlan Name
Vlan Name Tlv             : Not Advertised
-------------------------------------------------------------

Total Entries Displayed : 1
(JGSM7224)#
-----------------------------------------------------------------------
```

Related Commands

`set lldp` - Enable or disable lldp on the system.

`clear lldp table` - Clears LLDP neighbors information.

show lldp traffic

This command displays LLDP counters, including the number of frames sent, received, discarded, and so on.

Default Disabled

Syntax `show lldp traffic [<slot/port>]`

Mode Privileged EXEC

`slot/port` - Interface information.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show lldp traffic
Total Frames Out                : 33
Total Entries Aged              : 1
Total Frames In                 : 26
Total Frames Received In Error  : 0
Total Frames Discarded          : 0
Total TLVS Unrecognized         : 0
Total TLVs Discarded            : 0
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`clear lldp counters` - Clears LLDP transmit and receive statistics.

show lldp local-device

This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.

Default Disabled

Syntax `show lldp local-device [<slot/port> | [mgmt-addr]`

Mode Privileged EXEC

`slot/port` - Interface information.

`mgmt-addr` - Management address.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show lldp local-device 0/1
Port Id SubType         : Interface Alias
Port Id                 : Slot0/1
Port Description        : Ethernet Interface
Enabled Tx Tlvs         : Port Description, System Name,
                          System Description, System Capability,
                          Management Address

Extended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto-Neg Support & Status  : Supported, Enabled
Advertised Capability Bits : 6c11
10base-T(HD)
10base-T(FD)
100base-TX(HD)
100base-TX(FD)
Asym and Symm PAUSE(FD)
1000base-T(FD)
Operational MAU Type       : 30

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`lldp transmit-tlv basic-tlv` - Enables the basic TLV transmission on a given port.

`lldp port-id-subtype` - Configures lldp port id subtype and port id value.

`lldp transmit-tlv dot3tlv` - Enables the dot3t TLV transmission on a given port.

lldp

This command enables LLDP packets transmitted or received on an interface. The `no` form of this command disables it.

Default	Enable lldp packets for transmit and receive
Syntax	`lldp {transmit | receive}` `no lldp {transmit | receive}`
Mode	Interface Configuration

`transmit` - transmit LLDP packets

`receive` - receive LLDP packets.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp transmit
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp interface` - Displays LLDP configuration details on a particular interface or all interfaces.

lldp notification

This command enables LLDP trap notification on an interface. The `no` form of this command disables it and specifies the lldp notification type as mis-configuration by default.

Default Disabled LLDP trap notification on an interface

Syntax
```
lldp notification
no lldp notification
```

Mode Interface Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp notification
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp interface` - Displays LLDP configuration details on a particular interface or all interfaces.

lldp notification type

This command specifies the LLDP trap notification type on an interface.

Default mis-configuration

Syntax `lldp notification type [remote-table-chg][mis-configuration]`

Mode Interface Configuration

`remote-table-chg` - Enables lldp trap on remote table change.

`mis-configuration` - Enables lldp trap on mis-configuration.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp notification type remote-table-chg
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp interface` - Displays LLDP configuration details on a particular interface or all interfaces.

lldp transmit-tlv basic-tlv

This command enables the basic TLV transmission on a given port. The `no` form of this command disables it.

Default Enabled

Syntax

```
lldp transmit-tlv basic-tlv {[port-descr] [sys-name] [sys-descr]
[sys-capab] [mgmt-addr]}
no lldp transmit-tlv basic-tlv {[port-descr] [sys-name] [sys-descr]
[sys-capab] [mgmt-addr]}
```

Mode Interface Configuration

`port-descr` - Port description.

`sys-name` - System name.

`sys-descr` - System description.

`sys-capab` - System capability.

`mgmt-addr` - Management address.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp transmit-tlv basic-tlv port-descr sys-name
sys-descr sys-capab mgmt-addr
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp local-device` - Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.

lldp port-id-subtype

This command configures the lldp port id subtype and port id value.

Default Port Id Subtype is Interface Alias

Syntax `lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr | if-name | local <string(255)>}`

Mode Interface Configuration

`if-alias` - Interface alias.

`port-comp` - Port component.

`mac-addr` - MAC address.

`if-name` - Interface name.

`local` - Locally assigned.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp port-id-subtype if-name
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp local-device` - Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.

lldp transmit-tlv dot3tlv

This command enables the dot3t TLV transmission on a given port. The `no` form of this command disables it.

Default Enabled

Syntax `lldp transmit-tlv dot3tlv macphy-config`
`no lldp transmit-tlv dot3TLV macphy-config`

Mode Interface Configuration

`macphy-config` - MAC PHY configuration.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp transmit-tlv dot3tlv macphy-config
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp local-device` - Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.

LLDP-MED

11

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management, and location information.

lldp med

This command enables the lldp med function. The no form of the command disables the lldp med function.

Default	Disabled
Syntax	`lldp med` `no lldp med`
Mode	Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp med
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp med interface` - Displays lldp med interface configuration information.

lldp med confignotification

This command enables the lldp med notification function. The no form of the command disables the lldp med notification.

Default Disabled

Syntax
```
lldp med confignotification
no lldp med confignotification
```

Mode Interface Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp med confignotification
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp med interface` - Displays lldp med interface configuration information.

lldp med transmit-tlv

This command enables LLDP-MED TLV transmission on a given port. The no form of this command disables it.

Default Disabled

Syntax
```
lldp med transmit-tlv {[capabilities] [network-policy]}
no lldp med transmit-tlv {[capabilities] [network-policy]}
```

Mode Interface Configuration

`capabilities` - Enables the LLDP-MED endpoints to determine the capabilities that the connected device supports and what capabilities the device has enabled.

`network-policy` - Enables the LLDP-MED network policy TLV, which contains related information such as voice VLAN.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# lldp med transmit-tlv capabilities
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show lldp med interface` - Displays lldp med interface configuration information.

lldp med faststartrepeatcount

This command configures the value of the fast start repeat count.

Default 3

Syntax
```
lldp med faststartrepeatcount <times(1-10)>
no lldp med faststartrepeatcount
```

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# lldp med faststartrepeatcount 5
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show lldp med` - Displays lldp med global configuration information.

show lldp med

This command displays LLDP med global configuration information.

Syntax `show lldp med`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show lldp med

LLDP is enabled
LLDP MED Global Configuration
Fast Start Repeat Count: 3
Device Class: Network Connectivity
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`ldp med faststartrepeatcount` - Configures the value of the fast start repeat count.

show lldp med interface

This command displays LLDP MED configuration details on a particular interface or all interfaces.

Syntax `show lldp med interface { <slot/port> | all }`

Mode Privileged EXEC

`slot/port` - Interface information.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show lldp med interface 0/3
Interface    Link   configMED  operMED    ConfigNotify  TLVsTx
----------   -----  ---------  ---------  ------------  ---------
0/3          up     Enabled    Enabled    Disabled      0;1;
TLV Codes: 0- Capabilities,              1- Network Policy
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`lldp med` - Enable or disable lldp med on the system.

`lldp med configNotification` - Enable or disable lldp med notification on the system.

`lldp med transmit-tlv` - Enables the lldp med TLV transmission on a given port.

show lldp med local-device

This command displays the current switch information that will be used to populate outbound LLDP MED advertisements for a specific interface.

Syntax `show lldp med local-device detail { <slot/port> }`

Mode Privileged EXEC

`slot/port` - Interface information.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show lldp med local-device detail 0/3

LLDP MED Local Device Detail

Interface: 0/3

Network Policies
```

```
Media Policy Application Type : voice
Vlan ID: 1
Priority: 4
DSCP: 0
Unknown: True
Tagged: False
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`llpd med transmit-tlv` - Enables the lldp med TLV transmission on a given port.

show lldp med remote-device

Syntax `show lldp med remote-device { <slot/port> | all }`

Mode Privileged EXEC

`slot/port` - Interface information.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show lldp med remote-device 0/5

LLDP MED Remote Device Summary

Local Interface  Remote ID Device Class
---------------- --------  ------------
0/5              4         Network Con
(JGSM7224)#
--------------------------------------------------------------------------------
```

show lldp med remote-device detail

Syntax `show lldp med remote-device detail {<slot/port>}`

Mode Privileged EXEC

`slot/port` - Interface information.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show lldp med remote-device detail 0/3

LLDP MED Remote Device Detail
```

```
Local Interface: 0/3
Remote Identifier: 2 Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse,
inventory
MED Capabilities Enabled: capabilities, networkpolicy, location, extendedpse,
Device Class: Network Connectivity

Network Policies

Media Policy Application Type : voice
Vlan ID: 50
Priority: 6
DSCP: 46
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: version abc
Firmware Rev: Not Advertised
Software Rev: Not Advertised
Serial Number: Not Advertised
Manufacture Name: Not Advertised
Model Name: Not Advertised
Asset ID: Not Advertised

Location
Subtype: Civic Address LCI
Info: US CA Roseville Foothills 8000 R3L

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 6.5 Watts
Source: Unknow
Priority: low
(JGSM7224)#
--------------------------------------------------------------------------------
```

12 VLAN

VLANs (Virtual LANs) can be viewed as a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment. In other words, a VLAN is a network of computers that behave as if they are connected to the same wire even though they might be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible.

A VLAN provides the following benefits for switched LANs:

- Improved administration efficiency
- Optimized Broadcast/Multicast Activity
- Enhanced network security

vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Syntax `vlan database`

Mode Privileged Exec

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# vlan database
(JGSM7224)(vlan)#
-------------------------------------------------------------------------------
```

Related Commands

`vlan` - Creates a new VLAN and assigns it an ID.

`vlan name` - Changes the name of a VLAN.

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The no form of the command deletes an existing VLAN.

Syntax `vlan <vlan_list>`
`no vlan <vlan_list>`

Mode VLAN Config

`<vlan_list>` - Contains Vlan Ids in the range 1-4094. Separate non-consecutive IDs with ',' with no spaces and no zeros between the range. Use '-' for a range.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(vlan)# vlan 4,8-10
(JGSM7224)(vlan)#
-------------------------------------------------------------------------------
```

Related Commands

`vlan database` - Enter VLAN Config mode.

`show vlan` - Displays a list of all configured VLANs.

`show vlan <vlan-id>` - Displays detailed information, including interface information for a specific VLAN.

vlan name

This command changes the name of a VLAN. The no form of the command sets the name of a VLAN to a blank string. The default VLAN's name cannot be changed, including vlan1, vlan2 (VoiceVLAN), and vlan3 (AutoVideo).

Default Blank string

Syntax `vlan name <1-4094> <string>`
`no vlan name <1-4094>`

Mode VLAN Config

`<1-4094>` - VLAN identification number, in the range 1-4094.

`<string>` - An alphanumeric string of up to 32 characters.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(vlan)# vlan name 4 vlan4
(JGSM7224)(vlan)#
```

```
--------------------------------------------------------------------------------
```

Related Commands

`vlan database` - Enter VLAN Config mode.

`show vlan` - Displays a list of all configured VLANs.

`show vlan <vlan-id>` - Displays detailed information, including interface information for a specific VLAN.

vlan participation

This command configures the degree of participation for a specific interface in a VLAN.

Default	For VLAN ID1, the default is include untagging. For others, the default is auto.
Syntax	`vlan participation {auto | include | exclude} <vlan_list>`
Mode	Interface Configuration

`auto` - The interface is dynamically added to this VLAN.

`include` - The interface is always a member of this VLAN.

`exclude` - The interface is never a member of this VLAN.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# vlan participation include 1,3
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Commands

`vlan tagging` - Configures the tagging behavior for a specific interface in a VLAN to enabled.

`show vlan <vlan-id>` - Displays detailed information, including interface information for a specific VLAN.

vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. The `no` form of the command configures it to disabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames.

The VLAN list contains VLAN IDs in the range <1-4094>. Separate non-consecutive IDs with a comma, with no spaces or zeros in the range. Use a dash for a range.

Default Disabled

Syntax
```
vlan tagging <vlan_list>
no vlan tagging <vlan_list>
```

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# vlan tagging 1,3
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`vlan participation` - Configures the degree of participation for a specific interface in a VLAN.

`show vlan <vlan-id>` - Displays detailed information, including interface information for a specific VLAN.

vlan pvid

This command changes the VLAN ID per interface. The `no` form of the command sets the VLAN ID per interface to 1.

Default 1

Syntax
```
vlan pvid <1-4094>
no vlan pvid
```

Mode Interface Configuration

`<1-4094>` - VLAN ID in the range 1-4094.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# vlan pvid 3
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show vlan port` - Displays VLAN port information.

vlan acceptframe

This command sets the frame acceptance mode per interface. The no form of the command resets the frame acceptance mode for the interface to the default value.

Default all

Syntax
```
vlan acceptframe {all | vlanonly | admituntaggedonly}
no vlan vlan acceptframe {all | vlanonly | admituntaggedonly}
```

Mode Interface Configuration

`all` - Both untagged frames and tagged frames are accepted. Untagged frames or priority frames received on this interface are assigned the value of the interface VLAN ID for this port. VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

`vlanonly` - Untagged frames or priority frames received on this interface are discarded. VLAN tagged frames are forwarded.

`admituntaggedonly` - Only frames received without VLAN tag will be forwarded. All other frames will be dropped.

Example

```
--------------------------------------------------------------------------
(JGSM7224)(config-if)# vlan acceptframe admituntaggedonly
(JGSM7224)(config-if)#
--------------------------------------------------------------------------
```

Related Command

`show vlan port` - Displays VLAN port information.

vlan ingressfilter

This command enables ingress filtering. The no form of the command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default Disabled.

Syntax
```
vlan ingressfilter
no vlan ingressfilter
```

Mode Interface Configuration

Example

```
--------------------------------------------------------------------------
(JGSM7224)(config-if)# vlan ingressfilter
(JGSM7224)(config-if)#
--------------------------------------------------------------------------
```

Related Command

`show vlan port` - Displays VLAN port information.

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface.

Default 0

Syntax `vlan priority <0-7>`

Mode Interface Configuration

`<0-7>` - The range for the priority.

Example

```
--------------------------------------------------------------------------
(JGSM7224)(config-if)# vlan priority 2
(JGSM7224)(config-if)#
--------------------------------------------------------------------------
```

Related Command

`show vlan port` - Displays VLAN port information.

vlan association mac

This command configures the VLAN-MAC address mapping. The no form of this command is used to delete the specific mac map entry. This command is valid only if the VLAN is configured as MAC-based.

Syntax `vlan association mac <aa:aa:aa:aa:aa:aa> <vlan-id(1-4094)>`
`no vlan association mac <aa:aa:aa:aa:aa:aa>`

Mode VLAN Config

`aa:aa:aa:aa:aa:aa` - MAC address.

`vlan` - VLAN Identifier.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(vlan)# vlan association mac 00:11:22:33:44:55 2
(JGSM7224)(vlan)#
-------------------------------------------------------------------------------
```

Related Command

`show vlan association mac` - Displays the entries in the MAC-VLAN database.

vlan association subnet

This command configures the VLAN-subnet address mapping. The `no` form of this command is used to delete the specific subnet map entry. This command is valid only if the VLAN is configured as subnet-based.

Syntax `vlan association subnet <ipaddr> <netmask> <vlan-id(1-4094)>`
`no vlan association subnet <ipaddr> <netmask>`

Mode VLAN Config

`ipaddr` - IP address.

`netmask` - Net mask.

`vlan` - VLAN Identifier.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(vlan)# vlan association subnet 10.0.0.0 255.0.0.0 2
(JGSM7224)(vlan)#
-------------------------------------------------------------------------------
```

Related Command

`show vlan association subnet` - Displays the entries in the subnet-VLAN database.

debug vlan

This command enables module-wise debug traces, which can be either Forwarding or Priority.

Default Disabled

Syntax

```
debug vlan { global | [{ fwd | priority | | redundancy } [initshut] [mgmt]
[data] [ctpl] [dump] [os] [failall] [buffer] [all]] }
no debug vlan { global | [{fwd | priority | | redundancy } [initshut]
[mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] }
```

Mode Privileged Exec

`global` - Global-related debug messages.

`fwd` - Forwarding Module.

`priority` - VLAN Priority Module.

`redundancy` - Redundancy-related debug messages.

`initshut` - Init and Shutdown.

`mgmt` - Management.

`data` - Data path.

`ctpl` - Control Plane.

`dump` - Packet dump.

`os` - Traces related to all Resources except Buffer.

`failall` - All Failures.

`buffer` - Buffer.

`all` - All Traces.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# debug vlan fwd all
(JGSM7224)#
--------------------------------------------------------------------------------
```

show vlan

This command displays a list of all configured VLANs.

Syntax `show vlan [brief]`

Mode Privileged Exec

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show vlan

VLAN ID    VLAN Name                       VLAN Type
------- -------------------------------- ---------
   1       Default                         Default
   2       VoiceVLAN                       Default
   3       AutoVideo                       Default
   4       vlan4                           Static

(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`vlan` - Creates a new VLAN and assigns it an ID.

`vlan name` - Changes the name of a VLAN.

show vlan <vlan-id>

This command displays detailed information, including interface information, for a specific VLAN.

Syntax `show vlan <vlan-id>`

Mode Privileged Exec

`<vlan-id>` - VLAN ID in the range 1-4094.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show vlan 1

VLAN ID: 1
VLAN Name: Default
VLAN Type: Default
```

```
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
0/1         Include   Include      Tagged
0/2         Include   Include      Untagged
0/3         Exclude   Autodetect   -------
0/4         Include   Include      Untagged
0/5         Include   Include      Untagged
0/6         Include   Include      Untagged
0/7         Include   Include      Untagged
0/8         Include   Include      Untagged
0/9         Include   Include      Untagged
0/10        Include   Include      Untagged
0/11        Include   Include      Untagged
0/12        Include   Include      Untagged
0/13        Include   Include      Untagged
0/14        Include   Include      Untagged
0/15        Include   Include      Untagged
0/16        Include   Include      Untagged
--More-- or (q)uit
--------------------------------------------------------------------------------
```

Related Command

`vlan participation` - Configures the degree of participation for a specific interface in a VLAN.

`vlan tagging` - Configures the tagging behavior for a specific interface in a VLAN to enabled.

show vlan port

This command displays VLAN port information.

Syntax `show vlan port { all | <slot/port> | port-channel <id (1-8)>}`

Mode Privileged Exec

`all` - Show all VLAN port information.

`<slot/port>` - Show VLAN port information for a specified port.

`port-channel` - Show VLAN port information for a specified channel.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show vlan port 0/2
          Port       Port                  Ingress
          VLAN ID    VLAN ID  Acceptable   Filtering  Default    Protected
```

```
Interface Configured Current  Frame Types  Current    Priority   Port
--------- ---------- -------- ----------- ---------   --------   ---------
0/2       1          1        untaggedonly  Enable    2          Disable

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`vlan pvid` - Changes the VLAN ID per interface.

`vlan acceptframe` - Sets the frame acceptance mode per interface.

`vlan ingressfilter` - Enables ingress filtering per interface.

`vlan priority` - Configures the default 802.1p port priority assigned for untagged packets for a specific interface.

show vlan association mac

This command displays the entries in the MAC-VLAN database.

Syntax `show vlan association mac`

Mode Privileged Exec

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show vlan association mac
-----------------------------------
Mac Address         Config Vlan ID  Current Vlan ID
----------          --------------  ---------------
00:00:01:01:01:01    1               1
00:00:01:01:01:02    1               1
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`vlan association mac` - Configures the VLAN-MAC address mapping status variables.

show vlan association subnet

This command displays the entries in the subnet-VLAN database.

Syntax `show vlan association subnet`

Mode Privileged Exec

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show vlan association subnet
-----------------------------------------
Subnet Address    Subnet Mask    Vlan ID
-----------------------------------------
10.0.0.1           255.0.0.0       1
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`vlan association subnet` - Configures the VLAN-subnet address mapping.

mac-address-table static unicast

This command configures a static unicast MAC address in the forwarding database. The `no` form of the command deletes a configured static Unicast MAC address from the forwarding database. The VLAN must have been configured, and member ports must have been configured for the specified VLAN.

Default Status = permanent

Syntax

```
mac-address-table static unicast <aa:aa:aa:aa:aa:aa>
vlan <vlan-id(1-4094)> interface {port-channel <integer (1-8)> |
<slot/port>} [status { permanent | deleteOnReset | deleteOnTimeout }]
no mac-address-table static unicast <aa:aa:aa:aa:aa:aa>
vlan <vlan-id(1-4094)>
```

Mode Global Configuration

`aa:aa:aa:aa:aa:aa` - Destination MAC address.

`vlan` - VLAN Identifier.

`interface` - Member port type and ID.

`<slot/port>` - Port ID. Interface can be gigabitethernet type.

`port-channel` - Port channel ID.

`status` - Status of the Static unicast entry.

Related Command

`show mac-address-table static unicast` - Displays the statically configured unicast address from the MAC address table.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# mac-address-table static unicast
00:11:22:33:44:55 vlan 3 interface 0/1 status deleteOnTimeout
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

mac-address-table static multicast

This command configures a static mulitcast MAC address in the forwarding database. The VLAN must have been configured, and member ports must have been configured for the specified VLAN.

Default Status = permanent.

Syntax

```
mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan
<vlan-id(1-4094)> interface ([<0/ab, 0/c, ...>] [port-channel <a,b,c-d>])
[status { permanent|deleteOnReset|deleteOnTimeout }]
no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan
<vlan-id(1-4094)>
```

Mode Global Configuration

`aa:aa:aa:aa:aa:aa` - Multicast MAC address.

`vlan` - VLAN Identifier.

`interface` - Member Ports Interface type and ID. Interface can be gigabitethernet type.

`<0/a-b, 0/c, ...>` - Member Ports Interface type and ID. Interface can be gigabitethernet type.

`port-channel` - Port channel ID.

`status` - Status of the static multicast entry.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# mac-address-table static multicast
01:02:03:04:05:06 vlan 2 interface 0/1
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show mac-address-table static multicast` - Displays the statically configured multicast entries.

mac-address-table aging-time

This command sets the maximum age of a dynamically learned entry in the MAC address table. The no form of the command sets the maximum age of an entry in the MAC address table to its default value. If traffic on an interface is not very frequent, the aging time must be increased to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding.

Default 300

Syntax
```
mac-address-table aging-time <10-1000000 seconds>
no mac-address-table aging-time
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# mac-address-table aging-time 200
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show mac-address-table aging-time` - Displays the MAC address-table with aging time.

show mac-address-table

This command displays the static and dynamic unicast and multicast MAC address table. If executed without the optional parameters, this command displays all the static and dynamic MAC entries.

Syntax
```
show mac-address-table [vlan <vlan-range>] [address<aa:aa:aa:aa:aa:aa>]
[{interface port-channel <integer(1-8)|<slot|port>}]
```

Mode Privileged Exec Mode

`vlan` - VLAN ID.

`address` - MAC address.

`interface` - Interface type and ID.

`<slot/port>` - Port ID.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show mac-address-table vlan 2
Vlan  Mac Address        Type    Ports
----  -----------        ----    -----
2     00:01:02:03:04:21  Learnt    0/1
Total Mac Addresses displayed: 1
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`mac-address-table static unicast` - Configures a static unicast MAC address in the forwarding database.

`mac-address-table static multicast` - Configures a static mulitcast MAC address in the forwarding database.

show mac-address-table count

This command displays the number of MAC addresses present on all the VLANs or on the specified VLAN. If executed without the optional parameter this command displays the MAC addresses present on all the VLANs.

Syntax `show mac-address-table count [vlan <vlan-id(1-4094)>]`

Mode Privileged Exec

`vlan` - VLAN ID.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show mac-address-table count
Mac Entries for Vlan 1:
-------------------------
Dynamic Unicast Address Count : 1
Dynamic Multicast Address Count :0
Static Unicast Address Count : 1
Static Multicast Address Count :1
---------------------------------------
Mac Entries for Vlan 2:
-------------------------
Dynamic Unicast Address Count : 1
Dynamic Multicast Address Count :0
Static Unicast Address Count : 1
Static Multicast Address Count :0
---------------------------------------
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`mac-address-table static unicast` - Configures a static unicast MAC address in the forwarding database.

`mac-address-table static multicast` - Configures a static mulitcast MAC address in the forwarding database.

show mac-address-table static unicast

This command displays the statically configured unicast addresses from the MAC address table. If executed without the optional parameters, this command displays the MAC address table for all available interfaces.

Syntax `show mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{ interface port-channel <integer(1-8)>|<slot/port> }]`

Mode Privileged Exec

`vlan` - VLAN ID.

`address` - MAC address.

`interface` - Interface type and ID.

`<slot/port>` - Port ID.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show mac-address-table static unicast
Vlan  Mac Address        Status          Ports
----  -----------        --------        -----
2     00:11:22:33:44:55  Del-OnTimeout   0/3
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`mac-address-table static unicast` - Configures a static unicast MAC address in the forwarding database.

`show mac-address-table dynamic unicast` - Displays the dynamic MAC address table for the specified address or for all the addresses.

show mac-address-table static multicast

This command displays the statically configured multicast entries. If executed without the optional parameters, this command displays the MAC address table for all available interfaces.

Syntax `show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{ interface port-channel <integer(1-8)>|<slot/port> }]`

Mode Privileged Exec

`vlan` - VLAN ID.

`address` - MAC address.

`interface` - Interface type and ID.

`<slot/port>` - Port ID.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show mac-address-table static multicast
Static Multicast Table
----------------------
Vlan : 1
Mac Address : 01:02:03:04:05:06
Member Ports : 0/1
Status : Permanent
-----------------------------------------------
Total Mac Addresses displayed: 1
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`mac-address-table static multicast` - Configures a static mulitcast MAC address in the forwarding database.

show mac-address-table dynamic unicast

This command displays the dynamically learned unicast entries from the MAC address table. If executed without the optional parameters, this command displays the MAC address table of all available interfaces.

Syntax `show mac-address-table dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{ interface port-channel <integer(1-8)>|<slot/port>}]`

Mode Privileged Exec

`vlan` - VLAN ID.

`address` - MAC address.

`interface` - Interface type and ID.

`<slot/port>` - Port ID.

Related Commands

`mac-address-table static unicast` - Configures a static unicast MAC address in the forwarding database.

`show mac-address-table static unicast` - Displays the statically configured unicast address from the MAC address table.

Example

```
--------------------------------------------------------------------------------
(JGSM7224) # show mac-address-table dynamic unicast vlan 2
Vlan Mac Address     Type     Ports
---------------     ----     -----
2 00:01:02:03:04:21  Learnt   0/1
Total Mac Addresses displayed: 1
(JGSM7224) #
--------------------------------------------------------------------------------
```

show mac-address-table dynamic multicast

This command displays the dynamically learned unicast entries from the MAC address table. If executed without the optional parameters, this command displays the MAC address table for all available interfaces.

Syntax `show mac-address-table dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{ interface port-channel <integer(1-8)>|<slot/port> }]`

Mode Privileged Exec

`vlan` - VLAN ID.

`address` - MAC address.

`interface` - Interface type and ID.

`<slot/port>` - Port ID.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show mac-address-table dynamic unicast vlan 2
Vlan Mac Address     Type     Ports
---------------     ----     -----
2 00:01:02:03:04:21  Learnt   0/1
Total Mac Addresses displayed: 1
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`mac-address-table static unicast` - Configures a static unicast MAC address in the forwarding database.

`show mac-address-table static unicast` - Displays the statically configured unicast address from the MAC address table.

show mac-address-table aging-time

This command displays the MAC address-table aging time.

Syntax `show mac-address-table aging time`

Mode Privileged Exec

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show mac-address-table aging-time
Mac Address Aging Time: 300
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`show mac-address-table` - Displays the static and dynamic MAC entries.

`mac-address-table aging-time` - Configures the MAC address table entry maximum age.

clear mac-addr-table

This command clears the dynamically learned MAC addresses of the switch.

Syntax `clear mac-addr-table {all|interface{<slot/port> | port-channel<integer(1-8)>} | vlan<vlan-id(1-4094)>}`

Mode Privileged Exec

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# clear mac-addr-table all
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`vlan` - VLAN Identifier.

`interface` - Interface ID of the MAC address to clear.

Double VLAN

13

Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost-effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own 802.1Q domain.

dvlan-tunnel enable

This command enables double vlan function globally. The `no` form of the command disables double vlan function.

Default	Disabled
Syntax	`dvlan-tunnel enable` `no dvlan-tunnel enable`
Mode	Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# dvlan-tunnel enable
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show dvlan-tunnel` - Displays global double vlan status and ether-type value.

dvlan-tunnel ethertype

This command configures the ether-type for all interfaces. The no form of the command resets the ether-type value to 802.1Q.

Default	802.1Q
Syntax	`dvlan-tunnel ethertype { 802.1Q | vman | custom <1-65535> }` `no dvlan-tunnel ethertype`
Mode	Global Configuration

`802.1Q` - Set ether-type value to 0x8100.

`vman` - Set ether-type value to 0x88a8.

`custom` - Set ether-type value to others from 1 to 65535.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# dvlan-tunnel ethertype custom 0x9100
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`dvlan-tunnel enable` - Enables double VLAN function globally.

`show dvlan-tunnel` - Displays global double VLAN status and ether-type value.

mode dvlan-tunnel

This command enables Double VLAN Tunneling on the specified interface. The no form of the command disables Double VLAN Tunneling on the specified interface.

Default	Disabled
Syntax	`mode dvlan-tunnel` `no mode dvlan-tunnel`
Mode	Interface Configuration

Note: When you use the `mode dvlan-tunnel` command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# mode dvlan-tunnel
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`dvlan-tunnel enable` - Enables double VLAN function globally.

`show dvlan-tunnel interface` - Displays detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

show dvlan-tunnel

This command displays global double VLAN status and ether-type value.

Syntax	`show dvlan-tunnel`
Mode	Privileged Exec

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show dvlan-tunnel

Global Status : Disabled
Ether Type : 0x8100

(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`dvlan-tunnel enable` - Enables double VLAN function globally.

`dvlan-tunnel ethertype` - Configures the ether-type for all interfaces.

show dvlan-tunnel interface

This command displays detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Syntax	`show dvlan-tunnel interface {all | <slot/port> | port-channel <id (1-8)>}`
Mode	Privileged Exec

`all` - Displays information for all interfaces.

`<slot/port>` - Displays information for a specified port.

`port-channel` - Displays information for a specified port channel.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show dvlan-tunnel interface 0/2

Interface   Mode
---------   ---------
0/2         Disabled
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`mode dvlan-tunnel` - Enable Double VLAN Tunneling on the specified interface.

debug dvlan-tunnel

This command configures double VLAN debug flags.

Syntax `debug dvlan-tunnel { all | management | failure}`
`no debug dvlan-tunnel { all | management | failure}`

Mode Privileged Exec

`all`- Turn on all debug trace.

`management` - Turn on management debug trace.

`failure` - Turn on failure debug trace.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug dvlan-tunnel all
DVLAN: Trace Option is set with value: 0x42
(JGSM7224)#
-------------------------------------------------------------------------------
```

Port Security

14

Port security limits the dynamic and static MAC addresses of each port.

port security

This command enables port locking.

Default	Disabled
Syntax	`port security` `no port security`
Modes	Global Configuration Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# port security
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show port-security` - Displays the port-security settings.

port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Default	600
Syntax	`port-security max-dynamic <0-600>` `no port-security max-dynamic`
Mode	Interface Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# port-security max-dynamic 400
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show port-security` - Displays the port-security settings.

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a specific port.

Default 20

Syntax
```
port-security max-static <0-20>
no port-security max-static
```

Mode Interface Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# port-security max-static 10
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show port-security` - Displays the port-security settings.

snmp-server enable traps violation

This command enables sending new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

Default Disabled

Syntax
```
snmp-server enable traps violation
no snmp-server enable traps violation
```

Mode Interface Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# snmp-server enable traps violation
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Command

`show port-security` - Displays the port-security settings.

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked address.

Syntax	`port-security mac-address move`
Mode	Interface Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# port-security mac-address move
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

show port-security

This command displays the port-security settings. If no parameter is input, the default displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

Syntax	`show port-security { all | interface <slot/port> | port-channel <integer(1-8)> }`
Mode	Privileged Exec

`all` - All interfaces

`slot/port` - Interface ID

`port-channel` - Port channel ID

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show port-security
Port Security Administration Mode Enabled
-----------------------------------------------------------------------------
```

Related Commands

`port security` - Enables port locking.

`port-security max-dynamic` - Sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

`port-security max-static` - Sets the maximum number of statically locked MAC addresses allowed on a specific port.

`snmp-server enable traps violation` - Enables sending new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

Syntax `show port-security dynamic interface { <slot/port> | port-channel <integer(1-8)> }`

Mode Privileged Exec

`slot/port` - Interface ID

`port-channel` - Port channel ID

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show port-security dynamic interface 0/1
Number of Dynamic MAC addresses learned: 5
Dynamically learned MAC Address    VLAN ID
-----------------------------      -------
00:0D:88:F7:86:DE                  1
00:0F:06:84:7C:01                  1
00:13:20:5C:18:91                  1
00:13:25:20:13:14                  1
00:14:78:23:A9:09                  1
-------------------------------------------------------------------------------
```

Related Commands

`port security` - Enables port locking.

`port-security max-dynamic` - Sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Syntax `show port-security violation interface { <slot/port> | port-channel <integer(1-8)>`

Mode Privileged Exec

`slot/port` - Interface ID

`port-channel` - Port channel ID

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show port-security violation interface 0/1
Last Violation MAC Address     VLAN ID
00:0D:88:F7:86:AC                  1
-------------------------------------------------------------------------------
```

Related Commands

`port security` - Enables port locking.

`port-security max-dynamic` - Sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

`port-security max-static` - Sets the maximum number of statically locked MAC addresses allowed on a specific port.

15 Private Group

Private group is used to create a group of ports that can or cannot share traffic with each other in the same VLAN group. The main application is to isolate one group of users from another without using VLAN. Note the following:

- There are two mode groups: isolated and community.
- When the mode is isolated, the member port in the group cannot forward its egress traffic to any other members in the same group.
- By default, the mode is community. Each member port can forward traffic to other members in the same group, but not to members in other groups.

The ingress traffic from a port in a private group can be forwarded to anyone in the same VLAN that is not in a private group. The ingress traffic from a port in a private group cannot be forwarded to anyone in the same VLAN that is in a different private group.

private-group name

This command is used to create a private group with group name.

Syntax

```
private-group name <privategroup-name> [privategroup-id(1-24)]
[ mode { community | isolated }]
no private-group name <privategroup-name>
```

Mode Global Configuration

`privategroup-name` - Private group name.

`privategroup-id` - Private group ID.

`community | isolated` - Private group mode.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# private-group name JGSM7224
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show private-group` - Displays the private group's information.

switchport private-group

This command is used to assign one port or a range of ports to a private group.

Syntax

```
switchport private-group { name <privategroup-name> | id
<privategroup-id(1-24)> }
no switchport private-group { name <privategroup-name> | id
<privategroup-id(1-24)> }
```

Mode Interface Configuration

`privategroup-name` - Private group name.

`privategroup-id` - Private group ID.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# switchport private-group name JGSM7224
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show private-group` - Displays a private groups's information

show private-group

This command displays a private group's information.

Syntax

```
show private-group { name <privategroup-name> | id
<privategroup-id(1-24)> | interface <slot/port> }
```

Mode Privileged Exec

`privategroup-name` - Private group name.

`privategroup-id` - Private group ID.

`slot/port` - Interface ID.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show private-group name JGSM7224

          Port    Private Private          Private-Group
Interface VLANID  GroupID GroupName        Mode
--------- ------- ------- ------------------------ -------------
0/20      1       1       JGSM7224         community

--------------------------------------------------------------------------------
```

Related Commands

`private-group name` - Create a private group with group name.

`switchport private-group` - Assign one port or a range of ports to a private group.

Static MAC Filtering 16

Static MAC filtering is used to limit the source port of the destination MAC address. The limits are as follows:

- For unicast MAC address filters and multicast MAC address filters with source portlists, the maximum number of static MAC filter addresses supported is 20.
- For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 32.
- The restricted MAC addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:2F, and FF:FF:FF:FF:FF:FF.

macfilter

This command adds a static MAC filter entry for the MAC address on the VLAN

Syntax

```
macfilter <aa:aa:aa:aa:aa:aa> <vlan-id(1-4094)>
no macfilter <aa:aa:aa:aa:aa:aa> <vlan-id(1-4094)>
```

Mode Global Configuration

`(aa:aa:aa:aa:aa:aa)` - Filter MAC address.

`vlan-id` - VLAN ID.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# macfilter 00:01:00:00:00:08 1
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Command

`show mac-address-table staticfiltering` - Displays the static MAC filtering information for all static MAC Filters.

macfilter addsrc

This command adds the interface to the destination filter set for the MAC filter with the given MAC and VLAN ID.

Syntax

```
macfilter addsrc <aa:aa:aa:aa:aa:aa> <vlan-id(1-4094)>
no macfilter addsrc <aa:aa:aa:aa:aa:aa> <vlan-id(1-4094)>
```

Mode Interface Configuration

`(aa:aa:aa:aa:aa:aa)` - Filter MAC address.

`vlan-id` - VLAN ID.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# macfilter addsrc 00:01:00:00:00:08 1
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show mac-address-table staticfiltering` - Displays the static MAC filtering information for all static MAC filters.

macfilter addsrc all

This command adds all interfaces to the destination filter set for the MAC filter with the given MAC and VLAN ID.

Syntax

```
macfilter addsrc all <aa:aa:aa:aa:aa:aa> <vlan-id(1-4094)>
no macfilter addsrc all <aa:aa:aa:aa:aa:aa> <vlan-id(1-4094)>
```

Mode Global Configuration

`(aa:aa:aa:aa:aa:aa)` - Filter MAC address.

`vlan-id` - VLAN ID.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# macfilter addsrc all 00:01:00:00:00:08 1
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show mac-address-table staticfiltering` - Displays the static MAC filtering information for all static MAC filters.

show mac-address-table staticfiltering

This command displays the static MAC filtering information for all static MAC filters.

Syntax `show mac-address-table staticfiltering { <aa:aa:aa:aa:aa:aa> <vlan-id(1-4094)> | all }`

Mode Privileged Exec

`(aa:aa:aa:aa:aa:aa)` - Filter MAC address.

`vlan-id` - VLAN ID.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)#show mac-address-table staticfiltering all

Static Mac Filter Table
-----------------------
VLAN ID             : 1
MAC Address         : 00:01:00:00:00:01
Source Port(s)      : 0/3
Destination Port(s) :
-------------------------------------------
VLAN ID             : 1
MAC Address         : 00:01:00:00:00:08
Source Port(s)      : 0/20
Destination Port(s) :
-------------------------------------------
VLAN ID             : 1
MAC Address         : 01:01:00:00:00:09
Source Port(s)      : 0/21
Destination Port(s) : 0/22
-------------------------------------------------------------------------------
```

Related Commands

`macfilter` - Adds a static MAC filter entry for the MAC address on the VLAN.

`macfilter addsrc` - Adds the interface to the destination filter set for the MAC filter with the given MAC and VLAN ID.

`macfilter addsrc all` - Adds all interfaces to the destination filter set for the MAC filter with the given mac and VLAN ID.

Voice VLAN 17

Voice VLAN is a specific VLAN used for voice traffic. You can add the port statically or dynamically to the voice VLAN and configure the quality of service for this VLAN to ensure the priority and the quality of the IP phone. When you need to dynamically add to a voice VLAN, use the Organizationally Unique Identifier to identify the voice device.

voice vlan enable

This command enables voice VLAN function globally. The no form of the command disables the voice vlan function.

Default Disabled

Syntax
```
voice vlan <vlan(2-4094)> enable
no voice vlan
```

Mode Global Configuration

`vlan` - VLAN identifier.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# voice vlan 10 enable
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show voice vlan globals` - Displays global voice VLAN status.

voice vlan cos

This command sets the cos for voice VLAN function globally. The no form of the command resets the cos to default.

Default 6

Syntax
```
voice vlan cos <cos(0-7)>
no voice vlan cos
```

Mode Global Configuration

`cos` - cos value.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# voice vlan cos 3
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show voice vlan globals` - Displays global voice VLAN status.

voice vlan aging

This command sets the aging time for voice VLAN function globally. The no form of the command resets the aging time to the default.

Default 1 day

Syntax
```
voice vlan aging <days (0-30)> [<hours (0-23)> [<minutes(1-59)>]]
no voice vlan aging
```

Mode Global Configuration

`days` - Number of days.

`hours` - Number of hours.

`minutes` - Number of minutes.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# voice vlan aging 1 1 1
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show voice vlan globals` - Displays global voice VLAN status.

voice vlan oui

This command adds an oui for the voice VLAN function. The no form of the command deletes the oui.

Default	None
Syntax	`voice vlan oui <oui(32)> <description(30)>` `no voicevlan oui <oui(32)>`
Mode	Global Configuration

`oui` - Oui address format, such as 00:03:6b.

`description` - Description of the oui (30 character maximum).

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# voice vlan oui 00:03:6b cisco
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show voice vlan oui` - Displays ouis of voice VLAN.

voice vlan mode

This command sets voice VLAN function port mode.

Default	Auto
Syntax	`voice vlan mode { manual | auto }`
Mode	Interface Configuration

`manual` - Port is manually added to voice VLAN.

`auto` - Port is added dynamically

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# voice vlan manual
(JGSM7224)(config-if)#
```

```
-------------------------------------------------------------------------------
```

Related Command

`show voice vlan ports` - Displays port status of voice VLAN.

show voice vlan globals

This command shows voice VLAN function global configurations.

Syntax `show voice vlan globals`

Mode Privileged Exec

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show voice vlan globals

Voice Vlan Global Properties:
-----------------------------
Voice Vlan Status           : Enabled
Voice Vlan ID               : 2
Voice Vlan Cos              : 6
Voice Vlan Aging Time       : 1 days, 0 hours, 0 mins

(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`voice vlan enable` - Enable status of voice VLAN.

`voice vlan cos` - Set cos of voice VLAN.

`voice vlan aging` - Set aging time of voice VLAN.

show voice vlan oui

This command shows voice VLAN oui configurations.

Syntax `show voice vlan oui`

Mode Privileged Exec

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show voice vlan oui
```

```
Telephony  OUI       Description
---------------     --------------------
00:01:e3            SIEMENS
00:03:6b            CISCO1
00:04:0d            AVAYA1
00:0f:e2            H3C
00:12:43            CISCO2
00:1b:4f            AVAYA2
00:60:b9            NITSUKO
00:d0:1e            PINTEL
00:e0:75            VERILINK
00:e0:bb            3COM

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`voice vlan oui` - Add oui for voice VLAN.

show voice vlan ports

This command shows voice VLAN ports configurations.

Syntax	`show voice vlan ports`
Mode	Privileged Exec

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show voice vlan ports

Interface            Voice Vlan Mode      Membership
------------------   ------------------   ------------------

0/1                   AUTO                NOT ACTIVE
0/2                   AUTO                NOT ACTIVE
0/3                   AUTO                NOT ACTIVE

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`voice vlan mode` - Set port voice VLAN mode.

STP 18

STP (Spanning-Tree Protocol) is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. To establish path redundancy, STP creates a tree that spans all the switches in an extended network, forcing redundant paths into a standby, or blocked, state. For an Ethernet network to function properly, only one active path must exist between two stations. Multiple active paths between stations in a bridged network can cause loops in which Ethernet frames can endlessly circulate. STP can logically break such loops and prevent looping traffic from clogging the network. The dynamic control of the topology provides continued network operation in the presence of redundant or unintended looping paths.

The prompt for the Global Configuration Mode is `JGSM7224(config)#`.

spanning-tree mode

This command sets the spanning tree operating mode to multiple spanning tree protocol (MSTP). When the JGSM7224 boots up, Spanning Tree is enabled by default with MSTP operating in the switch. This command only starts and enables the spanning tree mode. However, port-roles and states will be computed only after enabling the spanning tree.

Syntax `spanning-tree mode mst`

Mode Global Configuration

`mst` - MSTP configuration.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree mode mst
--------------------------------------------------------------------------------
```

Related Commands

`shutdown spanning-tree` - Shuts down the spanning tree module.

`show spanning-tree - Detail` - Displays detailed spanning tree information.

spanning-tree

This command enables the spanning tree operation. The no form of the command disables the spanning tree operation.

Default	MSTP
Syntax	`spanning-tree` `no spanning-tree`
Mode	Global configuration

Example

```
-------------------------------------------------------------------------------
!Enable spanning-tree
(JGSM7224)(config)# spanning-tree
(JGSM7224)(config)#
-------------------------------------------------------------------------------
!Disable spanning-tree
(JGSM7224)(config)# no spanning-tree
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`show spanning-tree - Detail` - Displays detailed spanning tree information.

`show spanning-tree - brief` - Displays spanning tree information for active ports.

spanning-tree forceversion

This command sets the force version for the spanning tree protocol. The no form of the command sets the force version for spanning tree protocol to its default value.

Default	802.1s, MSTP compatible
Syntax	`spanning-tree forceversion {802.1d|802.1w|802.1s}` `no spanning-tree forceversion`
Mode	Global Configuration

`802.1d` - STP configuration.

`802.1w` - RSTP configuration.

`802.1s` - MSTP configuration.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree forceversion 802.1d
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`show spanning-tree` - Detail - Displays detailed spanning tree information.

`show spanning-tree` - brief - Displays spanning tree information of active ports.

spanning-tree timers

This command sets the spanning tree timers. The `no` form of the command sets the spanning tree timers to the default values. The following relation must be observed while configuring the timers: 2 x (Forward-time - 1) >= Max-age Max-Age >= 2 x (Hello-time +1). Configure the hello timers for forceversion MST on a per-port basis.

Default	max-age - 20 secs. forward-time - 15 secs. hello-time - 2 secs.
Syntax	`spanning-tree {forward-time <seconds(4-30)>|hello-time<seconds(1-2)>|maxage <seconds(6-40)>}` `no spanning-tree {forward-time|hello-time|max-age}`
Mode	Global Configuration

`forward-time` - Controls how fast a port changes its spanning tree state from Blocking state to Forwarding state.

`hello-time` - Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree.

`max-age` - The maximum age allowed for the Spanning Tree Protocol information learned from the network on any port before it is discarded.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree max-age 6
(JGSM7224)(config)# spanning-tree hello-time 1
(JGSM7224)(config)# spanning-tree forward-time 4
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`show spanning-tree` - Detail - Displays detailed spanning tree information.

`show spanning-tree` - brief - Displays spanning tree information of active ports.

spanning-tree hold-count

This command sets the transmit hold-count value. The `no` form of the command sets the transmit hold count to the default value. Transmit hold count value is a counter used to limit the maximum transmission rate of the switch.

Default 3

Syntax
```
spanning-tree hold-count <value (1-10)>
no spanning-tree hold-count
```

Mode Global configuration

`hold-count`- A counter used to limit the maximum transmission rate of the switch.

Example

```
--------------------------------------------------------------------------------
! Set Forward Time 5 seconds
(JGSM7224)(config)# spanning-tree hold-count 5
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`show spanning-tree - detail` - Displays detailed spanning tree information.

`show spanning-tree - brief` - Displays spanning tree information on active ports.

spanning-tree max-hops

This command sets the maximum number of hops permitted in the MST. The `no` form of the command sets the maximum number of hops permitted in the MST to the default value. The root switch of the instance always sends a BPDU with a cost of 0 and the hop count set to the maximum value.

Default 20

Syntax
```
spanning-tree max-hops <value(6-40)>
no spanning-tree max-hops
```

Mode Global configuration

`max-hops` - Maximum number of hops permitted in the MST.

Example

```
-----------------------------------------------------------------------------
!Set Max Hop 10
(JGSM7224)(config)# spanning-tree max-hops 10
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Command

`show spanning-tree mst` - Displays multiple spanning tree instance configuration.

spanning-tree priority

This command sets the Bridge Priority for the spanning tree only in steps of 4096. The no form of the command sets the Bridge Priority to the default value.

The command `spanning-tree priority` *xxx* configures the priority in RSTP, if RSTP is running, or configures the CIST priority if MSTP is running. The command `spanning-tree mst instance priority` configures the priority in MSTI and is supported only if MSTP is running.

Default	32768
Syntax	`spanning-tree mst priority <instance-id(0-16)> <value(0-61440)>` `no spanning-tree mst priority <instance-id(1-16)>`
Mode	Global configuration

`instance-id` - ID range of spanning tree instances. 0 is for CIST.

`priority` - Switch priority for the specified spanning-tree instance.

Example

```
-----------------------------------------------------------------------------
!Set CIST priority 4096
(JGSM7224)(config)# spanning-tree mst priority 0 4096
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

The command `spanning-tree mst priority 0` *xxx* configures the priority in RSTP if RSTP is running, or configures the CIST priority if MSTP is running. The command `spanning-tree mst priority (1-16)` *xxx* configures the priority in MSTP and is supported only if MSTP is running.

Related Commands

`show spanning-tree - detail` - Displays detailed spanning tree information.

`show spanning-tree - brief` - Displays spanning tree information on active ports.

spanning-tree edgeport all

This command sets all ports as edge ports. The no form of the command resets it.

Syntax `spanning-tree edgeport all`
`no spanning-tree edgeport all`

Mode Global configuration

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree edgeport all
(JGSM7224)(config)#
------------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning-tree configuration of the interface.

spanning-tree port mode all

This command sets all ports to enable stp. The no form of the command disables it.

Syntax `spanning-tree port mode all`
`no spanning-tree port mode all`

Mode Global configuration

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree port mode all
(JGSM7224)(config)#
------------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning-tree configuration of the interface.

spanning-tree configuration name

This command sets the configuration name for the MST region. The no form of the command resets the configuration name. The name string is case-sensitive.

Default Default configuration name is the bridge MAC address

Syntax
```
spanning-tree configuration name <string(32)>
no spanning-tree configuration name
```

Mode Global configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree configuration name regionone
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show spanning-tree mst configuration` - Displays multiple spanning tree instance configuration.

spanning-tree configuration revision

This command sets the configuration revision number for the MST region. The no form of the command deletes the configuration revision number.

Default 0

Syntax
```
spanning-tree configuration revision <value(0-65535)>
no spanning-tree configuration revision
```

Mode Global configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree configuration revision 100
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show spanning-tree mst configuration` - Displays multiple spanning tree instance configuration.

spanning-tree mst instance

This command creates an MST instance. The no form of the command deletes the instance.

Syntax `spanning-tree mst instance <instance-id(1-16)>`
`no spanning-tree mst instance <instance-id(1-16)>`

Mode Global configuration

`instance-id` - Instance ID.

Related Command

`show spanning-tree mst configuration` - Displays multiple spanning tree instance configuration.

spanning-tree mst vlan

This command maps VLANs to an MST instance. The no form of the command unmaps specific VLANs from the MST instance. A single VLAN identified by VLAN ID number is specified by a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.

Default VLANs mapped for instance 0: 1-1024, 1025-2048, 2049-3072, 3073-4094.

Syntax `spanning-tree mst vlan <instance-id(1-16)> <vlan-range>`
`no spanning-tree mst <instance-id(1-16)> [vlan <vlan-range>]`

Mode Global configuration

`instance-id` - Instance ID.

`vlan` - VLAN range associated with a spanning-tree instance.

Example

```
--------------------------------------------------------------------------------
! Map vlan 2 to instance 2
(JGSM7224)(config)# spanning-tree mst vlan 2 2
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show spanning-tree mst configuration` - Displays multiple spanning tree instance configuration.

spanning-tree auto-edge

This command enables automatic detection of a bridge attached on an interface. The no form of the command disables automatic detection of a bridge attached on an interface.

Default auto

Syntax
```
spanning-tree auto-edge
no spanning-tree auto-edge
```

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree auto-edge
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning-tree configuration of the interface.

spanning-tree link-type edgeport

This command sets the spanning tree properties of an interface. The no form of the command sets the spanning tree properties of an interface to the default value. In case of MSTP, this configuration applies to the CIST content.

Default edgeport - Not in edgeport
link-type - Auto-detect

Syntax
```
spanning-tree {link-type {point-to-point | shared} | edgeport}
no spanning-tree {link-type | edgeport}
```

Mode Interface Configuration

`link-type` - The link can be a point-to-point link or can be a shared LAN segment on which another bridge is present.

`edgeport` - Specifies that the port has only hosts connected and can transition to forwarding rapidly.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree edgeport
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning-tree configuration of the interface.

spanning-tree - Properties of an interface

This command sets the spanning tree properties of an interface. The no form of the command sets the spanning tree properties of an interface to the default value. In case of MSTP, this configuration applies to the CIST content.

Default	cost - 0 means not set, and opercost is initialized on speed port-priority - 128 pseudoRootId - Default is bridge ID
Syntax	`spanning-tree mst 0 {cost <value(1-200000000)> | port-priority <value(0-240)> | pseudoRootId priority <short(0-61440)> mac-address <ucast_mac>}` `no spanning-tree mst 0 {cost | port-priority | pseudoRootId}`
Mode	Interface Configuration

`cost` - The pathcost value associated with the port.

`port-priority` - The port priority value.

`pseudoRootId` - The pseudo RootId.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree mst 0 cost 2200
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning-tree configuration of the interface.

spanning-tree port mode

This command sets the spanning tree status for the interface. In case of MSTP, this configuration applies to the CIST context.

Default	Enabled
Syntax	`spanning-tree port mode` `no spanning-tree port mode`
Mode	Interface Configuration

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree port mode
(JGSM7224)(config)#
------------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning-tree configuration of the interface.

spanning-tree guard root - none

This command enables the root-guard/restricted role feature, which prevents the specific port from becoming the root port. The no form of the command disables the root-guard/restricted role feature on the port.

Default	Disabled
Syntax	`spanning-tree guard {root | none}` `no spanning-tree guard`
Mode	Interface Configuration

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree guard root
(JGSM7224)(config-if)#
------------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning-tree configuration of the interface.

spanning-tree tcnguard

This command enables the topology change guard/restricted TCN feature, which prevents the topology change caused on that port. The no form of the command disables the topology change guard/restricted TCN feature on the port.

Default	Disabled
Syntax	`spanning-tree tcnguard` `no spanning-tree tcnguard`
Mode	Interface Configuration

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree tcnguard
(JGSM7224)(config-if)#
------------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning-tree configuration of the interface.

spanning-tree layer2-gateway-port

This command enables the layer2 gateway port, generates PseudoInfo Bpdu, and sends it to the port information state machine for further processing. It makes the switch a virtual root. The no form of the command disables layer2 gateway port on the port. Bpdu transmit should be disabled on the L2gp port.

Default	Disabled
Syntax	`spanning-tree layer2-gateway-port` `no spanning-tree layer2-gateway-port`
Mode	Interface Configuration

Example

```
------------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree layer2-gateway-port
(JGSM7224)(config-if)#
------------------------------------------------------------------------------
```

Related Commands

`spanning-tree bpdu-transmit` - Set bpdu transmit status of an interface.

`show spanning-tree interface` - Displays the spanning tree properties of an interface.

spanning-tree bpdu-receive

This command enables and disables the bpdu receive status on the port.

Default	Enabled
Syntax	`spanning-tree bpdu-receive {enabled | disabled}`
Mode	Interface Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree bpdu-receive disabled
(JGSM7224)(config-if)#
-----------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning tree properties of an interface.

spanning-tree bpdu-transmit

This command enables and disables the bpdu transmit status on the port.

Default	Enabled
Syntax	`spanning-tree bpdu-transmit {enabled | disabled}`
Mode	Interface Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree bpdu-transmit disabled
(JGSM7224)(config-if)#
-----------------------------------------------------------------------------
```

Related Command

`show spanning-tree interface` - Displays the spanning tree properties of an interface.

spanning-tree pathcost dynamic

This command enables dynamic pathcost calculation. The `no` form of the command disables dynamic pathcost calculation.

On execution of this command, the pathcost of all the ports will be calculated dynamically based on the speed of the interface. If the cost has already been configured for a cist or an rstp interface, then this command has no effect on those interfaces. If the cost has been configured previously for an mst instance on a particular interface, then this command has no effect on that instance in the specified interface. Whereas the pathcost of all the other instances on the same interface will be calculated dynamically.

Default	Disabled
Syntax	`spanning-tree pathcost dynamic` `no spanning-tree pathcost dynamic`
Mode	Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree pathcost dynamic
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`spanning-tree forceversion` - Sets the force version for the spanning tree protocol.

`spanning-tree - Properties of an interface` - Sets the spanning tree properties of an interface.

`spanning-tree mst - Properties of an interface for MSTP` - Sets the spanning tree properties of an interface for MSTP.

spanning-tree bpdumigrationcheck

This command restarts the protocol migration process on all interfaces and forces renegotiation with the neighboring switches. The port protocol migration count gets incremented consistently when there is a protocol migration.

Syntax `spanning-tree bpdumigrationcheck { {<slot/port> | port-channel <integer(1-8)>} | all}`

Mode Global Configuration

`interface` - Restarts the protocol migration process on the specified interface. Valid interfaces include physical ports and port channels.

Example

```
-------------------------------------------------------------------------------
!Reset STP Migration
(JGSM7224)(config)# spanning-tree bpdumigrationcheck interface 0/1
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`show spanning-tree interface` - Displays the spanning tree properties of an interface.

`show spanning-tree mst -` Port Specific Configuration - Displays multiple spanning tree port specific configuration.

spanning-tree bpduforwarding

This command enables the bpdu flooding feature. The no form of the command disables it. The bpdu forwarding will take effect only if stp is disabled globally.

Default Disabled

Syntax
```
spanning-tree bpduforwarding
no spanning-tree bpduforwarding
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
!Set BPDU forwarding
(JGSM7224)(config)# spanning-tree bpduforwarding
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show spanning-tree - brief` - Displays spanning tree information of active ports.

spanning-tree mst - Properties of an interface for MSTP

This command sets the spanning tree properties of an interface for MSTP. The no form of the command sets the spanning tree properties of an interface to the default value. The MST instance must exist prior to using this command. If all interfaces have the same priority value, the MST sets the interface with the lowest interface number in the forwarding state and blocks other interfaces.

Default cost - 0 means not set, and opercost is initialized on speed.
port-priority - 128.
disable - Not set.
pseudoRootId - Default is bridge ID

Syntax
```
spanning-tree mst <instance-id(1-16)> {cost
<value(1-200000)>|port-priority <value(0-240)>|disable|
pseudoRootId priority <short(0-61440)> mac-address <ucast_mac>}
no spanning-tree mst
<instance-id(1-16)>{cost|port-priority|disable|pseudoRootId}
```

Mode Interface Configuration

`cost` - The cost value associated with the port.

`port-priority` - Port priority value.

`disable` - Disables the spanning tree on the port.

`pseudoRootId` - Set the pseudo RootID.

Example

```
-----------------------------------------------------------------------------
! Configure the MSTP instance 2 cost to 4000
(JGSM7224)(config)# spanning-tree mst 2 cost 4000
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Command

`show spanning-tree mst` - `CIST (`or specified MST Instance) - Displays the spanning tree properties of an interface for an MSTP instance.

spanning-tree mst hello-time

This command sets the port-based hello timer value. The `no` form of the command sets the port-based hello timer value to its default. Changing the spanning-tree mst hello-time value affects all spanning-tree instances active on the interface.

Default 2 seconds

Syntax

```
spanning-tree mst hello-time <value(1-10)>
no spanning-tree mst hello-time
```

Mode Interface Configuration

`hello-time` - Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# spanning-tree mst hello-time 5
(JGSM7224)(config-if)#
-----------------------------------------------------------------------------
```

Related Command

`show spanning-tree mst` - Port Specific Configuration - Displays multiple spanning tree port specific configuration.

spanning-tree mst max-instance

This command configures the Maximum MSTP Instance value (restricts the maximum instances that can be created). The no form of the command resets it to the default.

Default 16 instances

Syntax
```
spanning-tree mst max-instance <1-16>
no spanning-tree mst max-instance
```

Mode Global Configuration

`max-instance` - The maximum instances that can be created.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree mst max-instance 15
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show spanning-tree` - Detail - Displays detailed spanning tree information.

spanning-tree mst extended-sysid

This command enables the extended-sysid feature (the extended-sysid will add the instance ID into the bridge priority). The no form of the command disables extended-sysid.

Default Disabled

Syntax
```
spanning-tree mst extended-sysid
no spanning-tree mst extended-sysid
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# spanning-tree mst extended-sysid
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show spanning-tree` - Detail - Displays detailed spanning tree information.

clear spanning-tree counters

This command resets all bridge and port level statistics counters. Valid interfaces include physical ports and port channels. The port protocol migration count gets incremented consistently when there is a protocol migration.

Syntax `clear spanning-tree counters`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# clear spanning-tree counters
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`show spanning-tree interface` - Displays the spanning tree properties of an interface.

`show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific configurations.

shutdown spanning-tree

This command shuts down the spanning tree operation and releases memory. All configuration will be lost. The Bridge Module must be enabled for the MSTP to be started. The Bridge Module is always enabled and can never be disabled in JGSM7224.

Syntax `shutdown spanning-tree`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# shutdown spanning-tree
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`spanning-tree mode` - Sets the spanning tree operating mode.

`show spanning-tree - Detail` - Displays detailed spanning tree information for the STP/RST- P/MSTP configuration.

debug spanning-tree

This command provides spanning tree debugging support. The no form of the command disables debugging.

Default Disabled

Syntax

```
debug spanning-tree {global|
{all|errors|init-shut|management|memory|bpdu|events|timer|state-machine
{port-info|port-recieve|portrole-selection|role-transition|state-transit
ion|protocol-migration|topology-change|port-transmit|bridge-detection}|r
edundancy|semvariables}
no debug spanning-tree
{global|{all|errors|init-shut|management|memory|bpdu|events
|timer|state-machine {port-info|port-recieve |port-role-selection
|role-transition|state-transition|protocol-migration|topology-change
|port-transmit|bridge-detection}redundancy|semvariables}
```

Mode Privileged EXEC

`global` - Global debug messages.

`all` - All RSTP / MSTP debug messages.

`errors` - Error code debug messages.

`init-shut` - Init and shutdown debug messages.

`management`- Management messages.

`Memory` - Memory-related messages.

`bpdu`- BPDU-related messages.

`events`- Events-related messages.

`timer`- Timer module messages.

`state machine` - State-machine related debug messages.

`port-info` - Port information messages.

`port-receive` - Port received messages.

`port-role-selection` - Port - role selection messages.

`role-transition` - Role transition messages.

`state-transition` - State transition messages.

`protocol-migration` - Protocol migration messages.

`topology-change` - Topology change messages.

`port-transmit` - Port transmission messages.

`bridge-detection` - Bridge detection messages.

`redundancy` - Redundancy-related messages.

`semvariables` - State-machine variables debug messages.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug spanning-tree all
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show spanning-tree - Detail` - Displays detailed spanning tree information for the STP/RST- P/MSTP configuration.

show spanning-tree - summary

This command displays spanning tree information.

Default	Enabled by default with MSTP operating in the switch
Syntax	`show spanning-tree [summary]`
Mode	Privileged EXEC

`summary` - Summary of port states.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show spanning-tree
Root Id      Priority    32768
             Address     00:33:aa:11:44:55
             Cost        0
             Port        0 [0]
             This bridge is the root
             Max age 20 Sec, forward delay 15 Sec
Spanning tree Forward BPDU: Disabled
MST00
Spanning tree Protocol has been enabled
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id    Priority    32768
             Address     00:33:aa:11:44:55
             Max age is 20 sec, forward delay is 15 sec
             Dynamic Path Cost is Disabled
Name    Role          State         Cost      Prio    Type
----    ----          -----         ----      ----    ------
0/1     Designated    Forwarding    200000    128     P2P
(JGSM7224)#
(JGSM7224)# show spanning-tree summary
```

```
Spanning tree Protocol has been enabled
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Spanning Tree port pathcost method is Long
MST00 Port Roles and States
Port-Index      Port-Role    Port-State  Port-Status
----------      ---------    ----------  -----------
0/3 Disabled    Discarding   Enabled
0/4 Disabled    Discarding   Enabled
0/5 Disabled    Discarding   Enabled
0/6 Disabled    Discarding   Enabled
0/7 Disabled    Discarding   Enabled
--------------------------------------------------------------------------------
```

Related Commands

`spanning-tree mode` - Sets the spanning tree operating mode.

`spanning-tree` - Enables the spanning tree operation.

`spanning-tree forceversion` - Sets the force version for the spanning tree protocol.

`spanning-tree timers` - Sets the spanning tree timers.

`spanning-tree hold-count` - Sets the transmit hold-count value.

`spanning-tree priority` - Sets the Bridge Priority for the spanning tree only in steps of 4096.

`spanning-tree` - Properties of an interface - Sets spanning tree properties of an interface.

`spanning-tree mst` - Properties of an interface for MSTP - Sets the spanning tree properties of an interface for MSTP.

`show spanning-tree interface` - Displays spanning-tree port configuration.

show spanning-tree - detail

This command displays detailed spanning tree information.

Syntax `show spanning-tree detail`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show spanning-tree detail

Spanning tree Protocol has been enabled
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Identifier has Priority 40960, Address 00:21:a8:c8:18:68
Configured   Max age 20 sec, Forward delay 15 sec
Configured Hello Time 2 sec
```

```
Dynamic Path Cost Enabled
Extended system Id Disabled
Max instance number 16
We are root of the spanning tree
Current Root has priority 40960, address 00:21:a8:c8:18:68
cost of root path is 0
Number of Topology Changes 74, Time since topology Change 344 seconds ago
Mstp Up Count 1, Mstp Down Count 0
New Root Id Count 38
Transmit Hold-Count 3
Times : Max age 20 Sec,Forward delay 15 Sec

Port 11 [0/11] of MST00 is Designated, Forwarding
0/1 is operating in the MSTP Mode
Port path cost  200000, Port priority  128,
Port Identifier  128.11. Port HelloTime  2,
Timers: Hello - 0, Forward Delay - 0, Topology Change - 0
Designated root has priority 40960, address 00:21:a8:c8:18:68
Designated Bridge has priority 40960, address 00:21:a8:c8:18:68
Designated Port Id is 128.11, Designated pathcost is 0
Operational Forward delay 15, Max age 20
Number of Transitions to forwarding State : 5
AutoEdge is enabled
AdminEdge is disabled
OperEdge is enabled
Link type is point to Point
BPDUs : sent 228463, received 0
Restricted TCN is disabled.
bpdu-transmit enabled
bpdu-receive enabled
BPDU Flood Mode disabled
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`spanning-tree mode` - Sets the spanning tree operating mode.

`spanning-tree` - Enables the spanning tree operation.

`spanning-tree forceversion` - Sets the compatibility version for the spanning tree protocol.

`spanning-tree timers` - Sets the spanning tree Timers.

`spanning-tree hold-count` - Sets the transmit hold-count value.

`spanning-tree priority` - Sets the Bridge Priority for the spanning tree only in steps of 4096.

`spanning-tree` - Properties of an interface - Sets spanning tree properties of an interface.

`spanning-tree mst` - Properties of an interface for MSTP - Sets the spanning tree properties of an interface for MSTP.

`show spanning-tree interface` - Displays Spanning-tree port configuration.

show spanning-tree - brief

This command displays spanning tree information about active ports.

Syntax `show spanning-tree brief`

Mode Privileged EXEC

`brief` - Displays brief information about the port and bridge.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show spanning-tree brief
Root Id        Priority    32768
               Address     00:05:04:03:02:01
               Cost        6666
               Port        25 [po1]
               Max age 20 Sec, forward delay 15 Sec
Spanning tree Forward BPDU: Enabled
MST00
Spanning tree Protocol has been enabled
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id      Priority    32768
               Address     00:33:aa:11:44:55
               Max age is 20 sec, forward delay is 15 sec
               Dynamic Path Cost is Enabled
Name    Role        State       Cost     Prio  Type
----    ----        -----       ----     ----  ------
0/1     Designated  Forwarding  200000   128   P2P
0/12    Alternate   Discarding  20000    128   P2P
po1     Root        Forwarding  6666     128   P2P
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`spanning-tree mode` - Sets the spanning tree operating mode.

`spanning-tree` - Enables the spanning tree operation.

`spanning-tree forceversion` - Sets the compatibility version for the spanning tree protocol.

`spanning-tree timers` - Sets the spanning tree Timers.

`spanning-tree hold-count` - Sets the transmit hold-count value.

`spanning-tree priority` - Sets the Bridge Priority for the spanning tree only in steps of 4096.

`spanning-tree` - Properties of an interface - Sets spanning tree properties of an interface.

`spanning-tree mst` - Properties of an interface for MSTP - Sets the spanning tree properties of an interface for MSTP.

`show spanning-tree interface` - Displays Spanning-tree port configuration.

show spanning-tree interface

This command displays the Spanning-tree port configuration. Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels.

Syntax `show spanning-tree interface <slot/port> | port-channel <integer (1-8)> [detail | stats]`

Mode Privileged EXEC

`detail` - Displays details about the port and bridge.

`stats` - Displays statistics about the port.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show spanning-tree interface 0/7

Instance  Role        State       Cost     Prio      type
--------  ----        -----       ----     ----      ----
MST00     Designated  Forwarding  200000   128.7     P2P

(JGSM7224)# show spanning-tree interface 0/7 detail

Port 11 [0/11] of MST00 is Designated, Forwarding
0/11 is operating in the MSTP Mode
Port path cost 200000, Port priority 128,
Port Identifier 128.1. Port HelloTime 2,
Timers: Hello - 0, Forward Delay - 0, Topology Change - 0
Designated root has priority 40960, address 00:21:a8:c8:18:68
Designated Bridge has priority 40960, address 00:21:a8:c8:18:68
Designated Port Id is 128.11, Designated pathcost is 0
Operational Forward delay 15, Max age 20
Number of Transitions to forwarding State : 5
AutoEdge is enabled
AdminEdge is disabled
OperEdge is enabled
```

```
Link type is point to Point
BPDUs : sent 228711, received 0
Restricted Role is disabled.
Restricted TCN is disabled.
bpdu-transmit enabled
bpdu-receive enabled
BPDU Flood Mode disabled

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`spanning-tree` - Properties of an interface - Sets spanning tree properties of an interface.

`spanning-tree mst` - Properties of an interface for MSTP - Sets the spanning tree properties of an interface for MSTP.

`show spanning-tree` - Detail - Displays detailed spanning tree information.

`show spanning-tree` - brief - Displays spanning tree information of active ports.

`spanning-tree bpdumigrationcheck` - Restarts the protocol migration process on all the interfaces.

`clear spanning-tree counters` - Resets all bridge and port level statistics counters.

show spanning-tree layer2-gateway-port

This command displays the Spanning-tree port configuration.

Syntax `show spanning-tree layer2-gateway-port [interface <slot/port> | port-channel <integer (1-8)>]`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show spanning-tree layer2-gateway-port
Port 0/1
PseudoRootId
Instance   Priority   MacAddress            State
---------- ---------- ------------------   ----------
MST00      4096       00:00:00:00:00:01     Forwarding
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`spanning-tree layer2-gateway-port` - Sets layer2-gateway-port status of an interface.

show spanning-tree mst - CIST or specified mst Instance

This command displays multiple spanning tree information for the CIST (Common Internal Spanning Tree) Instance or specified MST Instance.

Syntax `show spanning-tree mst [<instance-id(1-16)>] [detail]`

Mode Privileged EXEC

`instance-id` - Range of Spanning tree instances.

`detail` - Spanning tree mst instance specific details.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show spanning-tree mst
## MST00
Bridge       Address  00:33:aa:11:44:55    Priority 32768
Root         Address  00:00:00:00:00:01    Priority 4096
                  Port 0/1 ,  path cost 0
IST Root Address 00:00:00:00:00:01 Priority  4096
                  Path cost 200000
Configured Forward delay 15, Max age 20, Max hops 20
Operational Forward delay 15, Max age 20
Interface    Role    Sts           Cost    Prio.Nbr   Type
---------    ----    ---           ----    --------   ----
0/1          Root    Forwarding    200000  128.1      P2P
(JGSM7224)# show spanning-tree mst 1 detail
## MST01 Vlans
mapped: 2 Bridge Address 00:01:02:03:04:11 Priority 32768
Root Address 00:01:02:03:04:11 Priority 32768 Root this switch for MST01
0/1 of MST01 is Master, Forwarding Port info port id 128.1
priority 128 cost 2000000 Designated root address 00:01:02:03:04:11
priority 32768 cost 0 Designated bridge address 00:01:02:03:04:11
priority 32768 port id 128.1
--------------------------------------------------------------------------------
```

Related Commands

`instance` - Maps VLANs to an MST instance.

`spanning-tree priority` - Sets the Bridge Priority for the spanning tree only in steps of 4096.

`spanning-tree mst` - Properties of an interface for MSTP - Sets the spanning tree properties of an interface for MSTP.

show spanning-tree mst configuration

This command displays the multiple spanning tree instance configuration.

Syntax `show spanning-tree mst configuration`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show spanning-tree mst configuration
Name [JGSM7224]
Revision 2
Digest Key 0x3ab68794d602fdf43b21c0b37ac3bca8
Format Selector 0
Instance   Vlans mapped
--------   ----------------------------------------
0          1,3-1024,1025-2048,2049-3072,3073-4094
1          2
--------------------------------------------------------
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`name` - Sets the configuration name.

`revision` - Sets the configuration revision number.

`instance` - Maps VLANs to an MST instance.

show spanning-tree mst - Port Specific Configuration

This command displays the multiple spanning tree port specific configuration. Valid interfaces include physical ports and port channels.

Syntax `show spanning-tree mst port [<instance-id(1-16)>] interface <slot/port> | port-channel <integer (1-8)> [{stats|hello-time|detail}]`

Mode Privileged EXEC

`instance-id` - Range of spanning tree instances.

`interface` - Details about a particular interface.

`stats` - Displays the input and output packets by switching path for the interface.

`hello-time` - Determines how often the switch broadcasts its hello message to other switches when it is the root of the spanning tree.

`detail` - Detailed multiple spanning tree port specific configuration.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show spanning-tree mst 1 interface 0/1
Instance  Role  Sts  Cost  Prio.Nbr
--------  ----  ---  ----  --------
1 Master Forwarding 2000000 128.1
(JGSM7224)# show spanning-tree mst 1 interface 0/1 stats
MST01 Bpdus sent 2, Received 0
(JGSM7224)# show spanning-tree mst 1 interface 0/1 hello-time
MST01 2
(JGSM7224)# show spanning-tree mst 1 interface 0/1 detail
0/1 of MST01 is Master , Forwarding Port info port id
128.1 priority 128 cost 2000000 Designated root address
00:01:02:03:04:11  priority 32768 cost 0 Designated bridge address
00:01:02:03:04:11  priority 32768 port id 128.1
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`instance` - Maps VLANs to an MST instance.

`spanning-tree mst hello-time` - Sets the port based hello timer value.

`spanning-tree` - Properties of an interface - Sets spanning tree properties of an interface. show customer spanning-tree - Displays the detailed customer spanning information.

`show spanning-tree mst` - CIST or specified mst Instance- Displays multiple. spanning tree information for the CIST Instance or specified MST Instance.

`show spanning-tree interface` - Displays Spanning-tree port configuration.

`spanning-tree bpdumigrationcheck` - Restarts the protocol migration process on all the interfaces.

`clear spanning-tree counters` - Resets all bridge and port level statistics counters.

PNAC 19

dot1x system-auth-control

This command enables dot1x in the switch. The no form of this command disables dot1x in the switch. You must enable authentication, authorization, and accounting (AAA), and specify the authentication method before enabling 802.1x globally. 802.1x can be enabled on L2 static access interfaces but can't be enabled on the lacp port.

Default Disabled

Syntax
```
dot1x system-auth-control
no dot1x system-auth-control
```

Mode Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# dot1x system-auth-control
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`shutdown dot1x` - Shuts down dot1x capability.

`show dot1x` - Displays dot1x information.

aaa authentication dot1x default

This command enables the dot1x local authentication or RADIUS server based remote authentication method for all ports.Only one method can be specified at a time. The first method will be used and the rest discarded if more than one are specified.

Default local

Syntax `aaa authentication dot1x default {group radius|local}`

Mode Global Configuration

`group radius` - RADIUS server-based authentication.

`local` - Local authentication.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# aaa authentication dot1x default group radius
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`radius-server host` - Specifies RADIUS query parameters.

`dot1x local-database` - Configures the dot1x authentication server database with user name and password.

`show dot1x` - Displays dot1x detailed information.

dot1x local-database

This command configures the dot1x authentication server database with username and password. The no form of the command deletes an entry from the dot1x authentication server database.

The command adds users to the local database only for local authentication. The auth-timeout parameter represents the time in seconds after which access to the port is denied for the user. When the timeout value is 0, the authenticator uses the re-authentication period of the authenticator port. If the port list is not configured, the user will be allowed or denied access on all the ports.

Default

`permission` - allow

`interface-list` - all physical interfaces

Syntax

```
dot1x local-database <username> password <password> permission
{allow|deny} [<auth-timeout (value(1-7200))>] [interface
<interface-list>]
no dot1x local-database <username>
```

Mode Global Configuration

`username` - User name.

`password` - Password.

`permission` - Specifies whether the user must be allowed or denied access on a set of ports.

`auth-timeout` - Number of seconds between authentication attempts.

`interface` - Port list of the interface on which dot1x authentication can be applied.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# dot1x local-database fsoft password admin123 permission
allow auth-timeout 6000
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`aaa authentication dot1x` default - Enables dot1x local authentication.

`show dot1x` - Displays dot1x local database information.

set nas-id

This command sets the dot1x network access server ID. The Network Access Server Identifier is set in the RADIUS packets sent to the Remote Authentication Server.

Default	fsNas1
Syntax	`set nas-id <identifier>`
Mode	Global Configuration

`identifier` - A string length of 16 that specifies the dot1x network access server ID.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# set nas-id Identifier
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show dot1x` - Displays dot1x information.

dot1x max-req

This command sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client before restarting the authentication process. The `no` form of the command sets the maximum number of EAP retries to the client to default value. The default value of this command must be changed only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with RADIUS server or local clients.

Default	Count
Syntax	`dot1x max-req <count(1-10)>` `no dot1x max-req`
Mode	Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# dot1x max-req 5
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show dot1x` - Displays dot1x information

dot1x reauthentication

This command enables periodic re-authentication from authenticator to client. The `no` form of the command disables periodic re-authentication from authenticator to client.The amount of time between periodic re-authentication attempts can be configured using the `dot1x timeout reauth-period` interface configuration command.

Default	Disabled
Syntax	`dot1x reauthentication` `no dot1x reauthentication`
Mode	Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# dot1x reauthentication
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`dot1x timeout` - Sets the dot1x timers.

`show dot1x` - Displays dot1x information.

dot1x timeout

This command sets the dot1x timers. The no form of the command sets the dot1x timers to the default values. Only one timer can be configured using this command. That is, the user can configure either the quiet-period or tx-period, but not both.

Default

`quiet-period` - 60 seconds.
`reauth-period` - 3600 seconds.
`server-timeout` - 30 seconds.
`supp-timeout` - 30 seconds.
`tx-period` - 30 seconds.
`guest-vlan-period` - 90 seconds.

Syntax

```
dot1x timeout {quiet-period <value (0-65535)> | {reauth-period |
servertimeout | supp-timeout | tx-period} <value (1-65535)> |
guest-vlan-period <value (1-300)>}
no dot1x timeout {quiet-period | reauth-period | server-timeout |
supp-timeout | tx-period | guest-vlan-period}
```

Mode Interface Configuration

`quiet-period` - Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.

`reauth-period` - Number of seconds between re-authentication attempts.

`server-timeout` - Number of seconds that the switch waits for the response from the authentication server.

`supp-timeout` - Number of seconds that the switch waits for the response from the client.

`tx-period` - Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.

`guest-vlan-period` - Number of seconds that the switch waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured).

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# dot1x timeout quiet-period 30


(JGSM7224)(config-if)# dot1x timeout supp-timeout 25
-------------------------------------------------------------------------------
```

Related Commands

`dot1x max-req` - Sets the maximum number of EAP retries to the client before restarting authentication process.

`dot1x reauthentication` - Enables periodic re-authentication of the client.

`show dot1x` - Displays dot1x information.

`dot1x guest-vlan` - Specifies an active VLAN as a guest vlan on a per port basis.

dot1x port-control

This command configures the authenticator port control parameter. The `no` form of the command sets the authenticator port control state to force authorized.

Syntax `dot1x port-control {auto | force-authorized | force-unauthorized | mac-based}`
`no dot1x port-control`

Mode Interface Configuration

`force-authorized` - All traffic will be allowed without any restrictions.

`force-unauthorized` - All traffic over the interface will be blocked.

`auto` - Enables 802.1x port-based authentication on the interface.

`mac-based` - Enables 802.1x MAC-based authentication on the interface.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# dot1x port-control auto
(JGSM7224)(config-if)#
-----------------------------------------------------------------------------
```

Related Commands

`show dot1x` - Displays dot1x information

dot1x control-direction

This command configures the port control direction. The `no` form of the command sets the authenticator port control direction to `both`.

Default both

Syntax `dot1x control-direction {in|both}`
`no dot1x control-direction`

Mode Interface Configuration

`in` - Authentication control is imposed only on the incoming packets.

`both` - Authentication control is imposed on both incoming and outgoing packets.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# dot1x control-direction in
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show dot1x` - Displays dot1x information.

dot1x initialize

This command initiates the authentication cycle of the specified port. The command initializes the port immediately.

Syntax `dot1x initialize interface <slot/port>`

Mode Privileged EXEC

`interface` - Port number of the interface to initialize.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# dot1x initialize interface 0/1
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show dot1x` - Displays dot1x information

dot1x re-authenticate

This command initiates re-authentication of the specified dot1x-enabled port. The command re-authenticates a port without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic reauthentication. Note that this command will be rejected if the port enabled MAC-based 802.1x authentication, or if the port is configured to force-authorized or force-unauthorized.

Syntax `dot1x re-authenticate interface <slot/port>`

Mode Privileged EXEC

`interface` - Port number of the interface to re-authenticate.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# dot1x re-authenticate interface 0/1
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show dot1x` - Displays dot1x information.

shutdown dot1x

This command shuts down dot1x capability. The `no` form of the command starts and enables dot1x capability. When shut down, all resources acquired by dot1x Module are released to the system.

Syntax	`shutdown dot1x` `no shutdown dot1x`
Mode	Global Configuration

`interface` - Port number of the interface to re-authenticate.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# shutdown dot1x
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`dot1x system-auth-control` - Enables dot1x in the switch.

`show dot1x` - Displays dot1x information.

debug dot1x

This command enables debugging of the dot1x module. The `no` form of the command disables debugging of dot1x module. A four-byte integer is used for enabling the level of tracing. Each BIT in the four-byte integer represents a particular level of Trace.

Default	Events debugging enabled
Syntax	`debug dot1x {all|errors|events|packets|state-machine|redundancy}` `no debug dot1x {all|errors|events|packets|state-machine|redundancy}`
Mode	Privileged EXEC

`all` - All dot1x debug messages.

`errors` - dot1x error code debug messages.

`events` - dot1x event debug messages.

`packets` - dot1x packet debug messages.

`state-machine` - State-machine related-event debug messages.

`redundancy` - Redundancy related debug messages.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug dot1x all
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show dot1x` - Displays dot1x information.

show dot1x

This command displays dot1x information. If no parameters are specified, global parameters appear. If the supplicant is not specified in the displaying of clients, than it will display all the authenticated or authenticating supplicant session table.

Syntax `show dot1x [{details interface <slot/port> | local-database | clients all | address <mac_addr> | statistics interface <slot/port> | summary {all | interface <slot/port>}}]`

Mode Privileged EXEC

`details` - Displays the detailed configuration for the specified port.

`local-database` - Displays the user database for the local authentication method.

`clients` - Displays the clients information for the specified client or all.

`statistics` - Displays the statistics information for the specified port.

`summary` - Displays the configuration summary of the specified port or all ports.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show dot1x

Dot1x Authentication Control          = Enabled
Dot1x Protocol Version                = 2
Dot1x Authentication Method           = Local
Vlan Assignment status                = Disabled
```

```
Nas ID                                  = fsNas1
(JGSM7224)# show dot1x local-database

Pnac Authentication Users Database
User name       test
Protocol        4
Timeout         0 seconds
Ports           0/1, 0/2, 0/3, 0/4, 0/5, 0/6, 0/7, 0/8,
                0/13, 0/14, 0/15, 0/16, 0/17, 0/19, 0/20,
                0/21, 0/22, 0/23,

Permission      Allow

(JGSM7224)

Port                  = 0/1
Protocol Version      = 2
PAE Capabilities      = Authenticator
Control Mode          = Mac-Based
AdminControlDirection = BOTH
OperControlDirection  = BOTH
Guest VLAN ID         = 0
Guest Vlan Period     = 90 Seconds
MaxReq                = 2
QuietPeriod           = 60 Seconds
Re-authentication     = Enabled
ReAuthPeriod          = 3600 Seconds
ServerTimeout         = 30 Seconds
SuppTimeout           = 30 Seconds
Tx Period             = 30 Seconds
Eapol Flood           = Disable
Supp MacAddress    AuthPAE State    Backend State   VLAN Assign
-------------      -------------    -------------   -----------
00:0a:eb:58:ab:17  AUTHENTICATED    IDLE            1   Default

(JGSM7224)# show dot1x statistics interface 0/1

PortStatistics Parameters for Dot1x
-----------------------------------
TxReqId         = 0
TxReq           = 0
TxTotal         = 0

RxStart         = 0
RxLogoff        = 0
RxRespId        = 0
RxResp          = 0
```

```
RxInvalid       = 0
RxLenErr        = 0
RxTotal         = 0

RxVersion       = 0
LastRxSrcMac    = 00:00:00:00:00:00

(JGSM7224)# show dot1x clients all

Pnac Mac Database
---------------------------------------
Supplicant Mac-Addr  = 00:0a:eb:58:ab:17
User Name            = admin
AuthSM State         = AUTHENTICATED
Auth-Session Status  = AUTHORIZED
Port Number          = 1
VLAN Id              = 1
VLAN Assigned        = Default
Terminate Cause      = Not Terminated Yet
Session time         = 500
--------------------------------------------------------------------------------
```

dot1x guest-vlan

This command specifies an active VLAN as a guest VLAN on a per port basis. The no form of the command disables guest VLAN on the interface.

Syntax `dot1x guest-vlan <vlan-id>`
`no dot1x guest-vlan`

Mode Interface Configuration

`vlan-id` - An active VLAN, the range is 1 to maximum VLAN ID.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# dot1x guest-vlan 4
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Commands

`show dot1x` - Displays dot1x information.

`dot1x timeout` - Sets the dot1x timers.

dot1x reauth-session

This command makes the supplicant device, which was authenticated on the MAC-based authentication enabled port, to re-authenticate.

Syntax `dot1x reauth-session <supp addr - aa.aa.aa.aa.aa.aa>`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# dot1x reauth-session 00:0a:eb:58:ab:98
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`dot1x port-control` - Sets the dot1x port control to auto, force-authorized, force-unauthorized, or MAC-based.

dot1x init-session

This command resets all authentication arguments for the supplicant device and initializes the authentication session. The command initiates the supplicant authentication session in the authenticator port, which enabled MAC-based 802.1x authentication.

Syntax `dot1x init-session <supp addr - aa.aa.aa.aa.aa.aa>`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# dot1x init-session 00:0a:eb:58:ab:98
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`dot1x port-control` - Sets the dot1x port control to auto, force-authorized, force-unauthorized, or mac-based.

dot1x eapol-flood

This command enables or disables the eapol flooding feature per port. The feature is affected only if the dot1x feature is disabled globally.

Default	Disabled
Syntax	`dot1x eapol-flood` `no dot1x eapol-flood`
Mode	Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# dot1x eapol-flood
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show dot1x` - Displays dot1x information.

RADIUS 20

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a client-server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices, such as routers, modem servers, switches, and so on. RADIUS is currently the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems. It is used for several reasons, including:

- RADIUS facilitates centralized user administration.
- RADIUS consistently provides some level of protection against an active attacker.

This chapter describes the CLI commands available for configuring RADIUS.

radius server host

This command configures the RADIUS client with the parameters (host, timeout, key, and retransmit). The no form of the command deletes RADIUS server configuration.

Default

`timeout` - 10 seconds.
`retransmit` - 3 attempts.
`key` - empty string.
`port` - 1812.

Syntax

```
radius server host <ip-address|hostname> [timeout <1-120>]
[retransmit <1-254>] key <secret-key-string> [port <1-65535>]
no radius server host <ip-address|hostname>
```

Mode

Global Configuration

`ipaddress` - Version 4 IP address.

`hostname` - DNS host name.

`timeout` - The time period in seconds that a client will wait for a response from the server before re-transmitting the request.

`retransmit` - The maximum number of attempts the client undertakes to contact the server.

`key` - Per-server encryption key. Specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The string length is 46.

`port` - UDP Port number.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# radius server host 10.0.0.1 key pass
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`aaa authentication dot1x` default - Enables the dot1x local authentication or RADIUS server based remote authentication method for all ports.

`show radius servers` - Displays RADIUS server configuration.

`show radius statistics` - Displays RADIUS statistics.

debug radius

This command enables RADIUS debugging options. The `no` form of the command disables RADIUS debugging options.

Default	Disabled
Syntax	`debug radius {all|errors|events|packets|responses|timers}` `no debug radius`
Mode	Privileged EXEC

`all` - All the RADIUS server messages.

`errors` - Error code debug messages.

`events` - Events related messages.

`packets` - Packets related messages.

`responses` - Server response related messages.

`timers` - Timer module related messages.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug radius all
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show radius server` - Displays RADIUS server configuration.

show radius server

This command displays the RADIUS server configuration.

Syntax `show radius servers`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show radius servers
Radius Server Host Information
------------------------------
Index                     : 1
Address Type              : ipv4
Server address            : 10.0.0.1
Shared secret             : admin123
Radius Server Status      : Enabled
Response Time             : 20
Maximum Retransmission    : 8
Port Number               : 1812
-----------------------------------------
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`radius server host` - Configures the RADIUS client with the parameters

show radius statistics

This command displays the RADIUS Server Statistics.

Syntax `show radius statistics`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show radius statistics
Radius Server Statistics
------------------------
```

```
Index                              : 1
Radius Server Address              : 10.0.0.1
UDP port number                    : 1812
Round trip time                    : 0
No of request packets              : 8
No of retransmitted packets        : 80
No of access-accept packets        : 0
No of access-reject packets        : 0
No of access-challenge packets     : 0
No of malformed access responses   : 0
No of bad authenticators           : 0
No of pending requests             : 97
No of time outs                    : 89
No of unknown types                : 0
No of Packets Dropped              : 0
-----------------------------------------
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`radius server host` - Configures the RADIUS client with the parameters

authorization network radius

Use this command to enable the switch to accept VLAN assignment by the RADIUS server. The no form of the command disables this option.

Default	Disabled
Syntax	`authorization network radius` `no authorization network radius`
Mode	Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# authorization network radius
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show dot1x` - Displays dot1x information.

TACACS 21

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client-server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing Network Access Security (NAS). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the Authentication, Authorization and Accounting (AAA) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration.
- Uses TCP for transport to ensure reliable delivery.
- Supports inbound authentication, outbound authentication, and change password requests for the Authentication service.
- Provides some level of protection against an active attacker.

This chapter describes the CLI commands available for configuring TACACS.

tacacs-server host

This command configures the TACACS server with parameters (host, timeout, and key). The no form of the command deletes the server entry from the TACACS server table.

Default `port` - 49.
`timeout` - 5 seconds.

Syntax
```
tacacs-server host <ipaddress|hostname> [single-connection] [port
<TCP port>] [timeout <time out in seconds>] [key <secret key>]
no tacacs-server host <ipaddress|hostname>
```

Mode Global Configuration

`ipaddress` - Version 4 IP address.

`hostname` - DNS host name.

`single-connection` - Establishes Single TCP connection to communicate with the TACACS server.

`port` - TCP Port number.

`timeout` - The time period in seconds for which a client will wait for a response from the server before closing the connection.

`key` - Per-server encryption key. Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The string length is 63.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# tacacs-server host 10.0.0.100 key TACACS
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show tacacs` - Displays the server for the TACACS client.

tacacs use-server address

This command selects a server from the list of servers maintained in the TACACS client and makes the TACACS client use the specified server. The no form of the command disables the configured TACACS active server.

Syntax

```
tacacs use-server address <ip-address>
no tacacs use-server address
```

Mode Global Configuration

`ipaddress` - Version 4 IP address.

`hostname` - DNS host name.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# tacacs use-server address 10.0.0.100
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show tacacs` - Displays the server for the TACACS client.

tacacs-server retransmit

This command specifies the number of times the client searches the active server from the list of servers maintained in the TACACS client, when the active server is not configured. The no form of the command sets the default retries.

Default 2

Syntax
```
tacacs-server retransmit <1-100>
no tacacs-server retransmit
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# tacacs-server retransmit 3
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

debug tacacs

This command sets the debug trace level for the TACACS client module. The no form of the command disables the debug trace level for the TACACS client module.

Default Disabled

Syntax
```
debug tacacs {all|info|errors|dumptx|dumprx}
no debug tacacs
```

Mode Privileged EXEC

`all` - All TACACS debug messages.

`info` - TACACS server information messages.

`errors` - Error code debug messages.

`dumptx` - Transmitted packet dump messages.

`dumprx` - Received packet dump messages.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug tacacs all
(JGSM7224)#
-------------------------------------------------------------------------------
```

show tacacs

This command displays the server for the TACACS client.

Syntax `show tacacs`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show tacacs
Server                        : 1
IPV4 Address                  : 10.0.0.5
     Single Connection        : no
     TCP port                 : 49
     Timeout                  : 5
     Secret Key               : TACACS
Server                        : 2
IPV4 Address                  : 12.0.0.5
     Single Connection        : no
     TCP port                 : 49
     Timeout                  : 5
     Secret Key               : TACACS
Client uses server            : 12.0.0.5
Tacacs server retransmit      : 2
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`tacacs-server host` - Configures the TACACS server with the parameters.

`tacacs use-server address` - Selects a server from the list of servers maintained in the TACACS client and makes the TACACS client use the specified server.

LA 22

Link aggregation (LA) is a method of combining physical network links into a single logical link for increased bandwidth. LA increases the capacity and availability of the communications channel between devices (both switches and end stations) using existing Fast Ethernet and Gigabit Ethernet technology. LA also provides load balancing where the processing and communication activity is distributed across several links in a trunk so that no single link is overwhelmed.

By taking multiple LAN connections and treating them as a unified, aggregated link, practical benefits in many applications can be achieved. LA provides the following important benefits:

- Higher link availability
- Increased link capacity
- Improvements are obtained using existing hardware (no upgrading to higher-capacity link technology is necessary)

When LA groups use LACP negotiation mode, a standby link will be determined if the number of ports in the aggregation exceeds the maximum number supported by the hardware. Traffic can be distributed across active links in the LA group. Other inactive links (including standby links) cannot distribute the traffic.

port-channel system priority

This command sets the LACP priority for the system. The no form of the command sets the LACP priority for the system to the default value. System Priority represents a 2-octet value indicating the priority value associated with the system involved in link aggregation. The switch with the lowest system priority value determines the standby and active links in the aggregation. Although this is a global configuration command, the priority takes effect only on EtherChannels that have physical interfaces with LACP enabled.

Default 0x8000 or 32768

Syntax
```
port-channel system priority <0-65535>
no port-channel system priority
```

Mode Global Configuration

`<0-65535>` - Port-channel system priority number in the range 0-65535.

Example

```
--------------------------------------------------------------------------------
! Set system-priority 5
(JGSM7224)(config)# port-channel system priority 5
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show port-channel system priority` - Displays the port-channel system priority.

port-channel load-balance

This command sets the load balancing policy. The no form of the command sets the load balancing policy to the default value. If the port-channel index is not mentioned in this command, the load-balancing must apply for all port-channels configured in the system. Initially, the port channel interface must have been configured for this command.

Default	Source and destination MAC address-based
Syntax	`port-channel load-balance {1|2|3|4|5|6}{lag <short (1-8)> | all}` `no port-channel load-balance {lag <short (1-8)> | all>}`
Mode	Global Configuration

1 - Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.

2 - Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.

3 - Load distribution is based on the source and destination MAC address.

4 - Load distribution is based on the source IP address.

5 - Load distribution is based on the destination IP address.

6 - Load distribution is based on the source and destination IP.

`<short (1-8)>` - Port channel number in the range 1-8.

`all` - Sets every configured port-channel with the same load-balance setting.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# port-channel load-balance 2 lag 1
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show port-channel` - Displays port-channels (LAGs) information.

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The `no` form of the command disables link trap notifications for the port-channel (LAG). The option `all` enables or disables link trap notifications for all the configured port-channels.

Syntax `port-channel linktrap {all | lag <integer (1-8)>}`
`no port-channel linktrap {all | lag <integer (1-8)>}`

Mode Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# port-channel linktrap all
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show port-channel` - Displays port-channels (LAGs) information.

port-channel name

This command defines a name for the port-channel (LAG), where `name` is an alphanumeric string of up to 15 characters.

Syntax `port-channel name {all | lag <integer (1-8)>}`

Mode Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# port-channel name all test
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show port-channel` - Displays port-channels (LAGs) information.

port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports. The no form of the command disables Link Aggregation Control Protocol (LACP) on all ports.

Syntax `port lacpmode enable all`
`no port lacpmode enable all`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# port lacpmode enable all
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show port-channel` - Displays port-channels (LAGs) information.

lacp actor port priority

This command sets the LACP port priority. The no form of the command sets the LACP port priority to the default value. Port priority determines whether the link is an active link or a standby link, when the number of ports in the aggregation exceeds the maximum number supported by the hardware. This command takes effect only on EtherChannel interfaces that are already configured for LACP. If the number of links in an aggregation exceeds the maximum supported by the hardware, then the links with lower priority become active links.

Default 128

Syntax `lacp actor port priority <0-65535>`
`no lacp actor port priority`

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# lacp actor port priority 1
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`port-channel system priority` - Globally sets the LACP system priority.

`show lacp` - Displays LACP actor/partner information.

addport

This command adds one port to the port-channel (LAG). If the port-channel is not present, then the port channel must be created.

Syntax `addport lag <channel-group-number(1-8)>`

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# addport lag 1
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`show port-channel` - Displays port-channels (LAG) information.

`show lacp` - Displays LACP actor/partner information.

deleteport

This command deletes the port from the port-channel (LAG).

Syntax `deleteport lag <channel-group-number (1-8)>`

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# deleteport lag 1
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show port-channel` - Displays port-channels (LAG) information.

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port. The `no` form of the command disables Link Aggregation Control Protocol (LACP) on a port.

Syntax `port lacpmode`
`no port lacpmode`

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# port lacpmode
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show port-channel` - Displays port-channels (LAG) information.

port-channel static

This command enables the static mode on a port-channel (LAG) interface. By default, the static mode for a new port-channel is disabled, which means the port-channel is dynamic. The `no` form of the command sets the static mode on a particular port-channel (LAG) interface to the default value. You can use this command only on port-channel interfaces.

Syntax

```
port-channel static
no port-channel static
```

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# port-channel static
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show port-channel` - Displays port-channels (LAG) information.

port lacptimeout

This command sets the LACP timeout period. The `no` form of the command sets the LACP timeout period to the default value. The `long` timeout value means that LACP PDU will be sent every 30 seconds and LACP timeout value (no packet is received from peer) is 90 seconds. The `short` timeout value means that LACP PDU will be sent every 1 second and timeout value is 3 seconds.

Default long

Syntax

```
port lacptimeout actor {long|short}
no port lacptimeout actor
```

Mode Interface Configuration

`long` - Long timeout value.

`short` - Short timeout value.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# port lacptimeout actor short
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show lacp` - Displays LACP actor/partner information.

show port-channel

This command displays port-channels (LAGs) information.

Syntax `show port-channel {<short (1-8)> | all | brief}`

Mode Privileged EXEC

`<short (1-8)>` - Port channel ID (1-8).

`all` - Show all port channel information.

`brief` - One-line summary per channel-group.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show port-channel 1

Local Interface ............................... lag 1
Channel Name .................................. ch1
Link State .................................... Up
Admin Mode .................................... Enabled
Type .......................................... Dynamic
Load Balance Option............................ 3
(Src/Dest MAC, VLAN, EType, incoming port)

Mbr     Device/   Port
Ports   Timeout   State
------------------------
0/1 actor/long    Bundle
    partner/long
0/2 actor/long    Bundle
    partner/long
0/3 actor/long    Down
    partner/long
```

```
(JGSM7224)#

(JGSM7224)# show port-channel brief

Logical Port-channel Name Link State Trap Type Mbr Ports Active Ports
Interface                          Flag
------------------------------------------------------------------------
lag 1   ch1               Up   Enabled Dynamic  0/1,      0/1,
                                                0/2,      0/2
                                                0/3
lag 2   ch2               Down Enabled Dynamic  0/5,
                                                0/6
lag 3   ch3               Down Enabled Dynamic
lag 4   ch4               Down Enabled Dynamic
lag 5   ch5               Down Enabled Dynamic
lag 6   ch6               Down Enabled Dynamic
lag 7   ch7               Down Enabled Dynamic
lag 8   ch8               Down Enabled Dynamic
------------------------------------------------------------------------------
```

Related Commands

`addport` - Adds one port to the port-channel (LAG).

`port-channel system priority` - Sets the LACP priority for the system.

`port-channel load-balance` - Sets the load balancing policy.

`lacp actor port priority` - Sets the LACP port priority.

`port lacptimeout` - Sets the LACP timeout period.

show port-channel system priority

This command displays the port-channel system priority.

Syntax `show port-channel system priority`

Mode Privileged EXEC

Example

```
------------------------------------------------------------------------------
(JGSM7224)# show port-channel system priority

System Priority ................................ 32768

(JGSM7224)#
------------------------------------------------------------------------------
```

Related Command

`port-channel system priority` - Sets the LACP priority for the system.

show lacp

This command displays LACP actor and partner information.

Syntax `show lacp {actor | partner} {<slot/port> | all}`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show lacp actor 0/1

Intf  Sys       Admin  Port      Admin
      Priority  Key    Priority  State
-----------------------------------------
0/1   0         1       128      ACT|AGG|LT0

(JGSM7224)#

-----------------------------------------
(JGSM7224)# show lacp partner 0/1

Intf  Sys     System            Oper     Prt    Prt    Oper
      Pri     ID                Key      Pri    Id     State
-------------------------------------------------------------------
0/1   32768   00:00:00:00:00:07  1       128    1       ACT|AGG|LT0

(JGSM7224)#
-------------------------------------------------------------------
```

Related Commands

`addport` - Adds one port to the port-channel (LAG).

`port-channel system priority` - Sets the LACP priority for the system.

`lacp actor port priority` - Sets the LACP port priority.

`port lacptimeout` - Sets the LACP timeout period.

debug lacp

This command specifies the debug levels for the LA module. The no form of the command resets the debug options for the LA module.

Default	Disabled
Syntax	`debug lacp ([all] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [shut])` `no debug lacp ([all] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [shut])`
Mode	Privileged EXEC

`all` - All messages.

`mgmt` - Management-related messages.

`data` - Data packets messages.

`ctrl` - Control-related messages.

`dump` - Dumping LACP frame messages.

`resources` - System resources management messages.

`buffer` - Buffer information messages.

`shut` - Shutdown messages.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug lacp all
(JGSM7224)#
-------------------------------------------------------------------------------
```

IGMP Snooping 23

IGMP (Internet Group Multicast Protocol) is the protocol a host uses to inform a router when it joins or leaves an Internet multicast group. IGMP is used only on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGS (IGMP Snooping) is a feature that allows the switch to listen in on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, the other computer can learn the multicast sessions to which other computers on the local network are listening. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

The prompt for the Global Configuration Mode is `(JGSM7224)(config)#`

set igmp

This command enables IGMP snooping in the switch or a specific VLAN. The no form of the command disables IGMP snooping in the switch or a specific VLAN.

Default Disabled

Syntax Global Configuration Mode:

```
set igmp
no set igmp
```

VLAN Mode:

```
set igmp <1-4094>
no set igmp <1-4094>
```

Mode Global Configuration
VLAN

Example

```
--------------------------------------------------------------------------------
!Enable igmp snooping
(JGSM7224)(config)# set igmp
(JGSM7224)(vlan)# set igmp 1
--------------------------------------------------------------------------------
```

Related Commands

`show igmpsnooping vlan-id` - Displays IGMP snooping information for a specific VLAN.

`show igmpsnooping` - Displays the IGMP snooping information for all VLANs.

set igmp mcrtrexpiretime

This command sets the IGMP snooping router port purge time-out, after which the port gets deleted if no IGMP router control packets are received. The no form of the command sets the IGMP snooping router port purge time-out to the default value.

Default 125

Syntax
```
set igmp mcrtrexpiretime <(60 - 600) seconds>
no set igmp mcrtrexpiretime
```

Mode Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# set igmp mcrtrexpiretime 70
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping mrouter` - Displays the router ports for all VLANs or specific VLAN.

set igmp groupmembership-interval

This command sets the IGMP snooping port purge time interval, after which the port gets deleted if no IGMP reports are received. The no form of the command sets the IGMP snooping port purge time to default value.

Default 260

Syntax
```
set igmp groupmembership-interval <(130 - 1225) seconds>
no set igmp groupmembership-interval
```

Mode Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# set igmp groupmembership-interval 150
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping` - Displays the IGMP snooping information for all VLANs.

set igmp auto-video

This command sets the IGMP snooping auto-video enabled or disable.

Default	Disabled
Syntax	`set igmp auto-video {enable | disable}`
Mode	Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# set igmp auto-video enable
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping auto-video` - Displays the IGMP snooping auto-video information for auto-video VLAN.

set igmp querier version

This command sets the IGMP snooping querier version.

Default	2
Syntax	`set igmp querier version <1-2>` `no set igmp querier version`
Mode	Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# set igmp querier version 1
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping` - Displays the IGMP snooping information for all VLANs.

set igmp querier address

This command sets the IGMP snooping querier source IP address.

Default	0.0.0.0.
Syntax	`set igmp querier address <ip_addr>` `no set igmp querier address`
Mode	Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# set igmp querier address 192.168.1.1
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping` - Displays the IGMP snooping information for all VLANs.

set igmp querier query-interval

This command sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The no form of the command sets the IGMP querier interval to the default value.

Default	125
Syntax	`set igmp querier query-interval <60-600>` `no set igmp querier query-interval`
Mode	Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# set igmp querier query-interval 60
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping` - Displays IGMP snooping information for all VLANs.

set igmp unknow-multicast filter

This command enables the filtering of unknown multicast packets to the VLAN. Packets with an unknown multicast address in the destination field will be dropped. This command is mainly used when IGMP snooping is enabled, to prevent flooding of unwanted multicast packets to every port. The no form of the command disables the filtering of unknown multicast packets. Unknown multicast packets will be flooded to all ports in the same VLAN.

Syntax `set igmp unknow-multicast filter`
`no set igmp unknow-multicast filter`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# set igmp unknow-multicast filter
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping` - Displays IGMP snooping information for all VLANs.

set igmp router-alert check

This command enables the Router-Alert validation for IGMP snooping packets. The no form of the command disables the Router-Alert validation for IGMP snooping packets.

Default Disabled

Syntax `set igmp router-alert-check`
`no set igmp router-alert-check`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# set igmp router-alert-check
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping` - Displays IGMP snooping information for all VLANs.

set igmp fast-leave

This command enables fast leave processing for a specific VLAN. The no form of the command disables fast leave processing for a specific VLAN.

Default Disabled

Syntax
```
set igmp fast-leave <1-4094>
no set igmp fast-leave <1-4094>
```

Mode VLAN

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(vlan)# set igmp fast-leave 1
(JGSM7224)(vlan)#
-------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping vlan-id` - Displays IGMP snooping information for a specific VLAN.

set igmp querier

This command configures the IGMP snooping switch as a querier for a specific VLAN. The no form of the command configures the IGMP snooping switch as non-querier for a specific VLAN.

Default Non-querier

Syntax
```
set igmp querier <1-4094>
no set igmp querier <1-4094>
```

Mode VLAN

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(vlan)# set igmp querier 1
(JGSM7224)(vlan)#
-------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping vlan-id` - Displays IGMP snooping information for a specific VLAN.

set igmp mrouter

This command statically configures the router ports for a VLAN. The no form of the command deletes the statically configured router ports for a VLAN.

Syntax

```
set igmp mrouter <1-4094>
no set igmp mrouter <1-4094>
```

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# set igmp mrouter 1
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping mrouter` - Displays the router ports for all VLANs or a specific VLAN.

debug igmpsnooping

This command specifies the debug levels for the IGMP snooping module. The no form of the command resets debug options for the IGMP snooping module.

Default Disabled

Syntax

```
debug igmpsnooping { [init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt]|all }
no debug igmpsnooping { [init][resources][tmr][src][grp][qry]
[vlan][pkt][fwd][mgmt]|all }
```

Mode Privileged EXEC

`init` - Init and shutdown messages.

`resources` - System resources management messages.

`tmr` - Timer messages.

`src` - Source information messages.

`grp` - Group information messages.

`qry` - Query-related messages.

`vlan` - VLAN information messages.

`pkt` - Packet dump messages.

`fwd` - Forwarding database messages.

`mgmt` - Management-related messages.

`all` - All messages.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# debug igmpsnooping fwd
(JGSM7224)#
--------------------------------------------------------------------------------
```

set igmp max-response

This command sets the maximum response code inserted in general queries sent to a host. The unit of the response code is a tenth of a second. The no form of the command sets the query response code to the default value.

Default	100
Syntax	`set igmp maxresponse <1-4094> <(0 - 255)>` `no set igmp maxresponse <1-4094>`
Mode	VLAN

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(vlan)# set igmp maxresponse 1 10
(JGSM7224)(vlan)#
--------------------------------------------------------------------------------
```

Related Command

`show igmpsnooping vlan-id` - Displays IGMP snooping information for a specific VLAN.

show igmpsnooping mrouter

This command displays the router ports for all VLANs or a specific VLAN.

Syntax	`show igmpsnooping mrouter [Vlan <vlan index>]`
Mode	Privileged EXEC

`Vlan` - VLAN ID value.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show igmpsnooping mrouter
Vlan  Ports
----- ------
1   0/1(dynamic), 0/2(static)
2   0/1(static), 0/2(dynamic)
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Command

`set igmp mrouter` - Statically configures the router ports for a VLAN.

show igmpsnooping

This command displays the IGMP snooping information for all VLANs.

Syntax	`show igmpsnooping`
Mode	Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show igmpsnooping
Snooping Configuration
----------------------------
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
Multicast forwarding mode is MAC based
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Reports are forwarded on router ports
Leave config level is Vlan based
IGMP querier version is 1
IGMP querier address is 1.1.1.1
IGMP querier interval is 125 seconds
Unknown Multicast Filtering disabled
IGMP Router-Alert check enabled
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`set igmp` - Enables IGMP snooping in the switch or a specific VLAN.

`set igmp groupmembership-interval` - Sets the IGMP snooping port purge time interval, after which the port gets deleted if no IGMP reports are received.

show igmpsnooping vlan-id

This command displays IGMP snooping information for a specific VLAN.

Syntax `show igmpsnooping [<vlan id>]`

Mode Privileged EXEC

`vlan` - VLAN ID.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show igmpsnooping 4
Snooping VLAN Configuration for the VLAN 4
  IGMP Snooping enabled
  Fast leave is disabled
  Snooping switch is configured as Non-Querier
  Snooping switch is acting as Non-Querier
  Query interval is 125 seconds
  Port Purge Interval is 260 seconds
  Max Response Time is 10 seconds
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`set igmp` - Enables IGMP snooping in the switch or a specific VLAN.

`set igmp fast-leave` - Enables fast leave processing for a specific VLAN.

`set igmp querier` - Configures the IGMP snooping switch as a querier for a specific VLAN.

`set igmp querier query-interval` - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN.

show mac-address-table igmpsnooping

This command displays the multicast forwarding entries for all VLANs. IGS must be enabled in the switch prior to executing this command.

Syntax `show mac-address-table igmpsnooping`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show mac-address-table igmpsnooping
Vlan MAC-Address       Ports
---- ----------------- -----
   2 01:00:5e:01:01:01   0/2, 0/3, 0/4, 0/5
   2 01:00:5e:02:02:02   0/2, 0/3
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`set igmp` - Enables IGMP snooping in the switch or a specific VLAN.

show igmpsnooping auto-video

This command displays auto video information for auto-video VLAN.

Syntax	`show igmpsnooping auto-video`
Mode	Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show igmpsnooping auto-video
Auto-Video Status : disabled
Auto-Video Vlan : 3
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`set igmp auto-video` - Enables or disables auto-video in the auto-video VLAN.

show igmpsnooping statistics

This command displays IGMP snooping statistics for all VLANs or a specific VLAN.

Syntax	`show igmpsnooping statistics [<vlan-id>]`
Mode	Privileged EXEC

`vlan id` - VLAN index value.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show igmpsnooping statistics 1

Snooping Statistics for VLAN 1
  General queries received : 0
  Group specific queries received : 0
  Group and source specific queries received : 0
  ASM reports received : 0
  Leave messages received : 0
  General queries transmitted : 0
  Group specific queries transmitted : 0
  ASM reports transmitted : 0
  Leaves transmitted : 0
  Packets dropped : 0

(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`set igmp` - Enables IGMP snooping in the switch or a specific VLAN.

Syslog 24

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is simply designed to transport the event messages.

One of the fundamental tenets of the syslog protocol and process is its simplicity. The transmission of syslog messages can be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

logging

This command enables the logging function and configures the log-level and other logging-related parameters. The no form of the command disables the logging function and resets the log-level and other logging-related parameters. The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server.

Defaults

console - enabled
severity - critical
buffered - 50

Syntax

```
logging { buffered <size (1-200)> | console | severity [{ <level (0-7)>  |
alerts | critical | debugging | emergencies | errors | informational  |
notification | warnings }]| on }
no logging { buffered | console | severity | on }
```

Mode Global Configuration

`buffered` - Limits Syslog messages displayed from an internal buffer.

`console` - Limits messages logged to the console.

`severity` - Level of severity.

`alerts` - Immediate action needed.

`critical` - Critical conditions.

`debugging` - Debugging messages.

`emergencies` - System is unusable.

`errors` - Error conditions.

`informational` - Information messages.

`notification` - Normal but significant messages.

`warnings` - Warning conditions.

`on` - Syslog enabled.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# logging buffered 100

(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show logging` - Displays logging status and configuration information.

logging timestamps

This command enables the timestamp option for logged messages. The `no` form of the command disables the timestamp option for logged messages. When enabled, the messages will hold the time stamp information. When disabled, the time stamp information will not be carried with the messages sent to the syslog servers.

Default	Enabled
Syntax	`logging timestamps` `no logging timestamps`
Mode	Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# logging timestamps
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`logging` - Enables Syslog Server and configures the log-level and other Syslog-related parameters.

`show logging` - Displays Logging status and configuration information.

clear logs

This command clears the system syslog buffers.

Syntax	`clear logs`
Mode	Global Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# clear logs
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Commands

`logging` - Enables Syslog Server and configures the log-level and other Syslog related parameters.

`show logging` - Displays Logging status and configuration information.

logging localstorage

This command enables the syslog local storage. The `no` form of command disables the syslog local storage.

Default	Disabled
Syntax	`logging localstorage` `no logging localstorage`
Mode	Global Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# logging localstorage
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Commands

`show logging localstorage` - Displays the syslog local storage.

`logging file` - Adds an entry into file table.

logging filesize

This command configures the logging file size. The value range is 1024 to 102400 bytes. The command controls log1, log2, and log3. It does not control the debug log, a temp file not stored in flash. The debug log is 100 logs maximum, with each log a maximum of 80 bytes.

Default 10240

Syntax `logging filesize <filesize>`

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# logging filesize 2048
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show logging filesize` - Displays the logging file size configurations.

logging file

This command adds an entry to the file table. The no form of the command deletes an entry from the file table. Syslog local storage must be enabled.

Syntax `logging file <string(16)> { log1 | log2 | log3 }`
`no logging file <string(16)> { log1 | log2 | log3 }`

Mode Global Configuration

`string` - Severity of syslog messages: emergency, alert, critical, error, warning, notice, info, or debug.

`log1` - First log file.

`log2` - Second log file.

`log3` - Third log file.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# logging file emergency log1
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`show logging file` - Displays the Syslog file table.

`logging localstorage` - Enables the syslog local storage.

logging host

This command adds an entry in the syslog server table. The no form of the command deletes an entry from the forward table.

Syntax

```
logging host <string(16)> <ipaddress | ipv6address | host-name>
[port <integer(0-65535)>]  [{udp | tcp }]
no logging host <string(16)>  <ipaddress | ipv6address | host-name>
```

Mode Global Configuration

`string` - Severity of syslog messages: emergency, alert, critical, error, warning, notice, info, or debug.

`ipaddress` - Version 4 IP address.

`ipv6address` - Version 6 IP address.

`host-name` - DNS host name.

`port` - Port number.

`udp`, `tcp` - Sets the transport type as either udp or tcp.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# logging host alert 12.0.0.3
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show logging hosts` - Displays the Syslog logging server table.

show logging

This command displays logging status and configuration information.

Syntax

```
show logging
```

Mode Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show logging

System Log Information
----------------------
Logging on         : enabled
Logging console    : enabled
TimeStamp option   : enabled
Severity           : Debugging
Buffered size      : 50 Entries

LogBuffer(1 Entries, 1028 bytes)
<134>Jan 1 00:57:37 1970JGSM7224 CLI User admin logged in

(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`logging` - Enables Syslog Server and configures the log-level and other Syslog-related parameters.

`logging timestamps` - Enables timestamp option for logged messages.

show logging local storage

This command displays the syslog local storage.

Syntax	`show logging localstorage`
Mode	Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show logging localstorage
Syslog Localstorage : Enabled

(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Command

`logging local storage` - Enables the syslog local storage.

show logging file

This command displays the Syslog file table.

Syntax `show logging file`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show logging file

Logging File Table Information
----------------------------
Severity   File-Name
--------   ----------
emergency  log1

alert      log2

(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`logging file` - Adds an entry in the file table.

show logging hosts

This command displays the Syslog logging server table.

Syntax `show logging hosts`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show logging hosts

Syslog Forward Table Information
--------------------------------

Severity    Address-Type    IpAddress   Port   Trans-Type
--------    ------------    ---------   ----   ----------
error       ipv4            192.168.1.1 514    udp

(JGSM7224)#
```

```
-------------------------------------------------------------------------------
```

Related Command

`logging hosts` - Adds an entry in the logging syslog server table.

show logging filesize

This command displays the logging file size.

Syntax	`show logging filesize`
Mode	Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show logging filesize

Logging File Size : 1050 bytes
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`logging filesize` - Configures logging file size.

SSH 25

SSH is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality, and integrity.
- The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with these protocols.

ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the `ip ssh server enable` command.)

Default	Disabled
Syntax	`ip ssh`
Mode	Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip ssh
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`ip ssh server enable` - Enables the IP secure shell server.

`ip ssh protocol` - Set or remove protocol levels (or versions) for SSH.

`show ip ssh` - Displays SSH server information.

ip ssh server enable

This command enables the IP secure shell server. The no form of the command disables the IP secure shell server.

Default Disabled

Syntax
```
ip ssh server enable
no ip ssh server enable
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip ssh server enable
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`ip ssh` - Enables SSH access to the system.

`ip ssh protocol` - Set or remove protocol levels (or versions) for SSH.

`show ip ssh` - Displays SSH server information.

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1(1), SSH2(2), or both SSH 1 and SSh 2(1 and 2) can be set.

Default 1 and 2

Syntax `ip ssh protocol ([1] [2])`

Mode Global Configuration

1 - ssh version 1

2 - ssh version 2

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip ssh protocol 2
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`ip ssh` - Enables SSH access to the system.

`ip ssh server enable` - Enables the IP secure shell server.

`show ip ssh` - Displays SSH server information.

sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5. The `no` form of the command sets the sessions to the default value.

Default 5

Syntax
```
sshcon maxsessions <0-5>
no sshcon maxsessions
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# sshcon maxsessions 2
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`sshcon timeout` - Set the SSH connection session timeout value, in minutes.

`show ip ssh` - Displays SSH server information.

sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160. The `no` form of the command sets the timeout value to the default.

Changing the timeout value for active sessions does not become effective until the session is re-accessed. Any keystroke activates the new timeout duration.

Default 30

Syntax
```
sshcon timeout <1-160>
no sshcon timeout
```

Mode Global Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# sshcon timeout 10
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Commands

`sshcon maxsessions` - Specifies the maximum number of SSH connection sessions that can be established.

`show ip ssh` - Displays SSH server information.

debug ssh

This command sets the given trace levels for SSH. The no form of the command resets the given SSH trace level. Setting all the bits will enable all the trace levels and resetting them will disable all the trace levels.

Default	Disabled
Syntax	`debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])` `no debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])`
Mode	Privileged EXEC

`all` - Initialization and shutdown messages.

`shut` - Shutdown messages.

`mgmt` - Management messages.

`data` - Data path messages.

`ctrl` - Control plane messages.

`dump` - Packet dump messages.

`resource` - Messages related to all resources except buffers.

`buffer` - Buffer messages.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# debug ssh all
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

show ip ssh

This command displays SSH server information.

Syntax `show ip ssh`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show ip ssh

SSH Configuration

Administrative Mode: ........................ Disabled
Protocol Levels: ............................ Versions 1 and 2
SSH Sessions Currently Active: ............... 0
Max SSH Sessions Allowed: .................... 5
SSH Timeout: ................................ 30

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`ip ssh` - Enables SSH access to the system.

`ip ssh server enable` - Enables the IP secure shell server.

`ip ssh protocol` - Set or remove protocol levels (or versions) for SSH.

`sshcon maxsessions` - Specifies the maximum number of SSH connection sessions that can be established.

`sshcon timeout` - Set the SSH connection session timeout value, in minutes.

SSL 26

SSL (Secure Sockets Layer), is a protocol developed for transmitting private documents through the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with `https` instead of `http`.

The SSL Protocol is designed to provide privacy between two communicating applications (a client and a server) and is designed to authenticate the server, and optionally the client. SSL requires a reliable transport protocol (for example, TCP) for data transmission and reception.

The advantage of the SSL Protocol is that it is application protocol independent. A higher level application protocol (for example HTTP, FTP, TELNET, and so on) can layer on top of the SSL Protocol transparently. The SSL Protocol can negotiate an encryption algorithm and session key as well as authenticate a server before the application protocol transmits or receives its first byte of data. All of the application protocol data is transmitted encrypted, ensuring privacy.

ip http secure-server

This command is used to enable the secure socket layer for secure HTTP. The `no` form of the command disables the secure socket layer.

Default Disabled

Syntax
```
ip http secure-server
no ip http secure-server
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip http secure-server
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`ip http secure-port` - Set the SSL port where port can be 1-65535.

`show ip http` - Displays the http settings for the switch.

ip http secure-port

This command is used to set the SSL port, where port can be 1-65535. The `no` form of the command resets the SSL port to the default value.

Default 443

Syntax
```
ip http secure-port <1-65535>
no ip http secure-port
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip http secure-port 1234
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`ip http secure-server` - Enables the secure socket layer for secure HTTP.

`show ip http` - Displays the http settings for the switch.

ip http secure-session timeout

This command configures the timeout for secure HTTP sessions in minutes. When this timeout expires, you are forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch. The `no` form of the command resets the timeout to the default value.

Default 30

Syntax
```
ip http secure-session timeout <1-60>
no ip http secure-session timeout
```

Mode Global Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip http secure-session timeout 10
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip http` - Displays the http settings for the switch.

crypto key generate rsa

This command is used to generate an RSA key pair for SSL.

Default	512 bits
Syntax	`crypto key generate rsa [{512 | 1024}]`
Mode	Global Configuration

`512` - Length of 512 bits.

`1024` - Length of 1024 bits.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# crypto key generate rsa 1024
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`crypto certificate generate` - Generates a self-signed certificate for HTTPS.

`show ssl server-cert` - Displays the SSL server certificate.

crypto certificate generate

This command is used to generate a self-signed certificate for HTTPS. The resulting certificate is generated with a common name equal to the IP address of the device and a duration of 365*2 days. The no form of the command is used to delete the HTTPS certificate file from the device, regardless of whether it is self-signed or downloaded from an outside source.

Syntax	`crypto certificate generate`
Mode	Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# crypto certificate generate
(JGSM7224)(config)#
--------------------------------------------------------------------------------
The certificate file in device is in the format of certificate + rsa
private key (both in PEM format) like:
```

```
-----BEGIN CERTIFICATE-----
**************************
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
**************************
-----END RSA PRIVATE KEY-----
--------------------------------------------------------------------------------
```

Related Commands

`crypto key generate rsa` - Generate an RSA key pair for SSL.

`show ssl server-cert` - Displays the SSL server certificate.

`show ip http` - Displays the http settings for the switch, status, and configuration information.

debug ssl

This command sets the given debug levels for SSL. The no form of the command resets the given SSL debug level. Setting all the bits will enable all the debug levels, and resetting them will disable all the debug levels.

Default	Disabled
Syntax	`debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])` `no debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])`
Mode	Privileged EXEC

`all` - Initialization and shutdown messages.

`shut` - Shutdown messages.

`mgmt` - Management messages.

`data` - Data path messages.

`ctrl` - Control plane messages.

`dump` - Packet dump messages.

`resource` - Messages related to all resources except buffers.

`buffer` - Buffer messages.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# debug ssl all
(JGSM7224)#
--------------------------------------------------------------------------------
```

show ssl server-cert

This command displays the SSL server certificate. The SSL server certificate must have been created.

Syntax `show ssl server-cert`

Mode Privileged EXEC

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show ssl server-cert

Certificate: Data:
    Version: 3 (0x2)
    Serial Number: 63:c4:92:9c:e9:ba:34:4e:f2:0a:e2:df:de:97:4d:e3
    Signature Algorithm: md5WithRSAEncryption
    Issuer: CN=self-signed
    Validity
      Not Before: Jan  1 00:27:00 1970 GMT
      Not After : Jan  1 00:27:00 1972 GMT
    Subject: CN=192.168.0.2
    Subject Public Key Info:
       Public Key Algorithm: rsaEncryption
       RSA Public Key: (1024 bit)
       Modulus (1024 bit):
          00:d4:7e:12:d9:42:15:32:61:14:95:72:e3:1d:97:
          30:81:c0:d6:01:14:b5:4b:4a:a6:00:03:9b:4a:11:
          69:0b:a2:54:71:c7:7f:c4:3e:47:ca:fd:02:f1:a7:
          3f:1e:e2:2f:ce:0f:83:35:c0:dc:19:83:8e:88:6a:
          5e:18:b0:d9:e1:5c:ca:9f:b0:8b:4d:6e:a8:2a:0e:
          c6:cd:e8:21:2b:a9:55:66:11:fe:2f:f3:3b:c8:60:
          bf:97:0f:8d:12:da:17:c1:df:e0:6a:06:04:06:6b:
          22:62:d5:34:f0:13:c6:d0:51:cc:46:d2:2a:7b:21:
          9e:e7:cb:7e:60:b0:b1:9c:d7
          Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
    38:8a:a0:e2:f6:81:61:28:35:bb:79:35:93:99:20:1d:dd:8d:
    f4:30:a1:a9:15:5f:0b:73:13:6d:74:fc:97:92:06:00:a6:80:
    02:5a:c8:4d:de:74:2d:14:ac:be:0d:08:48:66:eb:84:17:f8:
    cc:8a:db:e9:f4:4f:b8:84:8f:f1:4d:8e:d0:86:36:30:14:84:
    6b:84:25:5b:42:24:fe:6a:42:ce:ad:d9:db:20:c6:fa:d3:be:
    04:2a:95:bd:06:bd:cd:33:14:11:47:5e:02:d6:0c:98:2f:f5:
    cc:76:3f:ed:b6:f1:29:e5:49:ed:67:3f:36:20:2b:7a:94:7b:
    7d:09

(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`crypto key generate rsa` - Generate an RSA key pair for SSL.

`crypto certificate generate` - Generates self-signed certificate for HTTPS.

`copy` - Uploads and Downloads the file from the remote.

SNMPv3 27

SNMP (Simple Network Management Protocol) is the most widely-used network management protocol on TCP/IP-based networks. SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User-based Security Model) and VACM (View-based Access Control Model) are the main features added as part of the SNMPv3 specification. USM provides for both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees. Also, SNMPv3 specifies a generic management framework, which is expandable for adding new Management Engines, Security Models, Access Control Models, and so on. With SNMPv3, the SNMP communication is completely safe and secure.

SNMPv3 is a multi-lingual Agent supporting all three versions of SNMP (SNMPv1, SNMPv2c, and SNMPv3) while conforming to the latest specifications.

snmp-server community

This command adds and names a new SNMP community. A community name is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of name can be up to 16 case-sensitive characters. Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default `name` - private/public

Syntax
```
snmp-server community name <name>
no snmp-server community name <name>
```

Mode Global Configuration

`name` - Community name.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server community name switch
-----------------------------------------------------------------------------
```

Related Command

`show snmpcommunity` - Displays the configured SNMP community details

snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients can use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Default `ipaddr` - 0.0.0.0.

Syntax
```
snmp-server community ipaddr <ipaddr> <name>
no snmp-server community ipaddr <ipaddr> <name>
```

Mode Global Configuration

`ipaddr` - client ip address

`name` - community name

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server community ipaddr 192.168.0.1 public
-------------------------------------------------------------------------------
```

Related Command

`show snmpcommunity` - Displays the configured SNMP community details

snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients can use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Default ipmask - 0.0.0.0

Syntax
```
snmp-server community ipmask <ipmask> <name>
no snmp-server community ipmask <ipmask> <name>
```

Mode Global Configuration

`ipmask` - Client ipaddress mask

`name` - Community name

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server community ipmask 255.255.255.0 public
-------------------------------------------------------------------------------
```

Related Command

`show snmpcommunity` - Displays the configured SNMP community details

snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Default	default - ro
Syntax	`snmp-server community ro <name>`
Mode	Global Configuration

`name` - community name

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server community ro switch
-------------------------------------------------------------------------------
```

Related Command

`show snmpcommunity` - Displays the configured SNMP community details

snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Syntax	`snmp-server community rw <name>`
Mode	Global Configuration

`name` - Community name

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server community rw switch
--------------------------------------------------------------------------------
```

Related Command

`show snmpcommunity` - Displays the configured SNMP community details

snmptrap

This command adds an SNMP trap receiver. The maximum length of name is 16 case-sensitive alphanumeric characters. The snmpversion is the version of SNMP. The version parameter options are snmpv1 or snmpv2. The SNMP trap address can be set using both an IPv4 address format as well as an IPv6 global address format.

Default `snmpversion` - snmpv2

Syntax

```
snmptrap name <name> {ipaddr <ipaddr> | ip6addr <ip6addr>}
[snmpversion { snmpv1 | snmpv2 }]
no snmptrap name <name> {ipaddr <ipaddr> | ip6addr <ip6addr>}
```

Mode Global Configuration

`name` - Community name

`ipaddr` - ipv4 address

`ip6addr` - ipv6 address

`snmpversion` - Trap packet version, snmpv1 or snmpv2

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# snmptrap name public 192.168.0.1
--------------------------------------------------------------------------------
```

Related Command

`show snmptrap` - This command displays SNMP trap receivers

snmptrap snmpversion

This command modifies the SNMP version of a trap. The maximum length of name is 16 case- sensitive alphanumeric characters. The snmpversion parameter options are snmpv1 or snmpv2.

Syntax `snmptrap snmpversion name <name> {<ipaddr> | <ip6addr>} {snmpv1 | snmpv2}`

Mode Global Configuration

`name` - Community name

`ipaddr` - ipv4 address

`ip6addr` - ipv6 address

`snmpversion` - Trap packet version: snmpv1 or snmpv2

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# snmptrap snmpversion name public 192.168.0.1 snmpv1
-------------------------------------------------------------------------------
```

Related Command

`show snmptrap` - This command displays SNMP trap receivers

snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

Syntax `snmptrap ipaddr name <name> <oldipaddr> <newipaddr>`

Mode Global Configuration

`name` - Community name

`oldipaddr` - Old ipv4 address

`newipaddr` - New ipv4 address

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# snmptrap ipaddr name public 192.168.0.1 10.0.0.1
-------------------------------------------------------------------------------
```

Related Command

`show snmptrap` - This command displays SNMP trap receivers

snmptrap ip6addr

This command assigns an IPv6 address to a specified community name. The maximum length of the name is 16 case-sensitive alphanumeric characters.

Syntax `snmptrap ipaddr name <name> <oldipaddr> <newipaddr>`

Mode Global Configuration

`name` - Community name

`oldip6addr` - Old ipv6 address

`newip6addr` - New ipv6 address

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# snmptrap ip6addr name public 2020::1 2020::2
--------------------------------------------------------------------------------
```

Related Command

`show snmptrap` - This command displays SNMP trap receivers

snmp-server user

This command configures the SNMP user details. The `no` form of the command removes the SNMP user details. SNMP passwords are localized using the local SNMP engine ID.

Default username - admin/guest.
Authentication Protocol - none.
Privacy Protocol - none.

Syntax `snmp user <username> [auth { md5|sha } <passwd> [priv des <passwd>]]`
`no snmp-server user <username>`

Mode Global Configuration

`username` - snmpv3 user name

`auth` - Authentication Algorithm, which can be Message Digest 5 or Secure Hash Algorithm

`passwd` - Password associated with the Authentication type

`priv des` - Private encryption password

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server user user1
--------------------------------------------------------------------------------
```

Related Command

`show snmpuser` - Displays the configured SNMP users.

snmp-server user accessmode

This command configures the SNMP user access privilege.

Default	access mode - readonly
Syntax	`snmp-server user <username> accessmode {readonly | readwrite}`
Mode	Global Configuration

`username` - snmpv3 user name

`accessmode` - readonly or readwrite access mode

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server user user1 readwrite
--------------------------------------------------------------------------------
```

Related Command

`show snmpuser` - Displays the configured SNMP users.

snmp-server enable traps authentication

This command enables generation of authentication traps for SNMPv1 and SNMPv2c. The no form of the command disables generation of authentication traps for SNMPv1 and SNMPv2c.

Default	Disabled
Syntax	`snmp-server enable traps authentication` `no snmp-server enable traps authentication`
Mode	Global Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server enable traps authentication
--------------------------------------------------------------------------------
```

Related Command

`show trapflag` - Displays trap conditions.

snmp-server enable traps

This command enables generation of a particular trap. The no form of the command disables generation of a particular trap.

Syntax `snmp-server enable traps { coldstart | warmstart | stpmode | linkmode }`
`no snmp-server enable traps { coldstart | warmstart | stpmode | linkmode }`

Mode Global Configuration

`coldstart` - Coldstart trap

`warmstart` - Warmstart trap

`stpmode` - stp trap

`linkmode` - link up/down trap

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# snmp-server enable traps coldstart
-------------------------------------------------------------------------------
```

Related Command

`show trapflag` - Displays trap conditions.

show snmpcommunity

This command displays SNMP community information. Ten communities are supported. You can add, change, or delete communities.

Syntax `show snmpcommunity`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show snmpcommunity
SNMP Community Name Client IP Address Client IP Mask    Access Mode
------------------- ----------------- ----------------- -----------
public              0.0.0.0           0.0.0.0           Read Only
private             0.0.0.0           0.0.0.0           Read/Write
```

Related Commands

`snmp-server community name` - Configures the SNMP community details

`snmp-server community ipaddr` - Configures the SNMP community client ipaddress

`snmp-server community ipmask` - Configures the SNMP community client ipaddress mask

`snmp-server community ro/rw` - Configures the SNMP community access mode

show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Ten trap receivers are simultaneously supported.

Syntax `show snmptrap`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show snmptrap
   SNMP Trap Name      IP Address       IPv6 Address     SNMP Version
------------------- -------------- -------------------- -------------
public              192.168.0.1                         v2c
--------------------------------------------------------------------------------
```

Related Command

`snmptrap name` - This command adds an SNMP trap receiver

show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers.

Syntax `show trapflags`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show trapflags

Link Up/Down Flag.............................. Enable
Cold Start Flag................................ Enable
Warm Start Flag................................ Enable
Authentication Flag............................ Enable
Spanning Tree Flag............................. Disable
-------------------------------------------------------------------------------
```

Related Commands

`snmp-server enable traps authentication` - Enables generation of authentication traps for SNMPv1 and SNMPv2c

`snmp-server enable traps` - Enables generation of a particular trap

show snmpuser

This command displays the configured SNMP users.

Syntax	`show snmpuser`
Mode	Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show snmpuser
User Name       Access Mode Authentication Encryption
--------------- ----------- -------------- ----------
admin           Read/Write      None           None
guest           Read Only       None           None
-------------------------------------------------------------------------------
```

Related Commands

`snmp-server user` - Configures the SNMP user details

`snmp-server user accessmode` - Configures the SNMP user access mode

RMON 28

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

set rmon

This command is used to enable or disable the RMON feature. All the other RMON Module commands can be executed only when the RMON module is enabled. Fatal error messages are displayed when commands are executed without enabling the RMON feature.

Default	Disabled
Syntax	`set rmon { enable|disable }`
Mode	Global Configuration

`enable` - Enables the RMON feature in the system.

`disable` - Disables the RMON feature in the system

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# set rmon enable
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show rmon` - Successful execution of this command without any messages indicates that RMON feature is enabled in the system.

rmon collection history

This command enables history collection of interface statistics in the buckets for the specified time interval. The no form of the command disables the history collection on the interface. The RMON feature must be enabled for the successful execution of this command. The polling cycle is the bucket interval where the interface statistics details are stored.

Default `bucket number` - 50.
`interval` - 1800 seconds

Syntax
```
rmon collection history <index (1-65535)> [buckets <bucket-number
(1-65535)>] [interval <seconds (1-3600)>] [owner <ownername
(127)>]
no rmon collection history <index (1-65535)>
```

Mode Interface Configuration

`index` - History table index.

`buckets` - The maximum number of buckets desired for the RMON collection history group of statistics.

`interval` - The number of seconds in each polling cycle.

`owner` - Optional field - allows the user to enter the name of the owner of the RMON group of statistics.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# rmon collection history 1 buckets 2 interval 20
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show rmon` - Displays the history collection for the configured bucket (`show rmon history [history-index (1-65535)>]`)

rmon collection stats

This command enables RMON statistic collection on the interface. The no form of the command disables RMON statistic collection on the interface. The RMON feature must be enabled for the successful execution of this command.

Syntax
```
rmon collection stats <index (1-65535)> [owner <ownername (127)>]
no rmon collection stats <index (1-65535)>
```

Mode Interface Configuration

`index` - Statistics table index.

owner - Optional field - allows the user to enter the name of the owner of the RMON group of statistics with a string length of 127.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# rmon collection stats 1
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

show rmon - Displays the RMON collection statistics (show rmon statistics [<stats-index (1-65535)>])

rmon event

This command adds an event to the RMON event table. The added event is associated with an RMON event number. The no form of the command deletes an event from the RMON event table. The RMON feature must be enabled for the successful execution of this command.

Syntax

```
rmon event (1-65535)> [description <event-description (127)>]
[log] [owner <ownername (127)>] [trap <community (127)>]
no rmon event <number (1-65535)>
```

Mode Global Configuration

number - Event number.

description - Description of the event.

log - Used to generate a log entry.

owner - Owner of the event.

trap - Used to generate a trap. The SNMP community string is to be passed for the specified trap.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# rmon event 1 log owner netgear trap public
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

rmon alarm - Sets an alarm on a MIB object.

show rmon - Displays the RMON events (show rmon events).

show snmptrap - Displays trap conditions.

rmon alarm

This command sets an alarm on a MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured. The no form of the command deletes the alarm configured on the MIB object.

The RMON Feature must be enabled for the successful execution of this command. RMON events must have been configured. The JGSM7224 cannot monitor all the mib objects through RMON. This will be applicable only to the Ethernet interfaces.

Syntax

```
rmon alarm <alarm-number (1-65535) > <mib-object-id (255)>
<sample-intervaltime
(1-65535)> { absolute|delta } rising-threshold <value (0-2147483647)>
<rising-event-number (1-65535)> falling-threshold <value (0-2147483647)>
<falling-event-number (1-65535)> [owner <ownername (127)>]
no rmon alarm <number (1-65535)>
```

Mode Global Configuration

`alarm-number` - Alarm number.

`mib-object-id` - The MIB object identifier.

`sample-intervaltime` - Time in seconds during which the alarm monitors the MIB variable.

`absolute` - Used to test each mib variable directly delta Used to test the change between samples of a variable.

`rising-threshold` - A rising threshold value at which the alarm is triggered

`falling-threshold` - A falling threshold value at which the alarm is triggered

`value` - A number at which the alarm is reset.

`rising-eventnumber` - The event number to trigger when the rising threshold exceeds its limit.

`falling-eventnumber` - The event number to trigger when the falling threshold exceeds its limit.

`owner` - Owner of the alarm.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.11.1 20 absolute
rising-threshold 15 2 falling-threshold 14 2
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Commands

`rmon collection stats` - Enables RMON statistic collection on the interface.

`rmon event` - Adds an event to the RMON event table.

`show rmon` - Displays the RMON alarms (show rmon alarms).

show rmon

This command displays the RMON statistics, alarms, events, and history configured on the interface.

Syntax `show rmon [alarms] [events] [history history-index (1-65535)] [overview]] [statistics [<stats-index (1-65535)>]]`

Mode Privileged EXEC

`statistics` - The configured stats index value.

`alarms` - The configured alarm.

`events` - The configured event.

`history` - The configured history index.

`overview` - Displays only the overview of rmon history entries.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show rmon statistics 2
RMON is enabled
Collection 2 on 0/2 is active, and owned by fsoft,
Monitors ifEntry.1.2 which has
Received 1240 octets, 10 packets,
2 broadcast and 10 multicast packets,
0 undersized and 1 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 10, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
(JGSM7224)# show rmon
RMON is enabled
(JGSM7224)#
--------------------------------------------------------------------------------
(JGSM7224)# show rmon history
RMON is enabled
Entry 1 is active, and owned by fsoft
Monitors ifEntry.1.1 every 3000 second(s)
Requested # of time intervals, ie buckets, is 3,
Granted # of time intervals, ie buckets, is 3,
Sample 1 began measuring at 0
Received 0 octets, 0 packets,
```

```
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,


# of dropped packet events is 0
Network utilization is estimated at 0
Sample 2 began measuring at 0
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events is 0
Network utilization is estimated at 0
(JGSM7224)#
--------------------------------------------------------------------------------
(JGSM7224)# show rmon events
RMON is enabled
Event 1 is active, owned by
Description is end
Event firing causes nothing,
Time last sent is 0 seconds
Event 2 is active, owned by fsoft
Description is trapcheck
Event firing causes log and trap to community 5,
Time last sent is 3 seconds
(JGSM7224)#
--------------------------------------------------------------------------------
(JGSM7224)# show rmon alarms
RMON is enabled
Alarm 1 is active, owned by
Monitors 1.3.6.1.2.1.2.2.1.11.1 every 65 second(s)
Taking absolute samples, last value was 35
Rising threshold is 15, assigned to event 1
Falling threshold is 14, assigned to event 2
On startup enable rising or falling alarm
(JGSM7224)#
--------------------------------------------------------------------------------
(JGSM7224)# show rmon alarms events history 2 overview statistics 2
RMON is enabled
Collection 2 on 0/2 is active, and owned by fsoft,
Monitors ifEntry.1.2 which has
Received 4712 octets, 38 packets,
0 broadcast and 38 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
```

```
0 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 38, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm 1 is active, owned by
Monitors 1.3.6.1.2.1.2.2.1.11.1 every 65 second(s)
Taking absolute samples, last value was 37
Rising threshold is 15, assigned to event 1
Falling threshold is 14, assigned to event 2
On startup enable rising or falling alarm
Event 1 is active, owned by
Description is end
Event firing causes nothing,
Time last sent is 1708335 seconds
Event 2 is active, owned by fsoft
Description is trapcheck
Event firing causes log and trap to community 5,
Time last sent is 0 seconds
Entry 2 is active, and owned by fsoft
Monitors ifEntry.1.2 every 2000 second(s)
Requested # of time intervals, ie buckets, is 5,
(JGSM7224)#
--------------------------------------------------------------------------------
(JGSM7224)# show rmon history overview
RMON is enabled
Entry 1 is active, and owned by fsoft
Monitors ifEntry.1.1 every 3000 second(s)


Requested # of time intervals, ie buckets, is 3, Granted # of time intervals, ie
buckets, is 3
--------------------------------------------------------------------------------
```

If the show rmon command is executed without enabling the RMON feature, then the following output is displayed.

```
--------------------------------------------------------------------------------
(JGSM7224)# show rmon
RMON is disabled
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`set rmon` - Enables or disables the RMON feature.

`rmon collection history` - Enables history collection of interface statistics in the buckets for the specified time interval.

`rmon collection stats` - Enables RMON statistic collection on the interface.

`rmon event` - Adds an event to the RMON event table.

`rmon alarm` - Sets an alarm on a MIB object.

IPV4 29

IP (Internet Protocol) is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example:10.5.25.180.

Every computer that communicates over the Internet is assigned an IP address that uniquely identifies the device and distinguishes it from other computers on the Internet. Within an isolated network, IP addresses can be assigned at random as long as each one is unique. However, to connect a private network to the Internet, the registered IP addresses must be used (called Internet addresses) to avoid duplicates. The four numbers in an IP address are used in different ways to identify a particular network and a host on that network.

ip address

This command configures the IPv4 address of the interface. The no form of the command deletes the configured IPv4 address.

Syntax

```
ip address <ucast_addr> <ip_mask>
no ip address
```

Mode Interface Configuration

`ucast addr` - IPv4 prefix for the interface.

`ip mask` - IPv4 prefix mask.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# ip address 1.1.1.1 255.255.255.0
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show management vlan` - Displays the IPv4 interfaces.

ip gateway

This command configures the IPv4 default gateway on the interface. The no form of the command deletes the configured IPv4 default gateway.

Syntax `ip gateway <ucast_addr>`
`no ip gateway`

Mode Interface Configuration

`ucast addr` - IPv4 address for the gateway.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# ip gateway 1.1.1.1
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show management vlan` - Displays the IPv4 interfaces.

ip address {dhcp | bootp}

This command enables an IPv4 DHCP client or bootp client on the interface.

Syntax `ip address {dhcp | bootp}`

Mode Interface Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# ip address dhcp
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Commands

`show management vlan` - Displays the IPv4 interfaces.

`no ip address` - Delete the IP address.

ping

This command sends IPv4 echo messages.

Default	size - 100 bytes. count - 1. interval - 1 second.
Syntax	`ping <ipaddress | hostname> [size <value>] [count <value> ] [interval <value>]`
Mode	Privileged EXEC

`ipaddress | hostname` - IPv4 destination prefix or hostname.

`size` - Size of the ping message.

`count` - Number of the ping message.

`interval` - Timeout of the ping message.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# ping 1.1.1.4
(JGSM7224)#
--------------------------------------------------------------------------------
```

traceroute

This command traces the path to the IPv4 host.

Default	max hop - 30
Syntax	`traceroute <ipaddress | hostname>`
Mode	Privileged EXEC

`ipaddress | hostname` - Host IPv4 address or hostname

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# traceroute 1.1.1.1
(JGSM7224)#
--------------------------------------------------------------------------------
```

show ip arp

This command displays the IPv4 ARP Cache Entries.

Syntax `show ip arp`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip arp

Address         Hardware Address   Type   Interface   Mapping
-------         ----------------   ----   ---------   -------
192.168.1.108   00:0a:eb:56:dc:07  ARPA   vlanMgmt    Dynamic

(JGSM7224)#
-------------------------------------------------------------------------------
```

show ip information

This command displays the IPv4 stack attribution.

Syntax `show ip information`

Mode Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip information

Global IP Configuration:
------------------------
Default TTL is 64
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP echo replies are always sent
ICMP mask replies are always sent

(JGSM7224)#
-------------------------------------------------------------------------------
```

IPV6 30

IPv6 is a new version of IP which is designed to be an evolutionary step up from IPv4. It can be installed as a normal software upgrade in Internet devices and is interoperable with the current IPv4. It has expanded routing and addressing capabilities because of its 128-bit addressing, compared to the 32-bit addressing in IPv4. Its deployment strategy is designed not to have any flag days or other dependencies. IPv6 is designed to run well on high performance networks (for example, Gigabit Ethernet, OC-12, ATM, and so on) and at the same time still be efficient for low bandwidth networks (for example, wireless). In addition, it provides a platform for new Internet functionality that will be required in the near future. IPv6 includes a transition mechanism, which is designed to allow users to adopt and deploy IPv6 in a highly diffuse fashion and to provide direct interoperability between IPv4 and IPv6 hosts. The IPv6 transition allows the users to upgrade their hosts to IPv6, and the network operators to deploy IPv6 in routers, with very little coordination between the two. The differences between IPv4 and IPv6 fall primarily into the following commands.

ipv6 enable

This command enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address. The no form of the command disables IPv6 processing on the interface that has not been configured with an explicit IPv6 address.

Default	Enabled
Syntax	`ipv6 enable` `no ipv6 enable`
Mode	Interface Configuration

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# ipv6 enable
(JGSM7224)(config-if)#
-----------------------------------------------------------------------------
```

Related Commands

`ipv6 address` - Configures IPv6 address on the interface.

`show ipv6 interface` - Displays the IPv6 interfaces.

ipv6 address

This command configures IPv6 address on the interface. The `no` form of the command deletes the configured IPv6 address. The prefix length for `eui64` type must be 64.

Default Unicast

Syntax
```
ipv6 address <prefix> <prefix Len> [unicast | eui64]
no ipv6 address <prefix> <prefix Len> [unicast |eui64]
```

Mode Interface Configuration

`prefix` - IPv6 prefix for the interface.

`prefix Len` - IPv6 prefix length.

`unicast` - Unicast type of Prefix.

`eui64` - Type of Prefix where the latter 64-bits are formed from the link layer address.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# ipv6 address 3333::1111 64 unicast
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show management vlan` - Displays the IPv6 interfaces.

ipv6 gateway

This command configures the IPv6 gateway on the interface. The `no` form of the command deletes the configured IPv6 gateway.

Syntax
```
ipv6 gateway <prefix>
no ipv6 gateway <prefix>
```

Mode Interface Configuration

`prefix` - IPv6 prefix for the gateway.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# ipv6 gateway 2001::1
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show management vlan` - Displays the IPv6 interfaces.

ping ipv6

This command sends IPv6 echo messages.

Default	size - 100 bytes
Syntax	`ping ipv6 <ipv6-address | hostname> [size <value>]`
Mode	Privileged EXEC

`prefix` - IPv6 Destination Prefix.

`size` - Size of the ping message.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# ping ipv6 3333::1111
(JGSM7224)#
--------------------------------------------------------------------------------
```

traceroute ipv6

This command traces the path to the host.

Default	max hop - 30
Syntax	`traceroute ipv6 <ipv6-address | hostname>`
Mode	Privileged EXEC

`ipv6-address hostname` - Host IPv6 destination address or hostname.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# traceroute ipv6 3333::1111
(JGSM7224)#
--------------------------------------------------------------------------------
```

debug ipv6

This command enables IPv6 Trace. The no form of the command disables IPv6 Trace.

Default	Disabled
Syntax	`debug ipv6 IP6|ICMP|UDP6|ND|PING6` `no debug ipv6`
Mode	Privileged EXEC

`IP6` - IP6 Trace.

`ICMP` - ICMP Trace.

`UDP6` - UDP6 Trace.

`ND` - Neighbor Discovery Trace.

`PING6` - PING6 Trace.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# debug ipv6 IP6
(JGSM7224)#
--------------------------------------------------------------------------------
```

clear ipv6 neighbors

This command removes all the entries in the IPv6 neighbor table.

Default	Disabled
Syntax	`clear ipv6 neighbors`
Mode	Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# clear ipv6 neighbors
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`show ipv6 neighbors` - Displays the IPv6 Neighbor Cache Entries.

show ipv6 neighbors

This command displays the IPv6 Neighbor Cache Entries.

Syntax `show ipv6 neighbors`

Mode Privileged EXEC

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show ipv6 neighbors

IPv6 Address   Age    LinkLayer Addr State     Intf
5555::1111     58     0011.2233.4455 Static    vlanMgmt
5556::1111     58     1122.3344.5566 Static    vlanMgmt

(JGSM7224)#
--------------------------------------------------------------------------------
```

31 Port Protected

This chapter describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default. If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected

This command enables the port protected feature. The no form disables the port protected feature.

Note that the interface 0/1 will not be shown. If you configured a port protected, add this port to a port-channel, and then enable the port-channel protocol, this port will be removed from the VLAN port table, and the protected configuration will be cleared on the port.

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports. You can't set the port protected, which is already in a isolated group (private group).

Syntax

```
switchport protected
no switchport protected
```

Mode Interface Configuration

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# interface 0/1
(JGSM7224)(config-if)# switchport protected
(JGSM7224)(config-if)# exit
(JGSM7224)(config)# interface 0/2
(JGSM7224)(config-if)# switchport protected
(JGSM7224)(config-if)# end
(JGSM7224)# show vlan port all

          Port       Port     Ingress
          VLAN ID    VLAN ID  Acceptable  Filtering Default  Protected
Interface Configured Current  Frame Types Current   Priority Port
--------- ---------- -------- ----------- --------- -------- ---------
0/1        1           1        Admit All   Disable    0      Enable
0/2        1           1        Admit All   Disable    0      Enable
0/3        1           1        Admit All   Disable    0      Disable
...

0/24       1           1        Admit All   Disable    0      Disable

(JGSM7224)(config)# interface port-channel 1
(JGSM7224)(config-if)# exit
(JGSM7224)(config)# interface 0/1
(JGSM7224)(config-if)# addport 1 mode active
(JGSM7224)(config-if)# exit
(JGSM7224)(config)# set port-channel enable
(JGSM7224)(config)# exit
(JGSM7224)(config)# show vlan port all

          Port       Port                   Ingress
          VLAN ID    VLAN ID   Acceptable   Filtering Default  Protected
Interface Configured Current   Frame Types  Current   Priority  Port
--------- ---------- -------- -----------  --------- --------  ---------
0/2        1           1        Admit All   Disable    0        Enable
0/3        1           1        Admit All   Disable    0        Disable
...
0/24       1           1        Admit All   Disable    0        Disable
--------------------------------------------------------------------------------
```

Green Feature 32

This feature enables the switch to perform the dynamic power management on the phyport. It supports two modes: Auto power down and short cable.

Auto Power Down Mode - This mode sets whether or not the auto power down mode green feature is enabled for a particular port. The default is enabled. When the port link is down, the PHY automatically goes down for a short period of time, and then wakes up to check link pulses. This allows auto-negotiation and saves power consumption when no link partner is present.

Short Cable Mode - This mode sets whether or not the short cable mode green feature is enabled for a particular port. The factory default is disabled. When the port link is up at 1Gbps speed, a cable length test is performed and if the length of the cable is less then 10m, PHYs are put into low power mode so only enough power is used to support a short cable.

set green-feature auto-power-down

This command enables or disables the auto power down mode globally in the system. The default mode is enabled. When you disable the auto power down using this command, it will disable this feature in the whole system, even though the status on the port is set to enabled.

Syntax `set green-feature auto-power-down {disable | enable}`

Mode Global Configuration

Example

```
!enable the feature globally
-------------------------------------------------------------------------------
(JGSM7224)(config)# set green-feature auto-power-down enable
-------------------------------------------------------------------------------
!disable the feature globally
-------------------------------------------------------------------------------
(JGSM7224)(config)# set green-feature auto-power-down disable
-------------------------------------------------------------------------------
```

set port green-feature auto-power-down

This command enables or disables the auto power down mode per port. The default mode is enabled. If you want to enable this feature on a port, also enable the system feature using the command `set green-feature auto-power-down`.

Syntax `set port green-feature auto-power-down <slot/port> { enable | disable }`

Mode Global Configuration

Example

```
!enable the feature per port
-------------------------------------------------------------------------------
(JGSM7224)(config)# set port green-feature auto-power-down 0/1 enable
-------------------------------------------------------------------------------
!disable the feature per port
-------------------------------------------------------------------------------
(JGSM7224)(config)# set port green-feature auto-power-down 0/1 disable
-------------------------------------------------------------------------------
```

set green-feature short-cable

This command enables or disables the short cable mode globally. The default mode is disabled. If you disable the short cable using this command, it will disable this feature in the whole system, even though the status on the port is set to enabled. Because the short-cable feature will detect the cable status of the port linked up with 1G speed if it has also been enabled on the port, and the detection of one port will take a time of about 2 seconds, the command will take a long time if the there are many ports linked up with 1G speed.

Syntax `set green-feature short-cable { enable | disable }`

Mode Global Configuration

Example

```
!enable the feature globally
-------------------------------------------------------------------------------
(JGSM7224)(config)# set green-feature short-cable enable
-------------------------------------------------------------------------------
!disable the feature globally
-------------------------------------------------------------------------------
(JGSM7224)(config)# set green-feature short-cable disable
-------------------------------------------------------------------------------
```

set port green-feature short-cable

This command sets the short cable mode to enabled or disabled per port. The default mode is disabled. If you want to enable this feature on a port, also be sure to enable the system feature using the command `set green-feature short-cable`.

Default	Disabled
Syntax	`set port green-feature short-cable <slot/port> { enable | disable }`
Mode	Global Configuration

Example

```
!enable the feature per port
-------------------------------------------------------------------------------
(JGSM7224)(config)# set port green-feature short-cable 0/1 enable
-------------------------------------------------------------------------------
!disable the feature per port
-------------------------------------------------------------------------------
(JGSM7224)(config)# set port green-feature short-cable 0/1 disable
-------------------------------------------------------------------------------
```

show green feature

This command displays the green feature status of the global and individual port.

Syntax	`show green-feature [{all | interface <slot/port>}]`
Mode	Privileged EXEC

Example

```
!show the global setting of the green-feature
-------------------------------------------------------------------------------
(JGSM7224)# show green-feature

Green Feature device configurations

Auto Power Down Status          Enabled
Short Cable Status              Disabled
-------------------------------------------------------------------------------
!show the green feature status on the port
(JGSM7224)# show green-feature all

Green Feature Port Configuration Table
---------------------------------------
Port 0/1
Port Auto Power Down            Enabled
```

```
Port Short Cable                Disabled
----------------------------------------
Port 0/2
Port Auto Power Down            Enabled
Port Short Cable                Disabled
----------------------------------------
Port 0/24
Port Auto Power Down            Enabled
Port Short Cable                Disabled
--------------------------------------------------------------------------------
```

IP-ARP-INSPECTION 33

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address. DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid MAC address, IP address, VLAN, and interface tuples. When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

ip arp inspection vlan

Use this command to enable or disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default Disabled

Format
```
ip arp inspection vlan <vlan-list>
no ip arp inspection vlan <vlan-list>
```

Mode Global Configuration Mode

`<vlan list>` - Contains VLAN ID's in range 1-4094. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

Example

```
------------------------------------------------------------------------------
! To enable ARP inspection on VLAN 1-3.
(JGSM7224)(config)# ip arp inspection vlan 1-3
(JGSM7224)(config)#
------------------------------------------------------------------------------
!To disable ARP inspection on VLAN 3.
(JGSM7224)(config)# no ip arp inspection vlan 3
(JGSM7224)(config)#
------------------------------------------------------------------------------
```

Related Command

`show ip arp inspection` - Displays IP ARP inspection VLAN information.

ip arp inspection validate

Use this command to enable or disable additional validation checks like source-mac validation, destination- mac validation, and ip address validation on the received ARP packets.

Default Disabled

Format
```
ip arp inspection validate {[src-mac] [dst-mac] [ip]}
no ip arp inspection validate {[src-mac] [dst-mac] [ip]}
```

Mode Global Configuration Mode

`src-mac` - Check the source MAC address in the Ethernet header against the sender MAC address in the ARP body.

`dst-mac` - Check the destination MAC address in the Ethernet header against the target MAC address in ARP body.

`ip` - Check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip arp inspection validate ip
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip arp inspection` - Displays ip arp inspection vlan information

ip arp inspection vlan logging

Use this command to enable or disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format
```
ip arp inspection vlan <vlan-list> logging
no ip arp inspection vlan <vlan-list> logging
```

Mode Global Configuration Mode

`<vlan list>` - Contains VlanIds in the range 1-4094. Separate non-consecutive IDs with ',' and use no spaces and no zeros in the range. Use '-' for the range.

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# ip arp inspection vlan 1 logging
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

Related Commands

`show ip arp inspection` - Displays ip arp inspection vlan information

`show running-config` - Displays the current operating configuration in the system

ip arp inspection trust

Use this command to configure an interface as trusted or untrusted for Dynamic ARP Inspection.

Default	Untrusted
Format	`ip arp inspection trust` `no ip arp inspection trust`
Mode	Interface Configuration Mode

Example

```
-----------------------------------------------------------------------------
!To configure interface 20 as a trusted interface.
(JGSM7224)(config)# interface 0/20
(JGSM7224)(config-if)# ip arp inspection trust
(JGSM7224)(config-if)#
! To configure interface 2 as an untrusted interface
(JGSM7224)(config)# interface 0/2
(JGSM7224)(config-if)# no ip arp inspection trust
(JGSM7224)(config-if)#
-----------------------------------------------------------------------------
```

Related Command

`show ip arp inspection interfaces` - Displays ip arp inspection interface information.

ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface. Configuring none for the limit means the interface is not rate-limited for Dynamic ARP Inspections. Use the no form of the command to set the rate limit and burst interval for an interface to the default values of 15 pps and 1 second, respectively.

Default 15 pps for rate and 1 second for burst-interval

Format `ip arp inspection limit {rate <0-100> [burst interval <1-15>] | none}`

`no ip arp inspection limit`

Mode Interface Configuration Mode

`<0-100>` - The range for the rate limit

`<1-15>` - The range for the burst interval

Note: The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# ip arp inspection limit none
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show ip arp inspection interfaces` - Displays ip arp inspection interface information

ip arp inspection filter

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. Use the no form of the command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format `ip arp inspection filter <string> vlan <vlan-list> [static]`

`no ip arp inspection filter <string> vlan <vlan-list> [static]`

Mode Global Configuration Mode

`<string>` - An alphanumeric string of up to 31 characters

`<vlan list>` - Contains VLAN IDs in the range 1-4094. Separate non-consecutive IDs with ',' with no spaces and no zeros between the range; Use '-' for range.

`static` - Use only ARP ACL, not DHCP snooping bindings

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip arp inspection filter aa vlan 1 static
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip arp inspection` - Displays ip arp inspection vlan information

arp access-list

Use this command to create or delete an ARP ACL.

Format	`arp access-list <string>` `no arp access-list <string>`
Mode	Global Configuration Mode

`<string>` - An alphanumeric string of up to 31 characters

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# arp access-list aa
(JGSM7224)(config-arp-access-list)#
-------------------------------------------------------------------------------
```

Related Command

`show arp access-list` - Displays ARP Access list configuration

permit ip host mac host

Use this command to configure or delete a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format	`permit ip host <sender-ip> mac host <sender-mac>` `no permit ip host <sender-ip> mac host <sender-mac>`
Mode	ARP Access-list Configuration Mode

<sender-ip> - IP Address in the ARP ACL rule

<sender-mac> - MAC Address in the ARP ACL rule

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-arp-access-list)# permit ip host 192.168.0.2 mac host
00:01:02:03:04:05
(JGSM7224)(config-arp-access-list)#
-------------------------------------------------------------------------------
```

Related Command

`show arp access-list` - Displays ARP Access list configuration

show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the vlan-list argument (that is, comma-separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the source mac validation, destination mac validation, and invalid IP validation information.

Format `show ip arp inspection [vlan <vlan-list>]`

Mode Privileged EXEC Mode

<vlan list> - Contains VLAN IDs in the range 1-4094. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range. Use '-' for the range.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip arp inspection
Source Mac Validation.................Disabled
Destination Mac Validation............Disabled
IP Address Validation.................Disabled
VLAN Configuration Log Invalid        ACL Name        Static Flag
1        Enabled         Enabled        aa            Enabled
2        Disabled        Enabled                      Disabled
3        Disabled        Enabled                      Disabled
(JGSM7224)#
(JGSM7224)# show ip arp inspection vlan 1
Source Mac Validation.................Disabled
Destination Mac Validation............Disabled
IP Address Validation.................Disabled
```

```
VLAN Configuration Log Invalid        ACL Name        Static Flag
1        Enabled        Enabled        aa              Enabled
------------------------------------------------------------------------------
```

Related Commands

`ip arp inspection vlan` - Enable or disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

`ip arp inspection validate` - Enable or disable additional validation checks like source-mac validation, destination- mac validation, and ip address validation on the received ARP packets.

`ip arp inspection vlan logging` - Enable or disable logging of invalid ARP packets on a list of comma- separated VLAN ranges.

`ip arp inspection filter` - Configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

show ip arp inspection statistics

Use this command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAIenabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format `show ip arp inspection statistics [vlan <vlan-list>]`

Mode Privileged EXEC Mode

`<vlan list>` - Contains VLAN IDs in range 1-4094. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range. Use '-' for the range.

Example

```
------------------------------------------------------------------------------
(JGSM7224)# show ip arp inspection statistics
VLAN        Forwarded      Dropped
----
1           9              6
2           0              0
3           0              0

(JGSM7224)#
------------------------------------------------------------------------------
```

Related Command

`clear ip arp inspection statistics` - Reset the statistics for Dynamic ARP Inspection on all VLANs

clear ip arp inspection statistics

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Format `clear ip arp inspection statistics`

Mode Privileged EXEC Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# clear ip arp inspection statistics
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`show ip arp inspection statistics` - Display the statistics of the ARP packets processed by Dynamic ARP Inspection

show ip arp inspection interfaces

Use this command to display the Dynamic ARP Inspection configuration on all interfaces.

Format `show ip arp inspection interfaces [{<slot/port> | port-channel <integer (1-8)>}]`

Mode Privileged EXEC Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip arp inspection interfaces
Interface    Trust State   Rate Limit   Burst Interval
                                (pps)        (seconds)
0/1                  No          15            1
0/2                  No          15            1
0/3                  No          15            1
0/4                  No          15            1
0/5                  No          15            1
0/6                  No          15            1
0/7                  No          15            1
```

```
0/8                    No          15            1
0/9                    No          15            1
0/10                   No          15            1
0/11                   No          15            1
0/12                   No          15            1
0/13                   No          15            1
0/14                   No          15            1
0/15                   No          15            1
0/16                   No          15            1
0/17                   No          15            1
0/18                   No          15            1
0/19                   No          15            1
0/20                   No          15            1
0/21                   No          15            1
0/22                   No          15            1
0/23                   No          15            1
0/24                   No          15            1
po1                    No          15            1
po2                    No          15            1
po3                    No          15            1
po4                    No          15            1
po5                    No          15            1
po6                    No          15            1
po7                    No          15            1
po8                    No          15            1
(JGSM7224)#
(JGSM7224)# show ip arp inspection interfaces 0/10
Interface    Trust State   Rate Limit   Burst Interval
                                (pps)        (seconds)
0/10                   No          15            1
(JGSM7224)#
```

Related Commands

`ip arp inspection trust` - Configure an interface as trusted or untrusted for Dynamic ARP Inspection

`ip arp inspection limit` - Configure the rate limit and burst interval values for an interface

show arp access-list

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format `show arp access-list [acl-name]`

Mode Privileged EXEC Mode

`acl-name` - ARP access list name

Example

```
--------------------------------------------------------------------------
(JGSM7224)# show arp access-list
arp access-list H1
permit ip host  192.168.0.1 mac host 00:01:02:03:04:01
arp access-list H2
permit ip host  192.168.0.2 mac host 00:01:02:03:04:02
arp access-list H3
permit ip host  192.168.0.3 mac host 00:01:02:03:03:03
(JGSM7224)#
(JGSM7224)# show arp access-list H2
arp access-list H2
permit ip host  192.168.0.2 mac host 00:01:02:03:04:02
(JGSM7224)#
--------------------------------------------------------------------------
```

Related Command

`arp access-list` - Create/delete an ARP ACL

`permit ip host mac host` - Configure or delete a rule for a valid IP address and MAC address combination used in ARP packet validation

debug dai

This command specifies the debug levels for DAI module and the no form of the command resets debug options for DAI module.

Default Disabled

Format `debug dai {all |[buffer] [ctpl] [data] [dump] [failall] [initshut] [mgmt] [os]}`
`no debug dai {all |[buffer] [ctpl] [data] [dump] [failall] [initshut] [mgmt] [os]}`

Mode Privileged EXEC Mode

`all` - All Messages

`buffer` - Buffer Information Messages

`ctrl` - Control Related Messages

`data` - Data Packets Messages

`dump` - Dumping ARP frame Messages

`failall` - All failures Messages

`initshut` - Init and Shutdown Messages

`mgmt` - Management Related Messages

`os` - Traces related to all resources except buffer

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# debug dai all
(JGSM7224)#
--------------------------------------------------------------------------------
```

ACL 34

access-list

This command is used to create an IP Standard or Extended ACL List identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs.

Format

```
access-list <access-list-number(1-99)> {deny | permit}
{every | <src-ip-address> <ip_mask>} [ assign-queue <queue-number(0-3)> ] [{ mirror
| redirect } <slot/port> | port-channel <short(1-8)>]

access-list <access-list-number(100-199)> {deny | permit}
{every | {{icmp | igmp | ip | udp | <protocol-type(1-255)>}
{any |<src-ip-addrss> <ip_mask>} [eq {domain | echo | ftp | ftpdata | http | smtp
| snmp | telnet |tftp | www | <port-number(0-65535)>}]{any | <dst-ip-address>
<ip_mask>}
[eq {domain | echo | ftp | ftpdata |http | smtp | snmp |
telnet |tftp | www | <port-number(0-65535)>}]
[{ tos <value(0x0-0xff)> <mask(0x0-0xff)> | dscp <ipdscp> |precedence <value(0-7)>
}]}}
[ assign-queue <queue-number(0-3)> ] [{mirror | redirect }
<slot/port> | port-channel <short(1-8)>]

access-list <access-list-number(100-199)> {deny | permit}
tcp {any |<src-ip-addrss> <ip_mask>} [eq {domain | echo | ftp | ftpdata | http |
smtp
| snmp | telnet |tftp | www | <port-number(0-65535)>}]{any | <dst-ip-address>
<ip_mask>}
[eq {domain | echo | ftp | ftpdata |http | smtp | snmp |
telnet |tftp | www | <port-number(0-65535)>}]
[{ tos <value(0x0-0xff)> <mask(0x0-0xff)> | dscp <ipdscp> |precedence <value(0-7)>
}]}}
[{flag <tcp_flag> [<tcp_flag>][<tcp_flag>][<tcp_flag>][<tcp_flag>][<tcp_flag>]
[ assign-queue <queue-number(0-3)> ] [{mirror | redirect }
{<slot/port> | port-channel <short(1-8)>} ]
|[ assign-queue <queue-number(0-3)> ] [{mirror | redirect }
{<slot/port> | port-channel <short(1-8)>} ]} ]

no access-list { <access-list-number(1-99)> | <access-list-number(100-199)>}
```

Mode Global Configuration Mode

`access-list-number(1-99)` - Specifies the number for standard ACL

`access-list-number(100-199)` - Specifies the number for extended ACL

`permit` - Specifies which IPv4 packets can be forwarded

`deny` - Specifies which IPv4 packets can be rejected

`every` - Matches all the IPv4 packets

`any` - Any IPv4 address

`src-ip-address` - Source IP address

`ip-mask` - Wildcard mask for IP address

`icmp` - Specifies which ICMP packets can be rejected or forwarded

`igmp` - Specifies which IGMP packets can be rejected or forwarded

`ip` - Specifies which IP packets can be rejected or forwarded

`tcp` - Specifies which TCP packets can be rejected or forwarded

`udp` - Specifies which UDP packets can be rejected or forwarded

`protocol-type(1-255)` - Specifies which protocol's packets can be rejected or forwarded

`domain` - Specifies domain L4 port and the port number is 53

`echo` - Specifies echo L4 port and the port number is 7

`ftp` - Specifies ftp L4 port and the port number is 21

`ftpdata` - Specifies ftpdata L4 port and the port number is 20

`http` - Specifies http L4 port and the port number is 80

`smtp` - Specifies smtp L4 port and the port number is 25

`snmp` - Specifies snmp L4 port and the port number is 161

`telnet` - Specifies telnet L4 port and the port number is 23

`tftp` - Specifies tftp L4 port and the port number is 69

`www` - Specifies www L4 port and the port number is 80

`port-number(0-65535)` - Specifies which L4 port number to be filtered

`dst-ip-address` - Destination IP address

`tos` - Specifies the tos value and mask as hexadecimal from 0x0 to 0xff

`dscp` - Specifies the dscp value or keyword

`precedence value(0-7)` - Specifies the ip precedence value

`flag` - Specifies a TCP flag keyword

`assign-queue queue-number(0-3)` - Specifies the assign queue for matched this rule

`mirror` - Specifies mirror interface which packets match this rule

`redirect` - Specifies redirect interface which packets match this rule

`port-channel` - Port Channel Identifier

`slot/port` - Physical interface ID including type, slot and port format

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# access-list 1 deny every
(JGSM7224)(config)# access-list 100 permit every
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip access-lists` - Displays IP access list information

ip access-list

This command is used to create an IP Extended ACL List which is identified by the access list name.

Format
```
ip access-list <access-list-name(1-31)>
ip access-list rename <old-list-name(1-31)> <new-list-name(1-31)>
no ip access-list <access-list-name(1-31)>
```

Mode Global Configuration Mode

`access-list-name` - Specifies the name with IP ACL

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip access-list ip1
(JGSM7224)(config-ipv4-acl)#
-------------------------------------------------------------------------------
```

Related Command

`show ip access-lists` - Displays ip access list information

ip access-list rule

This command is used to create an IP Extended ACL List rule which belongs the access-namelist.

Format

```
{deny | permit}
{every | {{icmp | igmp | ip |tcp | udp | <protocol-type(1-255)>}
{any |<src-ip-addrss> <ip_mask>} [eq {domain | echo | ftp |
ftpdata | http | smtp
| snmp | telnet |tftp | www | <port-number(0-65535)>}]{any |
<dst-ip-address> <ip_mask>}
[eq {domain | echo | ftp | ftpdata |http | smtp | snmp |
telnet |tftp | www | <port-number(0-65535)>}]
[{ tos <value(0x0-0xff)> <mask(0x0-0xff)> | dscp <ipdscp>
|precedence <value(0-7)> }]}}
[ assign-queue <queue-number(0-3)> ] [{mirror | redirect }
<slot/port> | port-channel <short(1-8)>]

{deny | permit}
tcp {any |<src-ip-addrss> <ip_mask>} [eq {domain | echo | ftp |
ftpdata | http | smtp
| snmp | telnet |tftp | www | <port-number(0-65535)>}]{any |
<dst-ip-address> <ip_mask>}
[eq {domain | echo | ftp | ftpdata |http | smtp | snmp |
telnet |tftp | www | <port-number(0-65535)>}]
[{ tos <value(0x0-0xff)> <mask(0x0-0xff)> | dscp <ipdscp>
|precedence <value(0-7)> }]}}
[{flag <tcp_flag>
[<tcp_flag>][<tcp_flag>][<tcp_flag>][<tcp_flag>][<tcp_flag>][<tcp_flag>]
[ assign-queue <queue-number(0-3)> ] [{mirror | redirect }

{<slot/port> | port-channel <short(1-8)>} ]
|[ assign-queue <queue-number(0-3)> ] [{mirror | redirect }
{<slot/port> | port-channel <short(1-8)>} ]} ]
```

Mode Acl ipv4 Configuration Mode

`permit` - Specifies which IPv4 packets can be forwarded

`deny` - Specifies which IPv4 packets can be rejected

`every` - Match all the IPv4 packets

`any` - Any IPv4 address

`src-ip-address` - Source IP address

`ip-mask` - Wildcard mask for IP address

`icmp` - Specifies which ICMP packets can be rejected or forwarded

`igmp` - Specifies which IGMP packets can be rejected or forwarded

`ip` - Specifies which IP packets can be rejected or forwarded

`tcp` - Specifies which TCP packets can be rejected or forwarded

`udp` - Specifies which UDP packets can be rejected or forwarded

`protocol-type(1-255)` - Specifies which protocol's packets can be rejected or forwarded

`domain` - Specifies domain L4 port and the port number is 53

`echo` - Specifies echo L4 port and the port number is 7

`ftp` - Specifies ftp L4 port and the port number is 21

`ftpdata` - Specifies ftpdata L4 port and the port number is 20

`http` - Specifies http L4 port and the port number is 80

`smtp` - Specifies smtp L4 port and the port number is 25

`snmp` - Specifies snmp L4 port and the port number is 161

`telnet` - Specifies telnet L4 port and the port number is 23

`tftp` - Specifies tftp L4 port and the port number is 69

`www` - Specifies www L4 port and the port number is 80

`port-number(0-65535)` - Specifies which L4 port number to be filtered

`dst-ip-address` - Destination IP address

`tos` - Specifies the tos value and mask as hexadecimal from 0x0 to 0xff

`dscp` - Specifies the dscp value or keyword

`precedence value(0-7)` - Specifies the ip precedence value

`flag` - Specifies a TCP flag keyword

`assign-queue queue-number(0-3)` - Specifies the assign queue for matched this rule

`mirror` - Specifies mirror interface which packets match this rule

`redirect` - Specifies redirect interface which packets match this rule

`port-channel` - Port Channel Identifier

`slot/port` - Physical interface ID including type, slot and port format

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-ipv4-acl)# deny every
(JGSM7224)(config-ipv4-acl)# permit every
(JGSM7224)(config-ipv4-acl)#
-------------------------------------------------------------------------------
```

Related Command

`show ip access-lists` - Displays IP access list information

mac access-list

This command is used to enter the ACL MAC configuration mode and creates Layer 2 MAC ACLs.

Format

```
mac access-list extended <access-list-name(1-31)>
mac access-list extended rename <old-list-name(1-31)>
<new-list-name(1-31)>
no mac access-list extended <access-list-name(1-31)>
```

Mode Global Configuration Mode

`access-list-name` - Specifies the name with MAC ACL

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# mac access-list extended list1
(JGSM7224)(config-ext-macl)#
-------------------------------------------------------------------------------
```

Related Command

`show mac access-lists` - Displays MAC access list information

mac access-list rule

This command creates a rule based on MAC address.

Format

```
{permit | deny } {{{ any | <src-mac-address>
<src-mac-address-mask> }
{ any | <dest-mac-address> <dest-mac-address-mask> | bpdu }
[ { appletalk | arp | ibmsna | ipv4 | ipv6 | ipx | mplsmcast |
mplsucast | netbios | novell | pppoe | rarp | <protocol
(0x600-0xffff)> } ]
[ vlan <vlan-id (0-4095)> ] [ cos <value(0-7)> ]} | every}
[ assign-queue <queue-number(0-3)> ] [{ mirror | redirect }
<slot/port> | port-channel <short(1-8)>]
```

Mode MAC ACL Configuration Mode

`permit` - Specifies packets can be forwarded

`deny` - Specifies packets can be rejected

`any` - Any L2 source or destination MAC address

`src-mac-address` - L2 source MAC address

`src-mac-address-mask` - L2 source MAC address wildcard mask

`dest-mac-address` - L2 destination MAC address

`dest-mac-address-mask` - L2 destination MAC address wildcard mask

`bpdu` - Match any BPDU destination MAC Address which is 01:80:C2:xx:xx:xx

`appletalk` - Specifies AppleTalk protocol and the protocol number is 0x809B

`arp` - Specifies ARP protocol and the protocol number is 0x0806

`ibmsna` - Specifies IBMSNA protocol and the protocol number is 0x80D5

`ipv4` - Specifies IPv4 protocol and the protocol number is 0x0800

`ipv6` - Specifies IPv6 protocol and the protocol number is 0x86DD

`ipx` - Specifies IPX protocol and the protocol number is 0x8037

`mplsmcast` - Specifies MPLS-Multicast protocol and the protocol number is 0x8848

`mplsucast` - Specifies MPLS-Unicast protocol and the protocol number is 0x8847

`netbios` - Specifies NETBIOS protocol and the protocol number is 0x8191

`novell` - Specifies NOVELL protocol and the protocol numbers are 0x8137 and 0x8138

`pppoe` - Specifies PPPOE protocol and the protocol number is 0x8863 and 0x8864

`rarp` - Specifies RARP protocol and the protocol number is 0x8035

`protocol` - Specifies the L2 filter protocol type hexadecimal value and also specifies above protocol No. directly

`vlan vlan-id(0-4095)` - Specifies VLAN ID

`cos value(0-7)` - Specifies vlan priority

`every` - Match all the packets

`assign-queue queue-number(0-3)` - Specifies the assign queue for matched this rule

`mirror` - Specifies mirror interface which packets match this rule

`redirect` - Specifies redirect interface which packets match this rule

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-ext-macl)# deny 00:11:22:33:44:55 00:00:00:ff:ff:00 any vlan 1
(JGSM7224)(config-ext-macl)#
--------------------------------------------------------------------------------
```

Related Command

`show mac access-lists` - Displays MAC access list information

ip access-group

This command specifies the IP access list number to binding to specify ingress ports.

Format `ip access-group {<access-list-number (1-199)> | <access-list-name(1-31)>} in [<sequence-number(1-4294967295)>]`

`no ip access-group {<access-list-number (1-199)> | <access-list-name(1-31)>} in`

Mode
- Interface Configuration Mode
- Global Configuration Mode

`access-list-number` - Specifies the number with ACL

`access-list-name` - Specifies the name with ACL

`in` - Ingress

`sequence-number` - Specifies the sequence number to rank precedence for this interface and direction. A lower sequence number has higher precedence.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# ip access-group 1 in 100
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show ip access-lists` - Displays IP access list information

mac access-group

This command specifies the MAC access list name to bind to specify ingress ports.

Format `mac access-group <access-list-name(1-31)> in [<sequence-number(1-4294967295)>]`

`no mac access-group <access-list-name (1-31)> in`

Mode
- Interface Configuration
- Global Configuration Mode

`access-list-name` - Specifies the name with ACL

`in` - Ingress

`sequence-number` - Specifies the sequence number to rank precedence for this interface and direction. A lower sequence number has higher precedence.

Note: Only MAC ACL can be bound to the ingress port.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# mac access-group list1 in 1002
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

Related Command

`show mac access-lists` - Displays MAC access list information

show ip or mac access-lists

This command displays access list information.

Default Displays all IP or MAC ACLs

Format
```
show { ip access-lists [<access-list-id(1-199)>]
[access-list-name(1-31)] | mac access-lists [
<access-list-name(1-31)> ]}
show access-lists interface {<slot/port> | port-channel
<number(1-8)>} in
```

Mode Privileged EXEC Mode

`ip` - Displays IP access list

`mac` - Displays MAC access list

`access-list-id` - Specifies the number with IP ACL

`access-list-name` - Specifies the number with MAC ACL

`slot/port` - Specifies interface port

`port-channel` - Specifies port channel number

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show ip access-lists
Current number of all ACLs: 2
Maximum number of all ACLs: 100

ACL ID/Name          Rules Direction Interface(s)

ip1                  0          inbound
```

```
(JGSM7224)#
------------------------------------------------------------------------------
------------------------------------------------------------------------------
(JGSM7224)# show ip access-lists 122

ACL ID                          : 122
Inbound Interface(s)            : 0/1,0/2
Rule Number 1
Action                          : Deny
Protocol Type                   : ANY
IP address Type                 : IPV4
Source IP address               : 1.1.1.1
Source IP address mask          : 255.255.255.0
Destination IP address          : 2.2.2.2
Destination IP address mask     : 255.255.255.0
TOS                             : 0x22
TOS Mask                        : 0xbb
(JGSM7224)#
(JGSM7224)# show access-lists interface 0/1 in
------------------------------------------------------------------------------
```

DOS 35

dos-control

This command is used to configure DOS control, and block specific types of Denial of Service attacks.

- SIP=DIP: Source IP address = Destination IP address.
- First Fragment:TCP Header size smaller than configured value.
- TCP Fragment: IP Fragment Offset = 1.
- TCP Flag: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- L4 Port: Source TCP/UDP Port = Destination TCP/UDP Port.
- ICMP: Limiting the size of ICMP Ping packets.

Default Disabled

Syntax

```
dos-control { all | firstfrag [<0-255>] | icmp [<0-1023>]| l4port | sipdip | tcpflag | tcpfrag }
no dos-control { all | firstfrag | icmp | l4port | sipdip | tcpflag | tcpfrag }
```

Mode Global Configuration

`all` - Configure dos protection checks globally.

`firstfrag [(0-255)]` - Configure minimum TCP header size DOS protection. The default size is 20.

`icmp [(0-1023)]` - Configure Maximum ICMP Packet Size DOS protections. The default size is 512.

`l4port` - Configure the L4 Port DOS protection.

`sipdip` - Configure the sip=dip DOS protection.

`tcpflag` - Configure the tcpflag DOS protection.

`tcpfrag` - Configure the tcpfrag DOS protection.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# dos-control firstfrag 22
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show dos-control` - Displays DOS control information.

show dos-control

This command Displays DOS control information.

Default	Display DOS control Disabled
Syntax	`show dos-control`
Mode	Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show dos-control

First Frag Mode      : Disabled
Min TCP Hdr Size     : 20
ICMP Mode            : Disabled
Max ICMP Packet Size : 512
L4 Port Mode         : Disabled
SIP=DIP Mode         : Disabled
TCP Flag Mode        : Disabled
TCP Frag Mode        : Disabled

(JGSM7224)#
-------------------------------------------------------------------------------
```

Diffserv 36

diffserv

This command sets the DiffServ operational mode. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format `diffserv`
`no diffserv`

Mode Global Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# diffserv
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show diffserv` - Displays `diffserv` general status

diffserv counterMode

This command sets the DiffServ counter mode format as either octets or packets.

Default Octets

Format `diffserv counterMode {octets | packets}`

Mode Global Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# diffserv counterMode packets
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show diffserv` - Displays `diffserv` general status

class-map

This command defines a DiffServ class of type `match-all`. When used without any match condition, this command enters the class-map mode. The `class-map-name` is a case-sensitive alphanumeric string from 1 to 31 characters, uniquely identifying an existing DiffServ class. The class type of `match-all` indicates all of the individual match conditions must be true for a packet to be considered a member of the class.This command can be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

The `no class-map` command can be issued at any time. If the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format `class-map { <class-map-name> | match-all <class-map-name> [ipv4] | rename <old-class-map-name> <new-class-map-name>}`

`no class-map <class-map-name>`

Mode Global Configuration Mode

`class-map-name` - Specifies the name of the class map

`ipv4` - (Optional) Specifies the layer3 protocol for this class. If not specified, this parameter defaults to `ipv4`. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# class-map match-all class1
(JGSM7224)(config-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show class-map` - Displays class map information

match

This command adds a match condition to the specified class definition.

Format `match {any | class-map <class-map-name> | cos <value(0-7)> | secondary-cos <value(0-7)> | secondary-vlan <value(0-4095)> | destination-address mac <mac_addr> <mac_addr_mask> | dstip <ip_addr> <ip_mask> | dstl4port {domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | www |<port-number(0-65535)>} | ethertype { appletalk | arp | ibmsna | ipv4 | ipv6 | ipx | mplsmcast | mplsucast | netbios | novell | pppoe | rarp | <ethernet-type-number(0x600-0xffff)> } | ip { dscp <ipdscp> | precedence <value(0-7)> | tos <value(0x0-0xff)> <mask(0x0-0xff)>} | protocol {icmp | igmp | ip | tcp | udp | <protocol-type(0-255)>} | source-address mac <mac_addr> <mac_mask> | srcl4port {domain | echo | ftp | ftpdata | http | smtp | snmp | telnet | tftp | www |<port-number(0-65535)>} | vlan <value(0-4095)>}`

Mode Class-Map Configuration Mode

`any` - All packets

`class-map` - Match a reference class map

`cos` - Specifies VLAN priority

`mac-addr` - L2 MAC address

`mac-addr-mask` - L2 MAC address mask

`ip-addr` - IP address

`ip-mask` - Network mask for IP address

`domain` - Specifies domain L4 port and the port number is 53

`echo` - Specifies echo L4 port and the port number is 7

`ftp` - Specifies ftp L4 port and the port number is 21

`ftpdata` - Specifies ftpdata L4 port and the port number is 20

`http` - Specifies http L4 port and the port number is 80

`smtp` - Specifies smtp L4 port and the port number is 25

`snmp` - Specifies snmp L4 port and the port number is 161

`telnet` - Specifies telnet L4 port and the port number is 23

`tftp` - Specifies tftp L4 port and the port number is 69

`www` - Specifies www L4 port and the port number is 80

`port-number(0-65535)` - Specifies which L4 port number to be matched

`appletalk` - Specifies AppleTalk protocol and the protocol number is 0x809B

`arp` - Specifies ARP protocol and the protocol number is 0x0806

`ibmsna` - Specifies IBMSNA protocol and the protocol number is 0x80D5

`ipv4` - Specifies IPv4 protocol and the protocol number is 0x0800

`ipv6` - Specifies IPv6 protocol and the protocol number is 0x86DD

`ipx` - Specifies IPX protocol and the protocol number is 0x8037

`mplsmcast` - Specifies MPLS-Multicast protocol and the protocol number is 0x8848

`mplsucast` - Specifies MPLS-Unicast protocol and the protocol number is 0x8847

`netbios` - Specifies NETBIOS protocol and the protocol number is 0x8191

`novell` - Specifies NOVELL protocol and the protocol numbers are 0x8137 and 0x8138

`pppoe` - Specifies PPPOE protocol and the protocol numbers are 0x8863 and 0x8864

`rarp` - Specifies RARP protocol and the protocol number is 0x8035

`ethernet-type-number` - Specifies the ethernet type value

`icmp` - Specifies which ICMP packets can be matched

`igmp` - Specifies which IGMP packets can be matched

`ip` - Specifies which IP packets can be matched

`tcp` - Specifies which TCP packets can be matched

`udp` - Specifies which UDP packets can be matched

`protocol-type(1-255)` - Specifies which protocol's packets can be matched

`tos value(0x0-0xff) mask(0x0-0xff)` - Specifies the tos value and mask

`dscp` - Specifies the dscp value or keyword

`precedence value(0-7)` - Specifies the ip precedence value

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-classmap)# match any
(JGSM7224)(config-classmap)# match protocol icmp
(JGSM7224)(config-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show class-map` - Displays class map information

policy-map

This command is used to create, rename, or destroy a policy map.

Format `policy-map {rename <old-policy-map-name> <new-policy-map-name> | <policy-map-name> [in]}`
`no policy-map <policy-map-name>`

Mode Global Configuration Mode

`policy-map-name` - Specifies the name of the policy map

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# policy-map policy1 in
(JGSM7224)(config-policy-map)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

class

This command is used to create a class instance associated with an existing class map.

Format `class <class-map-name>`
`no class <class-map-name>`

Mode Policy map Configuration Mode

`class-map-name` - Specifies the name of the class map

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-policy-map)# class class1
(JGSM7224)(config-policy-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

assign-queue

This command modifies the queue number to which the associated traffic stream is assigned.

Format	`assign-queue <queue-number(0-3)>`
Mode	Policy Class Map Configuration

`queue-number` - Specifies the queue number

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# assign-queue 2
(JGSM7224)(config-policy-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

conform-color

This command is used to establish the traffic policing color conform mode.

Format	`conform-color <string(31)>`
Mode	Policy Class Map Configuration

`string` - Specifies the color class name.The color class should contain a single, non-excluded match criterion for one of the following fields (provided the field does not conflict with the classifier of the policy instance itself):

- Cos
- IP DSCP
- IP Precedence

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# conform-color class1
(JGSM7224)(config-policy-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

exceed-color

This command is used to establish the traffic policing color exceed mode.

Format `exceed-color <string(31)>`

Mode Policy Class Map Configuration

`string` - Specifies the color class name.The color class should contain a single, non-excluded match criterion for one of the following fields (provided the field does not conflict with the classifier of the policy instance itself):

- Cos
- IP DSCP
- IP Precedence

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# conform-color class1 exceed-color class2
(JGSM7224)(config-policy-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format `drop`

Mode Policy Class Map Configuration

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# drop
(JGSM7224)(config-policy-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

mark

This command specifies that all packets for the associated traffic stream are to the new cos, dscp, or precedence value.

Format `mark { cos <value(0-7)> | cos-as-sec-cos | ip-dscp <ipdscp> | ip-precedence <value(0-7)>}`

Mode Policy Class Map Configuration

`cos` - Specifies the new COS value

`cos-as-sec-cos` - Specifies the outer VLAN tag priority bits as the inner tag VLAN priority

`dscp` - Specifies the dscp value or keyword

`precedence value(0-7)` - Specifies the ip precedence value

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# mark cos 3
(JGSM7224)(config-policy-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

mirror

This command specifies that all packets for the associated traffic stream are to be mirrored to a specified interface.

Format `mirror {<slot/port> | {lag <lagNum(1-8)>}}`

Mode Policy Class Map Configuration

`slot/port` - Specifies interface port

`lag` - Specifies port channel number

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# mirror 0/1
(JGSM7224)(config-policy-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

policy-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are `drop`, `set-cos-transmit`, `set-dscp-transmit`, `set-prec-transmit`, or `transmit`. In this simple form of the police command, the conform action defaults to `transmit` and the violate action defaults to `drop`.

Format `police-simple {<rate(1-4294967295)> <burst-size(1-128)> conform-action {drop | set-prec-transmit <value(0-7)> | set-dscp-transmit <ipdscp)> | set-cos-transmit <value(0-7)> | set-cos-as-sec-cos | transmit} [violate-action {drop | set-prec-transmit <value(0-7)> | set-dscp-transmit <ipdscp> | set-cos-transmit <value(0-7)> | set-cos-as-sec-cos | transmit}]}`

Mode Policy Class Map Configuration

`rate` - Specifies the conforming data rate as Kbps

`burst-size` - Specifies the conforming burst size as KB

`drop` - Specifies the data's action as drop

`set-prec-transmit` - Specifies the data’s action as set precedence

`set-dscp-transmit` - Specifies the data’s action as set dscp

`set-cos-transmit` - Specifies the data’s action as set cos

`set-cos-as-sec-cos` - Specifies the outer VLAN tag priority bits as the inner tag VLAN priority.

`transmit` - Specifies the data’s action as forwarding

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# police-simple 10240 64 conform-action
transmit violate-action set-prec-transmit 4
(JGSM7224)(config-policy-classmap)#
--------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

policy-two-rate

This command is used to establish the traffic policing style for the specified class. The two-rate form of the police command uses a two data rate and burst size, resulting in three outcomes: `conform`, `exceed` and `violate`. The conforming and peak data rate is specified in kilobits per second (Kbps) and is an integer from 1 to 4294967295. (The peak data rate should be equal to or greater than the conforming data rate). The conforming and peak burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are `drop`, `set-cos-transmit`, `set-cos-as-sec-cos`, `set-dscp-transmit`, `set-prec-transmit`, or `transmit`. In this simple form of the police command, the conform action defaults to transmit and the exceed/violate action defaults to drop.

Format `police-simple {<conform-rate(1-4294967295)> <conform-burst-size(1-128)> <peak-rate(1-4294967295)> <peak-burst-size(1-128)> conform-action {drop | set-prec-transmit <value(0-7)> | set-cos-as-sec-cos | set-dscp-transmit <ipdscp> | set-cos-transmit <value(0-7)> | transmit} [exceed-action {drop | set-prec-transmit <value(0-7)> | set-cos-as-sec-cos | set-dscp-transmit <ipdscp> | set-cos-transmit <value(0-7)> | transmit}]} [violate-action {drop | set-prec-transmit <value(0-7)> | set-cos-as-sec-cos | set-dscp-transmit <ipdscp> | set-cos-transmit <value(0-7)> | transmit}]}`

Mode Policy Class Map Configuration

`conform/peak-rate` - Specifies the conforming data rate as Kbps

`conform/peak-burst-size` - Specifies the conforming burst size as KB

`drop` - Specifies the data's action as drop

`set-prec-transmit` - Specifies the data's action as set precedence

`set-dscp-transmit` - Specifies the data's action as set dscp

`set-cos-transmit` - Specifies the data's action as set cos

`transmit` - Specifies the data's action as forwarding

`set-cos-as-sec-cos` - Specifies the outer VLAN tag priority bits as the inner tag VLAN priority

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# police-two-rate 10240 64 20444 88
conform-action transmit exceed-action set-cos-as-sec-cos violate-action
set-prec-transmit 4
(JGSM7224)(config-policy-classmap)#
--------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

redirect

This command specifies that all packets for the associated traffic stream are to be redirected to a specified interface.

Format `redirect {<slot/port> | {lag <lagNum(1-8)>}}`

Mode Policy Class Map Configuration

`slot/port` - Specifies interface port

`lag` - Specifies port channel number

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-policy-classmap)# redirect 0/1
(JGSM7224)(config-policy-classmap)#
-------------------------------------------------------------------------------
```

Related Command

`show policy-map` - Displays policy map information

service-policy

This command assigns a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

Format `service-policy in <policy-map-name>`
`no service-policy in <policy-map-name>`

Mode Global or Interface Configuration Mode

`policy-map-name` - Specifies the name with policy map

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# service-policy in policy1
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show service-policy` - Displays service policy information

show diffserv

This command displays the DiffServ General Status Group and service information.

Default	Displays diffserv general status group and service information
Format	`show diffserv [service {<slot/port> in | brief [in]}]`
Mode	Privileged EXEC Mode

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show diffserv
DiffServ Admin Mode                       Enable
Class Table Size Current/Max              2 / 32
Class Rule Table Size Current/Max         0 / 192
Policy Table Size Current/Max             2 / 32
Policy Instance Table Size Current/Max    2 / 320
Policy Attribute Table Size Current/Max 1 / 960
Service Table Size Current/Max            4 / 32
(JGSM7224)#
--------------------------------------------------------------------------------
(JGSM7224)# show diffserv service brief in
DiffServ Admin Mode                       Enable
Interface  Direction  OperStatus  Policy Name
0/7        In         Up          policy1
(JGSM7224)#
--------------------------------------------------------------------------------
```

show class-map

This command displays all configuration information for the specified class.

Default	Displays class map information
Format	`show class-map [<class-map-name>]`
Mode	Privileged EXEC Mode

`class-map-name` - Specifies the name of the class map

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show class-map
Class L3
Class Name          Type Proto          Reference Class Name
class3              ALL IPV4            class1
class1              ALL IPV4
(JGSM7224)#
-------------------------------------------------------------------------------
(JGSM7224)# show class-map class3
Class Name              class3
Class Type              ALL
Class Layer3 Protocol   IPV4

Match Criteria           Values
Reference Class          class1
Protocol                 ICMP
Source Layer 4 Port      69(tftp)
-------------------------------------------------------------------------------
```

show policy-map

This command displays all configuration information for the specified policy map.

Default	Displays policy map information
Format	`show policy-map [<policy-map-name>] [interface {<slot/port> | lag <lagNum(1-8)>} in]`
Mode	Privileged EXEC Mode

`policy-map-name` - Specifies the name of the policy map

`interface` - Display summary service information for Diffserv interfaces

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show policy-map
Policy Name       Policy Type   Class members
policy2           In            class3
policy1           In            class1
(JGSM7224)#
-------------------------------------------------------------------------------
```

```
(JGSM7224)# show policy-map policy3
Policy Name                      : policy2
Policy Type                      : In
Class Name                       : class1
Policing Style                   : Police Simple
Committed Rate                   : 10240
Committed Burst Size             : 64
Conform Action                   : Send
Non-Conform Action               : Mark IP Precedence
Non-Conform IP Precedence Value  : 4
Conform Color Mode               : Blind
(JGSM7224)#
--------------------------------------------------------------------------------
(JGSM7224)# show policy-map interface 0/7 in
Interface             : 0/7
Direction             : In
Operational Status    : Up
Policy Name           : policy3
Interface Summary:

Class Name            c1
In Offered Packets    0
In Discarded Packets  0
(JGSM7224)#
--------------------------------------------------------------------------------
```

show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Default	Displays a policy summary for all interfaces
Format	`show service-policy in`
Mode	Privileged EXEC Mode

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show service-policy in
Oper          Policy
Intf Stat     Name
-----------------------------------
0/1           Down policy1
0/2           Down policy1
0/3           Down policy1
0/4           Down policy2
0/5           Down policy1
0/6           Down policy2
0/7           Up policy1
0/8           Down policy1
0/9           Down policy2
0/10          Down policy1
(JGSM7224)#
--------------------------------------------------------------------------------
```

cos-queue strict

This command activates the strict policy scheduler mode for the specified queue.

Default	Value weighted
Format	`cos-queue strict <queue-id-0> <queue-id-1> <queue-id-2> <queue-id-3>` `no cos-queue strict <queue-id-0> <queue-id-1> <queue-id-2> <queue-id-3>`
Mode	Interface Configuration Mode Global Configuration Mode

`queue-id` - The queue ID, from 0 to 3.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# cos-queue strict 0 1 2 3
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show interfaces cos-queue` - Shows the class-of-service queue configuration for the specified interface.

cos-queue min bandwidth

This command sets the minimum transmission bandwidth guarantee for each interface queue, or sets the minbandwidth to 0 to disable minbandwidth.

Default	0
Format	`cos-queue min-bandwidth <integer(0-100)> <integer(0-100)> <integer(0-100)> <integer(0-100)>` **no** `cos-queue min-bandwidth`
Mode	Interface Configuration Mode Global Configuration Mode

`minbandwidth` - Minimum bandwidth percent of queue 0, 1, 2, and 3.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# cos-queue min-bandwidth 20 10 0 10
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show interfaces cos-queue` - Shows the class-of-service queue configuration for the specified interface.

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of soothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Default	0
Format	`traffic-shape <bw>` **no** `traffic-shape`
Mode	Interface Configuration Mode Global Configuration Mode

bw - Transmission bandwidth percent.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# traffic-shape 80
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show interfaces cos-queue` - Shows the class-of-service queue configuration for the specified interface.

classofservice ip-dscp-mapping

This command maps an IP dscp to an internal traffic class.

Syntax `classofservice ip-dscp-mapping <ipdscp (0-63)> <trafficclass (0-3)>`
no `classofservice ip-dscp-mapping`

Mode Interface Configuration Mode
Global Configuration Mode

`ipdscp` - DSCP value.

`trafficclass` - Traffic class.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# classofservice ip-dscp-mapping 63 2
--------------------------------------------------------------------------------
```

Related Command

`show classofservice ip-dscp-mapping`

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class.

Syntax `classofservice dot1p-mapping <priority value(0-7)> <Traffic class value(0-3)>`
no `classofservice dot1p-mapping`

Mode Interface Configuration Mode
Global Configuration Mode

`priority value` - Priority in VLAN tag.

`Traffic class value` - Traffic class value.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# classofservice dot1p-mapping 7 2
--------------------------------------------------------------------------------
```

Related Command

```
show classofservice dot1p-mapping
```

classofservice trust

This command sets the trust mode of all ports or the specified port.

Default	dot1p
Syntax	`classofservice trust {dot1p | ip-dscp | untrusted}`
Mode	Global Configuration Interface Configuration

`dot1p` - Dot1p mode

`ip-dscp` - Ip DSCP mode.

`untrusted` - Untrusted mode.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# classofservice trust dot1p
-------------------------------------------------------------------------------
(JGSM7224)(config)# classofservice trust ip-dscp
-------------------------------------------------------------------------------
```

Related Command

```
show classofservice trust
```

show interfaces cos-queue

This command shows the class-of-service queue configuration for the specified interface.

Syntax	`show interfaces cos-queue [interface {<slot/port> | port-channel <integer(1-8)>}]`
Mode	Privileged EXEC

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show interfaces cos-queue

Global Configuration
Interface Shaping Rate      80
```

```
Queue Id    Min. Bandwidth    Scheduler Type    Queue Management Type
0           20                Strict            Tail Drop
1           10                Weighted          Tail Drop
2            0                Strict            Tail Drop
3           10                Weighted          Tail Drop
----------------------------------------------------------------------------
```

Related Commands

```
cos-queue strict
cos-queue minbandwidth
traffic-shape
```

show classofservice dot1p-mapping

This command shows the current Dot1p priority mapping to internal traffic classes for a specific interface.

Syntax `show classofservice dot1p-mapping [interface{<slot/port> | port-channel <integer(1-8)>}]`

Mode Privileged Exec Mode

Example

```
----------------------------------------------------------------------------
(JGSM7224)# show classofservice dot1p-mapping

Port   User Priority  Traffic Class
-----  -------------  -------------
0/1    0              1
0/1    1              0
0/1    2              0
0/1    3              1
0/1    4              2
0/1    5              2
0/1    6              3
0/1    7              3
----------------------------------------------------------------------------
```

Related Command

`classofservice dot1p-mapping` - Sets the VLAN priority to queue map

show classofservice ip-dscp-mapping

This command shows dscp-map information.

Syntax `show classofservice ip-dscp-mapping [interface {<slot/port> | port-channel <integer(1-8)>}]`

Mode Privileged Exec Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show classofservice ip-dscp-mapping
DSCP to Queue Map Table
-----------------------
DSCP  QueueId
----  -------
0      1
1      1
2      1
3      1
4      1
-------------------------------------------------------------------------------
```

Related Command

`classofservice ip-dscp-mapping` - Sets the dscp to queue map

show classofservice trust

This command shows trust mode.

Syntax `show classofservice trust [interface {<slot/port> | port-channel <integer(1-8)>}]`

Mode Privileged Exec Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show classofservice trust

Class of Service Trust Mode: ip-dscp
-------------------------------------------------------------------------------
```

Related Command

`classofservice trust` - Sets the trust mode of all ports or the specified port

IP Source Guard 38

IP Source Guard is a security feature that restricts IP traffic on Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the Layer 2 ports.

ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the port-security option, the data traffic will be filtered based on the IP and MAC addresses.

Default	Disabled
Format	`ip verify source {port-security}` `no ip verify`
Mode	Interface Configuration Mode

`port-security`- Verify MAC addresses

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# ip verify source
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

Related Command

`show ip verify` - Displays port IPSG status

ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format `ip verify binding <mac-address> vlan <vlan id> <ip address> interface <slot/port> | port-channel <integer (1-8)>`

`no ip binding <mac-address> vlan <vlan id> <ip address> interface <slot/port> | port-channel <integer (1-8)>`

Mode Global Configuration Mode

`mac-address` - The mac address

`vlan id` - The VLAN ID

`ip address` - The IP address

`interface` - The interface ID

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip verify binding 00:00:00:22:22:22 vlan 1 1.1.1.1
interface 0/1
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`show ip verify source` - Displays static ipsg binding

show ip verify

Use this command to display the IPSG configurations on all ports.

Format `show ip verify [interface <slot/port> | port-channel <integer (1-8)>]`

Mode Privileged EXEC Mode

`interface` - The interface ID

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip verify
Interface      Filter Type
-------------------------
0/1            ip
0/2            N/A
```

```
0/3             N/A
0/4             N/A
0/5             N/A
0/6             N/A
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`ip verify source` - Set IPSG status of an interface

show ip verify source

Use this command to display the IPSG configurations of binding for all ports.

Format `show ip verify source [interface <slot/port> | port-channel <integer (1-8)>]`

Mode Privileged EXEC Mode

`interface` - The interface ID

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show ip verify source
Interface    Filter Type   IP Address    MAC Address   VLAN
0/1          ip            1.1.1.1                     1
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`ip verify binding` - Add static ipsg binding

show ip source binding

Use this command to display the IPSG binding of static and dynamic.

Format `show ip source binding [{static | dhcp-snooping}] [interface <slot/port> | port-channel <integer (1-8)>] [vlan <vlan-id(1-4094)>]`

Mode Privileged EXEC Mode

`static` - Static binding

`dhcp-snooping` - Dynamic binding

`interface` - The interface ID

`vlan-id` - VLAN ID

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# show ip source binding
MAC Address        IP Address     Type           VLAN      Interface
00:00:00:22:22:22     1.1.1.1     static         1         0/1
00:00:00:33:33:33     2.2.2.2     static         1         0/1
00:02:11:29:00:02    10.0.0.1     dhcp-snooping  1         0/1
00:02:11:29:00:03    10.0.0.1     dhcp-snooping  1         0/1
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Command

`ip verify binding` - Add static ipsg binding

DNS Client 39

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components.

ip domain lookup

Use this command to enable the DNS client. The `no` form of this command disables the DNS client.

Default	Enabled
Format	`ip domain lookup` `no ip domain lookup`
Mode	Global Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip domain lookup
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`ip domain name` - Define a default domain name that the software uses to complete unqualified host name

`ip name server` - Configure the available name servers

`show hosts` - Displays detailed information about domain name system

ip domain name

Use this command to define a default domain name that the software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. The no form of this command removes the default domain name.

Format `ip domain name <name>`
`no ip domain name`

Mode Global Configuration Mode

<name> - Cannot be longer than 255 characters and should not include an initial period

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip domain name switch.com
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

This example configures switch.com as a default domain name. For an unqualified hostname *xxx*, a DNS query is made to find the IP address corresponding to *xxx*.switch.com.

Related Commands

ip domain lookup - Enables the DNS client

show hosts - Displays detailed information about domain name system

ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The preference of the servers is determined by the order they were entered. The no form of this command removes name servers.

Format `ip name-server <server-address1>`
`[server-address2...server-address8]`
`no ip name-server[server-address1...server-address8]`

Mode Global Configuration Mode

<server-address> - A valid IPv4 or IPv6 address of the server

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip name server 192.168.0.99 172.17.144.2
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`ip domain lookup` - Enable the DNS client

`show hosts` - Displays detailed information about the domain name system

ip host

Use this command to define static host name-to-address mapping in the host cache. The no form of this command removes the name-to-address mapping.

Format `ip host <name> <ipaddress>`
`no ip host <name>`

Mode Global Configuration Mode

`<name>` - Host name

`<ipaddress>` - The IP address of the host

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip host sa-pc 192.168.0.5
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`clear host` - Delete entries from the host name-to-address cache

`show hosts` - Displays detailed information about the domain name system

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. The no form of this command removes the static host name-to-IPv6 address mapping in the host cache.

Format `ipv6 host <name> <v6 address>`
`no ipv6 host <name>`

Mode Global Configuration Mode

`<name>` - Host name

`<v6 address>` - The IPv6 address of the host

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ipv6 host sa6-pc 2001::2
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`clear host` - Delete entries from the host name-to-address cache

`show hosts` - Displays detailed information about the domain name system

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The `no` form of this command resets it to default value.

Default	2
Format	`ip domain retry <number>` **`no`** `ip domain retry`
Mode	Global Configuration Mode

`<number>` - Indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip domain retry 5
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Command

`ip domain timeout` - Specify the amount of time to wait for a response to a DNS query

`show hosts` - Displays detailed information about the domain name system

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The no form of this command resets it to default value.

Default 3

Format `ip domain timeout <seconds>`
`no ip domain timeout`

Mode Global Configuration Mode

<seconds> - Specifies the time, in seconds, to wait for a response to a DNS query. This seconds ranges from 0 to 3600.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# ip domain timeout 5
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

Related Commands

`ip domain retry` - Specify the number of times to retry sending DNS queries

`show hosts` - Displays detailed information about the domain name system

clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format `clear host {<name> | all}`

Mode Privileged Exec Mode

<name> - A particular host entry to remove. Name ranges from 1-255 characters

`all` - Removes all entries

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# clear host all
(JGSM7224)#
-------------------------------------------------------------------------------
```

Related Commands

`ip domain lookup` - Enable the DNS client

`show hosts` - Displays detailed information about the domain name system

show hosts

Use this command to display the default domain name, query retry times and timeout value, a list of name server hosts, the static and the cached list of host names and addresses. This command displays both IPv4 and IPv6 entries.

Format	`show hosts [name]`
Mode	Privileged Exec Mode

`[name]` - Ranges from 1-255 characters

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show hosts
Domain Name Lookup.................. Enabled
Default domain..................... switch.com
Number of retries.................. 2
Retry timeout period............... 3
Name servers(Preference order)...... 192.168.0.99, 172.17.144.5

Configured host name-to-address mapping:
Host             Addresses
sa-pc            192.168.0.5
Cached host name-to-address mapping:
Host               Total    Elapsed      Type     Addresses
----------------   -----    -------      ----     ----------
ha-pc.switch.com   300      5            IPv4     192.168.0.10
(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Commands

`ip domain lookup` - Enable the DNS client

`ip domain name` - Define a default domain name that the software uses to complete unqualified host name

`ip name server` - Configure the available name servers

`ip host` - Define static host name-to-address mapping in the host cache

`ipv6 host` - Define static host name-to-IPv6 address mapping in the host cache

`ip domain retry` - Specify the number of times to retry sending DNS queries

`ip domain timeout` - Specify the amount of time to wait for a response to a DNS query

debug dns

This command turns on DNS debug trace. The `no` form of this command turns off DNS debug trace.

Format `debug dns [ all | buffer | failure | management ]`
`no debug dns [ all | buffer | failure | management ]`

Mode Privileged Exec Mode

`all` - Turn on all debug trace

`buffer` - Turn on buffer debug trace

`failure` - Turn on failure debug trace.

`management` - Turn on management debug trace.

Example

```
-------------------------------------------------------------------------------
(JGSM7224)# debug dns all
(JGSM7224)#
-------------------------------------------------------------------------------
```

Storm Control 40

This chapter describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

JGSM7224 provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you enable the feature for all interfaces or for individual interfaces, and you set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the `no` version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the `no` version of the `storm-control` command (not stating a “level” disables that form of storm-control but maintains the configured “level” (to be active the next time that form of storm-control is enabled.)

Note: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes—used to calculate a packet-per-second (pps) rate—as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10 percent, this is converted to about 23500 pps (in consideration of IFG, PR, SD - 20 bytes altogether), and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512 bytes packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for a specific interface. If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

The no form of this command disables broadcast storm recovery mode for a specific interface.

Default	Enabled
Format	`storm-control broadcast` `no storm-control broadcast`
Mode	Interface Configuration Mode

Example

```
---------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control broadcast
(JGSM7224)(config-if)#
---------------------------------------------------------------------------
```

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for an interface as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

The no form of this command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Default	5
Format	`storm-control broadcast level <level-value(1-100)>` `no storm-control broadcast level`
Mode	Interface Configuration Mode

`<level-value>` - The threshold, which is a percentage of link speed

Example

```
---------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control broadcast level 10
(JGSM7224)(config-if)#
---------------------------------------------------------------------------
```

storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for an interface in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

The no form of this command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Default 0

Format
```
storm-control broadcast rate <rate-value(1-1488000)>
no storm-control broadcast rate
```

Mode Interface Configuration Mode

<rate-value> - The threshold in packets per second

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control broadcast rate 200000
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

storm-control broadcast (Global Config)

This command enables broadcast storm recovery mode for all interfaces. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

The no form of this command disables broadcast storm recovery mode for all interfaces.

Default Disabled

Format
```
storm-control broadcast
no storm-control broadcast
```

Mode Global Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# storm-control broadcast
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

storm-control broadcast level (Global Config)

This command configures the broadcast storm recovery threshold for all interfaces as a percentage of link speed and enables broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.This command also enables broadcast storm recovery mode for all interfaces.

The no version of this command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Default 5

Format
```
storm-control broadcast level <level-value(1-100)>
no storm-control broadcast level
```

Mode Global Configuration Mode

`<level-value>` - The threshold which is a percentage of link speed

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# storm-control broadcast level 10
-------------------------------------------------------------------------------
```

storm-control broadcast rate (Global Config)

Use this command to configure the broadcast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

The no version of this command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Default 0

Format
```
storm-control broadcast rate <rate-value(1-1488000)>
no storm-control broadcast rate
```

Mode Global Configuration Mode

`<rate-value>` - The threshold in packets per second

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# storm-control broadcast rate 200000
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

storm-control multicast

Use this command to enable multicast storm recovery mode for a specific interface. If the mode is enabled, multicast storm recovery is active and, if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

The no version of this command disables multicast storm recovery mode for a specific interface.

Default	Disabled
Format	`storm-control multicast` `no storm-control multicast`
Mode	Interface Configuration Mode

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control multicast
(JGSM7224)(config-if)#
-----------------------------------------------------------------------------
```

storm-control multicast level

Use this command to configure the multicast storm recovery threshold for an interface as a percentage of link speed and enable multicast storm recovery. If the mode is enabled, multi-cast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

The no version of this command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Default	5
Format	`storm-control multicast level <level-value(1-100)>` `no storm-control multicast level`
Mode	Interface Configuration Mode

`<level-value>` - The threshold which is a percentage of link speed

Example

```
------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control multicast level 10
(JGSM7224)(config-if)#
------------------------------------------------------------------------
```

storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for an interface in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

The no version of this command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Default	0
Format	`storm-control multicast rate <rate-value(1-1488000)>` `no storm-control multicast rate`
Mode	Interface Configuration Mode

`<rate-value>` - The threshold in packets per second

Example

```
------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control multicast rate 200000
(JGSM7224)(config-if)#
------------------------------------------------------------------------
```

storm-control multicast (Global Config)

This command enables multicast storm recovery mode for all interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

The no version of this command disables multicast storm recovery mode for all interfaces.

Default Disabled

Format
```
storm-control multicast
no storm-control multicast
```

Mode Global Configuration Mode

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# storm-control multicast
(JGSM7224)(config)#
-----------------------------------------------------------------------------
```

storm-control multicast level (Global Config)

This command configures the multicast storm recovery threshold for all interfaces as a percentage of link speed and enables multicast storm recovery. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.This command also enables multicast storm recovery mode for all interfaces.

The no version of this command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

Default 5

Format
```
storm-control multicast level <level-value(1-100)>
no storm-control multicast level
```

Mode Global Configuration Mode

<level-value> - The threshold which is a percentage of link speed

Example

```
-----------------------------------------------------------------------------
(JGSM7224)(config)# storm-control multicast level 10
-----------------------------------------------------------------------------
```

storm-control multicast rate (Global Config)

Use this command to configure the multicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold,

the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

The no version of this command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

Default 0

Format
```
storm-control multicast rate <rate-value(1-1488000)>
no storm-control multicast rate
```

Mode Global Configuration Mode

<rate-value> - The threshold in packets per second

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# storm-control multicast rate 200000
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

storm-control unicast

Use this command to enable unicast storm recovery mode for a specific interface. If the mode is enabled, unicast storm recovery is active and, if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

The no version of this command disables unicast storm recovery mode for a specific interface.

Default Disabled

Format
```
storm-control unicast
no storm-control unicast
```

Mode Interface Configuration Mode

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control unicast
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

storm-control unicast level

Use this command to configure the unicast storm recovery threshold for an interface as a percentage of link speed and enable unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unknown unicast traffic is limited to the configured threshold.

The no version of this command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Default 5

Format
```
storm-control unicast level <level-value(1-100)>
no storm-control unicast level
```

Mode Interface Configuration Mode

`<level-value>` - The threshold which is a percentage of link speed

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control unicast level 10
(JGSM7224)(config-if)#
-------------------------------------------------------------------------------
```

storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for an interface in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unknown unicast traffic is limited to the configured threshold.

The no version of this command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Default 0

Format
```
storm-control unicast rate <rate-value(1-1488000)>
no storm-control unicast rate
```

Mode Interface Configuration Mode

`<rate-value>` - The threshold in packets per second

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config-if)# storm-control unicast rate 200000
(JGSM7224)(config-if)#
--------------------------------------------------------------------------------
```

storm-control unicast (Global Config)

This command enables unicast storm recovery mode for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

The no version of this command disables unicast storm recovery mode for all interfaces.

Default Disabled

Format
```
storm-control unicast
no storm-control unicast
```

Mode Global Configuration Mode

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# storm-control unicast
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

storm-control unicast level (Global Config)

This command configures the unicast storm recovery threshold for all interfaces as a percentage of link speed and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for all interfaces.

The no version of this command sets the unicast storm recovery threshold to the default value for all interfaces and disables unicast storm recovery.

Default 5

Format
```
storm-control unicast level <level-value(1-100)>
no storm-control unicast level
```

Mode Global Configuration Mode

<level-value> - The threshold, which is a percentage of link speed

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# storm-control unicast level 10
-------------------------------------------------------------------------------
```

storm-control unicast rate (Global Config)

Use this command to configure the unicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unknown unicast traffic is limited to the configured threshold.

The no version of this command sets the unicast storm recovery threshold to the default value for all interfaces and disables unicast storm recovery.

Default	0
Format	`storm-control unicast rate <rate-value(1-1488000)>` `no storm-control unicast rate`
Mode	Global Configuration Mode

<rate-value> - The threshold, in packets per second

Example

```
-------------------------------------------------------------------------------
(JGSM7224)(config)# storm-control unicast rate 200000
(JGSM7224)(config)#
-------------------------------------------------------------------------------
```

storm-control flowcontrol

This command enables 802.3x flow control for the switch and applies only to full-duplex mode ports. The auto-negotiation must be enabled before enabling flow-control, and the remote device must support flow-control.

The no version of this command disables 802.3x flow control for the switch.

Default	Disabled
Format	`storm-control flowcontrol` `no storm-control flowcontrol`
Mode	Global Configuration Mode

Note: 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)(config)# storm-control flowcontrol
(JGSM7224)(config)#
--------------------------------------------------------------------------------
```

Related Command

`show interfaces` - Displays the interface status and configuration

show storm-control

This command displays the storm-control information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters.

Format `show storm-control [all | <slot/port>]`

Mode Privileged EXEC Mode

`all` - Keyword used to display the per-port configuration parameters for all interfaces.

`slot/port` - Physical interface ID, including type, slot, and port format, used to display information about a specific interface.

Example

```
--------------------------------------------------------------------------------
(JGSM7224)# show storm-control

Broadcast Storm Control Mode.............. Enable
Broadcast Storm Control Level............. 5%
Multicast Storm Control Mode.............. Enable
Multicast Storm Control Level............. 5%
Unicast Storm Control Mode................ Enable
Unicast Storm Control Level............... 5%

(JGSM7224)#
--------------------------------------------------------------------------------
```

Related Command

`show interfaces` - Displays the interface status and configuration

Dual Image 41

The software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced downtime when you upgrade or downgrade the software.

delete

This command deletes the supplied image file from the permanent storage. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, an error message appears.

Format `delete { image1 | image2 }`

Mode Privileged Configuration Mode

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# delete image1
Erase : 10...9...8...7...6...5...4...3...2...1...0
Delete Image Successfully !
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`copy` - Image download and upload

`show bootvar` - Displays boot information

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots.

Format `boot system { image1 | image2 }`

Mode Privileged Configuration Mode

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# boot system image1
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`copy` - Image download and upload

`show bootvar` - Displays boot information

show bootvar

This command displays the version information and the activation status for the current active and backup images. The command also displays any text description associated with an image.

Format `show bootvar`

Mode Privileged Configuration Mode

Example

```
-----------------------------------------------------------------------------
(JGSM7224)# show bootvar
Image Descriptions
image1 :
image2 :
Images currently available on Flash

image1    image2     current-active     next-active
-------------------------------------------------
          1.9.8      image2             image2
-------------------------------------------------
(JGSM7224)#
-----------------------------------------------------------------------------
```

Related Commands

`copy` - Image download and upload

`delete` - Delete a specific image

`boot system` - Activate a specific image

`filedescr` - Associates a given text description with an image

filedescr

This command associates a given text description with an image. Any existing description will be replaced.

Format	`filedescr { image1 | image2 } <string>`
Mode	Privileged Configuration Mode

`<string>` - Text description for a given image(1-256)

Example

```
-------------------------------------------------------------------------
(JGSM7224)# filedescr image1 DefaultImage
(JGSM7224)#
-------------------------------------------------------------------------
```

Related Commands

`copy` - Image download and upload

`show bootvar` - Displays boot information

Command List

42