

# MX-ROS V3 CLI Command Set User Manual

---

Version 1.2, July 2024

[www.moxa.com/products](http://www.moxa.com/products)

**MOXA**<sup>®</sup>

© 2024 Moxa Inc. All rights reserved.

# MX-ROS V3 CLI Command Set User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

## Copyright Notice

© 2024 Moxa Inc. All rights reserved.

## Trademarks

The MOXA logo is a registered trademark of Moxa Inc.  
All other trademarks or registered marks in this manual belong to their respective manufacturers.

## Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

## Technical Support Contact Information

[www.moxa.com/support](http://www.moxa.com/support)

# Table of Contents

<b>1. Overview .....</b>	<b>4</b>
Supported Series and Firmware Versions .....	4
Document Conventions .....	4
Command Modes .....	4
Command Sets .....	6
System .....	6
Security .....	43
Diagnostics .....	59
Network Services .....	88
<b>2. Interface and Routing Functions .....</b>	<b>105</b>
Command Modes .....	105
Command Sets .....	106
Interfaces .....	106
Routing .....	155
<b>3. NAT, VPN, and Firewall Functions .....</b>	<b>186</b>
Command Modes .....	186
Command Sets .....	187
Network Address Translation .....	187
Firewall .....	203
Virtual Private Network (VPN) .....	222
<b>4. Layer 2 Functions .....</b>	<b>239</b>
Command Modes .....	239
Command Sets .....	240
Port .....	240
Network Redundancy .....	257
Virtual LAN .....	267
Multicast .....	270
QoS and Rate Control .....	273
<b>5. Supplementary Information .....</b>	<b>282</b>
<b>6. Command Compatibility .....</b>	<b>283</b>

# 1. Overview

## Supported Series and Firmware Versions

This manual has been updated for the following products and firmware versions.

Moxa Router Series	Firmware Version
EDF-G1000 Series	V3.12
EDR-8000 Series	V3.12
EDR-G9000 Series	V3.12



### Note

Starting from V.3.12, the configuration backup/restore method has been optimized to prevent overwriting issues when users upgrade from an old version to a new version, ensuring a smoother upgrade process. Therefore, we recommend upgrading to V.3.12 or later and performing a configuration backup/restore.

The information in this document is applicable to other products and firmware that use MX-ROS V3, but the appearance and availability of feature and feature and settings may vary.

MX-ROS support will expand to other products in the future; please check the Moxa website for the latest information.

## Document Conventions

The remainder of this chapter describes the commands of the system functions for Moxa industrial secure routers.

The following table describes the notation used to indicate command-line syntax in this document:

Notation	Description
Bold <b>Text</b> without brackets	Required items. You must type as shown
[Text inside square brackets]	Optional items.
{Text inside braces}	Set of required items. You must choose one.
<Text inside angle brackets>	Placeholder for which you must supply a value.
Vertical bar	Also known as pipe, separator for mutually exclusive items. You must choose one.

## Command Modes

Refer to the following tables for the command mode descriptions.

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your router by using a normal user account and password.	#	Enter <b>exit</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"><li>Change terminal settings.</li><li>Perform basic tests.</li><li>Display system information.</li></ul>
Privileged EXEC	Begin a session with your router by using an admin type user	#	Enter <b>exit</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"><li>Change terminal settings.</li><li>Perform basic tests.</li></ul>

Mode	Access Method	Prompt	Exit Method	About This Mode
	account and password.			<ul style="list-style-type: none"> <li>• Display system information.</li> <li>• Enter configuration mode.</li> </ul>
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	(config)#	To exit to privileged EXEC mode, enter <b>exit</b> .	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example <b>ip dhcp pool &lt;index&gt;</b> command and press enter	(dhcp-config)#	To exit to global configuration mode, enter <b>exit</b> .	A sub-level to configure for example DHCP related arguments.

Tips:

1. Moxa's CLI supports command line tab completion. Type a few characters of a command and press the TAB key. Available commands will show in the console.
2. Moxa's CLI support a hot-key '?' to list an available command list under a specific command mode; or list available command parameters followed by a specific command.

Examples	
	<p>Example 1: List a command list (note that '?' will not be displayed on the console)</p> <pre>router# ? quit          - Exit Command Line Interface exit          - Exit Command Line Interface reload        - Halt and Perform a Cold Restart terminal      - Configure Terminal Page Length copy          - Import or Export File config-file   - configuration file no            - Negate a command or set its defaults save          - Save Running Configuration to Local Storage ping          - Send Echo Messages tcpdump       - Dump traffic on a network clear         - Clear Information show          - Show System Information configure     - Enter Configuration Mode sslcertgen    - Generate SSL certificate. sshkeygen     - Generate SSH host key. router#</pre> <p>Example 2: List command parameters (note that '?' will not be displayed on the console)</p> <pre>router(config)# snmp-server ? location      - Router Location description   - Router Description contact       - Router Maintainer Contact Information community     - SNMP Community Setting version       - SNMP Version Setting user          - SNMP User Setting host          - Hosts to Receive SNMP Notifications trap-mode     - SNMP Trap/Inform mode setting router(config)#</pre>

# Command Sets

## System

### Restart and Reload Factory Default

#### reload

Use the **reload** privileged command on the router to restart Moxa Router. Use the reload **factory-default** privileged command to restore the router configuration to the factory default values.

#### Synopsis

# reload [factory-default [no cert]]

<b>Option Description</b>	factory-default	Halt and perform a warm restart with factory default settings.
	no cert	By default, when resetting to factory default the device keeps the certificate configuration. Use this parameter to remove any installed "Certificate Management" and "Authentication Certificate" configuration.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	Warning: After resetting to factory defaults, previous settings cannot be recovered. To avoid this situation, you should export the current configuration file before proceeding.	
<b>Examples</b>	<ul style="list-style-type: none"><li>Reload factory default settings and keep existing certificates. router# reload factory-default Proceed with reload to factory default? [Y/n]</li><li>Reload factory default settings and remove existing certificates. router# reload factory-default no cert Proceed with reload to factory default? [Y/n]</li><li>Halt and perform a warm restart router# reload Proceed with reload ? [Y/n]</li></ul>	
<b>Error Messages</b>	N/A	
<b>Related Commands</b>	N/A	

# Information Settings

## hostname

To specify or modify the system name of the device, use the **hostname** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

(config)# **hostname** <token1> [<token2> [<token3> [<token4> [<token5>]]]]

(config)# **no hostname**

<b>Option Description</b>	token1	A set of characters without a whitespace.
	token2	A set of characters without a whitespace.
	token3	A set of characters without a whitespace.
	token4	A set of characters without a whitespace.
	token5	A set of characters without a whitespace.
<b>Defaults</b>	The default text is: "Firewall/VPN Router [6 last digits of serial number]"	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• The system name is composed of a maximum of 5 tokens, with a whitespace positioned between each token.</li><li>• Allowed characters: a-z, A-Z, 0-9 or . - _ @ ! # \$ % ^ &amp; * ( ) . /</li><li>• Maximum length of system name including whitespaces is 30.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Specify/modify the system name to "MOXA Ethernet Router TN-4908". In this example, token1=MOXA token2=Ethernet token3=Router token4=TN-4908 <pre>router# configure router(config)# hostname MOXA Ethernet Router TN-4908 router(config)# exit</pre></li><li>• Resetting router's name to default settings. <pre>router# configure router(config)# no hostname router(config)# exit</pre></li></ul>	
<b>Error Messages</b>	Length of router hostname is too long ^Parse error	
<b>Related Commands</b>	show system	

## snmp-server contact

To set the system Contact Information, use the **snmp-server contact** global configuration command. To remove the contact string, use the no form of this command.

### Synopsis

(config)# **snmp-server contact** <token1> [<token2> [<token3> [<token4> [<token5>]]]]

(config)# **no snmp-server contact**

<b>Option Description</b>	token1	A set of characters without a whitespace.
	token2	A set of characters without a whitespace.
	token3	A set of characters without a whitespace.
	token4	A set of characters without a whitespace.
	token5	A set of characters without a whitespace.
<b>Defaults</b>	Empty string	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>The contact information is composed of a maximum of 5 tokens, with a whitespace positioned between each token.</li><li>Allowed characters: a-z, A-Z, 0-9 or . - _ @ ! # \$ % ^ &amp; * ( ) . /</li><li>Maximum length of contact information including whitespaces is 40.</li></ul>	
<b>Examples</b>	<p>Specify/modify the system Contact Information to "Green Line Bob". In this example, token1=Green, token2=Line, token3=Bob</p> <pre>router# configure router(config)# snmp-server contact Green line Bob router(config)# exit</pre> <ul style="list-style-type: none"><li>Resetting contact info to default settings.</li></ul> <pre>router# configure router(config)# no snmp-server contact router(config)# exit</pre>	
<b>Error Messages</b>	Length of maintainer info is too long	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show system	



## snmp-server description

To set the system description, use the **snmp-server description** global configuration command. To remove the description string, use the **no** form of this command.

### Synopsis

(config)# **snmp-server description** <token1> [<token2> [<token3> [<token4> [<token5>]]]]

(config)# **no snmp-server description**

<b>Option Description</b>	token1	A set of characters without a whitespace.
	token2	A set of characters without a whitespace.
	token3	A set of characters without a whitespace.
	token4	A set of characters without a whitespace.
	token5	A set of characters without a whitespace.
<b>Defaults</b>	Empty string	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>The system description is composed of a maximum of 5 tokens, with a whitespace positioned between each token.</li><li>Allowed characters: a-z, A-Z, 0-9 or . - _ @ ! # \$ % ^ &amp; * ( ) . /</li><li>Maximum length of system description including whitespaces is 40.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>Specify/modify the system description to "Moxa TN router". In this example, token1=Moxa token2=TN token3=router <pre>router# configure router(config)# snmp-server description Moxa TN router router(config)# exit</pre></li><li>Resetting system description to default settings. <pre>router# configure router(config)# no snmp-server description router(config)# exit</pre></li></ul>	
<b>Error Messages</b>	Length of system description is too long	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show system	

## snmp-server location

To set the system location, use the **snmp-server location** global configuration command. To remove the location string, use the **no** form of this command.

### Synopsis

(config)# **snmp-server location** <token1> [<token2> [<token3> [<token4> [<token5>]]]]

(config)# **no snmp-server location**

<b>Option Description</b>	token1	A set of characters without a whitespace.
	token2	A set of characters without a whitespace.
	token3	A set of characters without a whitespace.
	token4	A set of characters without a whitespace.
	token5	A set of characters without a whitespace.
<b>Defaults</b>	The default text is "Device Location".	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>The location is composed of a maximum of 5 tokens, with a whitespace positioned between each token.</li> <li>Allowed characters: a-z, A-Z, 0-9 or . - _ @ ! # \$ % ^ &amp; * ( ) . /</li> <li>Maximum length of location including whitespaces is 80.</li> </ul>	
<b>Examples</b>	<p>Specify/modify the location of the device to "Consist 1". In this example, token1=Consist token2=1</p> <pre>router# configure router(config)# snmp-server location Consist 1 router(config)# exit</pre> <ul style="list-style-type: none"> <li>Resetting device location to default settings.</li> </ul> <pre>router# configure router(config)# no snmp-server location router(config)# exit</pre>	
<b>Error Messages</b>	Length of location is too long	
	% Not in correct format	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show system	

## show system

Use **show system** command to display system identification settings.

### Synopsis

# **show system**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router# show system System Information System Name : MOXA Ethernet Router TN-4908 System Location : Xidian No. 135 6F Taiwan System Description : MOXA TN router Maintainer Information : 8860289191230 MAC Address : 00:90:E8:49:08:12 Serial No. : MOXA00000000 System Uptime : 2d0h9m43s CPU Frequency : 1600 MHz
<b>Error messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	hostname snmp-server description snmp-server contact snmp-server location

## show version

Use **show version** command to display the model name and system firmware version.

### Synopsis

# **show version**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	Model Name: Display the standard model name of the device. Firmware version: Display the current installed firmware version on the device.
<b>Examples</b>	router# show version Model Name : TN-4908-8GTX-WV-T Firmware Version : V1.2 build 22092619
<b>Error messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	N/A

# Firmware Upgrade

## copy

To upgrade a firmware image to the Flash memory, use the **copy** privileged command on the router to select a remote server through TFTP, SFTP or SCP.

### Synopsis

```
# copy {{scp | sftp} <account> <password> <ip> device-firmware <filename> |
tftp <ip> device-firmware <filename>}
```

<b>Option Description</b>	scp	Specifies to download a file through an SCP server
	sftp	Specifies to download a file through an SFTP server
	account	Specifies the user name to login remote SCP or SFTP file server, max length is 31 characters.
	password	Specifies the password for authentication, max length is 63 characters.
	device-firmware	Specifies the firmware image
	ip	IP address of the file server
	filename	File name of the firmware image, max length is 63 characters.
	tftp	Specifies to download a file through TFTP
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	The system will reboot automatically, regardless of command success.	
<b>Examples</b>	<pre>Upgrade firmware from a remote SCP server. router# copy scp moxa moxa 192.168.127.102 device-firmware FWR_TN-4900_V3.0_Build_23072200.rom SCP Server IP: 192.168.127.102 Imported Firmware: FWR_TN-4900_V3.0_Build_23072200.rom Firmware transferring... Initial checking, please wait. Verified OK buildinPkg/ buildinPkg/Zeus/ buildinPkg/Zeus/MXSecurity_TN-4900_V2.0.12_Build_23072113.pkg buildinPkg/Janus/ buildinPkg/Janus/Security_TN-4900_V7.0.9_Build_23071914.pkg Checking transfer:Firmware Upgrade OK! Restart the device.</pre>	
<b>Error Messages</b>	Input error	
	Invalid parameter!	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	<pre>show version auto-backup enable</pre>	

# Configuration Backup and Restore

## copy running-config

Use the **copy** privileged command on the router to backup or restore a configuration file to/from either a USB storage device (e.g., ABC-02) or a remote file server.

### Synopsis

#### Backup configuration file:

```
# copy running-config {tftp <ip> <cfg-path-name> |
usb |
{scp | sftp} <account> <password> <ip> <cfg-path-name>}
```

#### Restore configuration file:

```
# copy { tftp <ip> config-file <cfg-path-name> |
usb <filename> |
{scp | sftp} <account> <password> <ip> config-file <cfg-path-name>}
```

<b>Option Description</b>	usb	Specifies local USB storage device
	tftp	Specifies to upload/download configuration file through TFTP file server
	ip	IP address of the file server
	cfg-path-name	Configuration file path name on remote server, max length is 63 characters
	scp	Specifies SCP file server for file transfers
	sftp	Specifies SFTP file server for file transfers, max length is 31 characters
	account	Specifies the user name to login remote SCP or SFTP file server
	password	Specifies the password for authentication, max length is 31 characters
	filename	Configuration file name, max length is 63 characters
	config-file	Specifies to import configuration
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>After importing configuration file successfully, console terminal will restart automatically.</li> <li>After exporting configuration file successfully, existing configuration file on USB will be replaced.</li> <li>Default configuration file name after export is Sys.ini.</li> <li>CLI treats the configuration file name as case-insensitive.</li> <li>Hardware interface must be enabled before selecting USB storage device.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Backup current configuration file to a remote TFTP server.  <pre>router# copy running-config tftp 192.168.127.102 sys_tftp.ini TFTP Server IP: 192.168.127.102 Exported Config File: sys_tftp.ini Config File is exporting now, please wait. Configuration Upload Success! router#</pre> </li> <li>Restore configuration from a remote SCP server.  <pre>router# copy scp moxa moxa 192.168.127.102 config-file sys_scp.ini SCP Server IP: 192.168.127.102 Imported Config File: sys_scp.ini Config File is importing now, please wait. Config file import successfully.</pre> </li> </ul>	
<b>Error Messages</b>	Input error No USB Device Invalid parameter! % Configuration Upload Fail! % Config file import failed. ^Parse error ^Incomplete command	
<b>Related</b>	show running-config	

<b>Commands</b>	auto-backup enable
-----------------	--------------------

## config-file

Use the **config-file** privileged command to configure encryption settings in the text-based config file. Use **no config-file digital-signature** command to disable Digital Signature option.

### Synopsis

```
# config-file {digital-signature |  
               data-encryption {sensitive |  
                                all} |  
               encryption-password <key-string>}
```

```
# no config-file digital-signature
```

<b>Option</b>	digital-signature	Enables / disables digital signature on the configuration file.
<b>Description</b>	data-encryption	Specifies to encrypt sensitive information (aka password) or all information in the configuration file.
	sensitive	Only sensitive information will be encrypted.
	all	All information will be encrypted.
	encryption-password	Encrypts sensitive passwords including: 1. 802.1X Server Key 2. 802.1X Local Database Account Password 3. DDNS password 4. PPTP Password 5. PPPoE password 6. IPSEC Pre-Shared Key 7. OSPF Auth key 8. OSPF MD5 Key 9. SNMP data encryption key 10. SMTP password
	key-string	An encryption key string. Maximum string length is 30. Whitespaces are not allowed.
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>This CLI command shall not be exported nor imported via a configuration file.</li><li>Users need to change "Digital Signature" / "Data Encryption" / "Encryption Password" via Web UI or CLI before importing a new configuration file if one of those settings are different than default ones.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>Enable Digital Signature. router# config-file digital-signature</li><li>Change Encryption Key to <b>moxa1234</b>. router# config-file encryption-password moxa1234</li></ul>	
<b>Error Messages</b>	Password Length should be less than 30	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	N/A	

## save config

Use the **save config** privileged command on the router to save running configuration to the local flash memory storage.

### Synopsis

# **save config**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC
<b>Usage Guidelines</b>	To guarantee the retention of all newly configured settings on the local flash memory, execute this command once all configurations are completed.
<b>Examples</b>	N/A
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	show running-config

## auto-backup config

Use the **auto-backup** global configuration commands on the router to enable auto-backup configurations to the local storage. Use the **no** form of this command to disable auto-backup function.

### Synopsis

```
(config)# auto-backup {enable |  
                          auto-load config |  
                          config}
```

```
(config)# no auto-backup {enable |  
                          auto-load |  
                          config}
```

<b>Option Description</b>	enable	Specifies to enable hardware interface (USB) to allow the router to import configuration files or export configuration file.
	auto-load config	Specifies to enable auto-load configurations from the ABC-02 on every bootup.
	config	Specifies to automatically backup configuration to ABC-02 whenever changes are made to settings.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>A local storage (ABC-02) has to be plugged in advance.</li><li>Hardware interface (USB) has to be enabled in advance. The corresponding CLI command is provided below: (config)# auto-backup enable</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>Enable auto-backup to import configuration file from the USB storage device. router# configure router(config)# auto-backup enable router(config)# auto-backup auto-load config router(config)# exit</li><li>Disable auto-backup to import configuration file from the USB storage device. router# configure router(config)# no auto-backup auto-load config router(config)# no auto-backup enable router(config)# exit</li></ul>	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related</b>	show auto-backup	

<b>Commands</b>	auto-backup event-log
-----------------	-----------------------

## config-fwr-ver-check

Use the **config-fwr-ver-check** privileged command on the router to enable firmware version checking in the configuration file. Use the **no** form of this command to disable firmware version checking.

### Synopsis

(config)# **config-fwr-ver-check**

(config)# **no config-fwr-ver-check**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC
<b>Usage Guidelines</b>	Upon activation of this feature, the configuration file will undergo firmware version checking. If the version number in the file is higher than the current version, restoration will be halted.
<b>Examples</b>	N/A
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	N/A

## show auto-backup

Use **show auto-backup** command to display system settings of auto-backup.

### Synopsis

# **show auto-backup**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router# show auto-backup auto-backup stat : Enable auto-backup auto-load config : Disable auto-backup event-log : Enable auto-backup config : Enable
<b>Error messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	auto-backup



## show running-config

Use the **show running-config** command to display the settings of the current system.

### Synopsis

# **show running-config**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC /User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show running-config ! ----- TN-4908-8GTX-WV-T----- router ospf 192.168.1.1  area 192.168.1.1  area 192.168.1.2 stub metric 999  area 192.168.3.254  area 192.168.1.1 virtual-link 192.168.1.11  area 192.168.1.1 range 192.168.3.0 255.255.255.0 vlan create 1 vlan create 2 vlan create 3 vlan create 6 vlan create 4040 vlan create 4041 interface ethernet 1/1  no shutdown  speed-duplex Auto  no flowcontrol  media cable-mode auto  switchport access vlan 6 interface ethernet 1/2 ... (omit the rest information)</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	copy config-file save config

# User Account

## username

To specify or modify the user name for local login, use the **username** global configuration command. To delete the user, use the **no** form of this command.

### Synopsis

```
(config)# username <name> {password <pwd-string> [privilege <privilege-level>] |  
privilege <privilege-level>}
```

```
(config)# no username <name>
```

<b>Option Description</b>	name	Set of characters without a whitespace. This field is case-sensitive, and allows between 4 to 32 characters
	password	Set a password for a new user or modify password for an existing user.
	pwd-string	Specifies a new password string, from 4 to 64 characters.
	privilege	Specifies user's privilege
	privilege-level	Specifies an integer: {system admin(1)   configuration admin(2)   user(3)   no login(4)} Use no login (4) to deactivate the user.
<b>Defaults</b>	user: admin pass: moxa privilege: 1 (admin) user: user pass: moxa privilege: 3 (user) user: configadmin pass: moxa privilege 2 (configuration admin)	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• &lt;pwd-string&gt; by default Min number of characters is 4 and Max number of characters is 16. and no rule for password creation is set.</li><li>• The current logged user cannot be deleted or have privilege changed.</li><li>• The default authority for a newly created account is set as User if the privilege level is not specified.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Add a new user with configuration admin privilege. router# configure router(config)# username test password test1234 privilege 2 router(config)# exit</li><li>• Delete an existing user router# configure router(config)# no username test router(config)# exit</li><li>• Modify existing user password. router# configure router(config)# username test password abc1234 router(config)# exit</li><li>• Modify existing user privilege router# configure router(config)# username test privilege 1 router(config)# exit</li><li>• Deactive an existing user router# configure router(config)# username test privilege 4 router(config)# exit</li></ul>	
<b>Error Messages</b>	% Privilege should be between 1 and 4	
	% Invalid password length	
	% The username is not available	
	% Delete login user is error operation	
	% Disable login user is error operation	
	% "admin" only to admin authority, and "user" only to user authority	
<b>Related Commands</b>	^Parse error	
	^Incomplete command	
	show users	
	password policy	

## show users

Use **show users** command to display system users information.

### **Synopsis**

# **show users**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show users Login account information:   Name             Authority   -----   admin            System admin   configadmin     Configuration admin   user             user   test            System admin</pre>
<b>Error messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	username

# Password Policy

## password-policy

To specify or modify the password policy for the login users, use the **password-policy** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

```
(config)# password-policy {minimum-length <length> |
                           complexity-check [{digit |
                                             alphabet |
                                             special-characters}] |
                           password max-life-time <days> }
```

```
(config)# no password-policy {minimum-length |
                               complexity-check [{digit |
                                                  alphabet |
                                                  special-characters}] |
                               password max-life-time}
```

<b>Option Description</b>	minimum-length	Specifies the minimum character length of user passwords.
	length	From 4 to 16 chars.
	complexity-check	Enables additional complexity requirements for password
	digit	Enables/disables password strength check: digit
	alphabet	Enables/disables password strength check: alphabet
	special-characters	Enables/disables password strength check: special characters
	password max-life-time	Specifies how long in days passwords will be valid for.
	days	Integer ranges from 0 to 365. If this is set to 0, passwords will not expire.
<b>Defaults</b>	By default no password rules are set	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	After enable password policy, existing passwords will not be affected and need to be changed manually or forced to change by next login to meet the new policy.	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Set password minimum length to 8  <pre>router# configure router(config)# password-policy minimum-length 8 router(config)# exit</pre> </li> <li>Revoking password minimum length  <pre>router# configure router(config)# no password-policy minimum-length router(config)# exit</pre> </li> <li>Set password complexity.  <pre>router# configure router(config)# password-policy complexity-check digit router(config)# password-policy complexity-check alphabet router(config)# password-policy complexity-check special-characters router(config)# exit</pre> </li> <li>Revoking password complexity  <pre>router# configure router(config)# no password-policy complexity-check router(config)# exit</pre> </li> </ul>	
<b>Error Messages</b>	% Password minimum length should between 4~16	
	% Password lifetime should be between 0~365	
	^Parse error	
<b>Related Commands</b>	^Incomplete command	
	show running-configuration	

## User Interface

### ip http-server

Use the **ip http-server** global configuration commands on the router to enable the HTTP/HTTPS service. Use the **no** form of this command to disable the HTTP/HTTPS service.

#### Synopsis

```
(config)# ip http-server [{secure [port <sec-port>] |  
                        port <port-number> |  
                        max-login-users <number>}]
```

```
(config)# no ip http-server [{secure |  
                             max-login-users}]
```

<b>Option Description</b>	secure	Specifies HTTPS support only
	port	Specifies HTTP or HTTPS port number
	sec-port	HTTPS listening port number, valid values are 443, and from 1024 to 65535, default is 443
	port-number	HTTP listening port number, valid values are 80, and from 1024 to 65535, default is 80
	max-login-users	Specify the maximum number of concurrent users for simultaneous operation of both HTTP and HTTPS
	number	Number of users, from 1 to 10, default 5.
<b>Defaults</b>	HTTP and HTTPS services are enabled.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Maximum number of concurrent login users for HTTP+HTTPS is 10.	
<b>Examples</b>	Enable HTTPS support and set port number to 404. router# configure router(config)# ip http-server secure router(config)# ip http-server secure port 404 router(config)# exit	
<b>Error Messages</b>	% Https port is invaild, the interval is 443 or from 1024 to 65535	
	% Http port is invaild, the interval is 80 or from 1024 to 65535	
	Maximum Login Users For HTTP+HTTPS should be in range of 1 to 10	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show ip http-server	

## ip telnet

To enable telnet service on the router, use the **ip telnet** global configuration command. To disable telnet service, use the **no** form of this command.

### Synopsis

```
(config)# ip telnet [port <port-number> |  
                  max-login-users <number>]
```

```
(config)# no ip telnet [max-login-users]
```

<b>Option</b>	port	Specifies telnet port number
<b>Description</b>	port-number	Server listening port number. Valid ranges are 23, 1024 to 65535, default is 23
	max-login-users	Specifies maximum number of concurrent login users
	number	Number of users, the valid ranges are 1 to 5, default is 5.
<b>Defaults</b>	Telnet service is enabled, default port number is 23	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>Valid port number ranges are 23, and from 1024 to 65535. Please make sure other services do not use the same port in advance.</li><li>Maximum number of concurrent login users for telnet+SSH is 5.</li></ul>	
<b>Examples</b>	Enable telnet support and set port number to 8080. router# configure router(config)# ip telnet port 8080 router(config)# ip telnet router(config)# exit	
<b>Error Messages</b>	Maximum Login Users For TELNET+SSH % should be in range of 1 to 5.	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show ip telnet	

## ip ssh

To enable ssh service on the router, use the **ip ssh** global configuration command. To disable ssh service, use the **no** form of this command.

### Synopsis

```
(config)# ip ssh [port <port-number>]
```

```
(config)# no ip ssh
```

<b>Option</b>	port	Specifies ssh port number
<b>Description</b>	port-number	Server listening port number. Valid ranges are 22, 1024 to 65535, default is 22
<b>Defaults</b>	SSH service is enabled, default port number is 22.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>Valid port number ranges are 22, and from 1024 to 65535. Please make sure other services do not use the same port in advance.</li><li>Maximum number of concurrent login users for telnet+SSH is 5.</li></ul>	
<b>Examples</b>	Enable ssh support and set port number to 4040. router# configure router(config)# ip ssh port 4040 router(config)# ip ssh router(config)# exit	
<b>Error Messages</b>	% SSH port xxx is invalid, the interval is from 1 to 65535.	
	% Assign duplicated port number is not allowed	
	^Parse error	
	^Incomplete command	

<b>Related Commands</b>	show ip telnet
-------------------------	----------------

## ip ping-response

### no ip ping-response

When an ICMP echo request is received on the network interface, this command determines whether or not to send an ICMP echo response.

To disable this feature, use the **no** form of this command.

#### **Synopsis**

(config-if)# **ip ping-response**

(config-if)# **no ip ping-response**

<b>Option</b>	ip	Configure IP Parameter
<b>Description</b>	ping-response	Enable Ping Response/Disable Ping Response
	no	Negate Command
<b>Defaults</b>	Disabled on all WAN interfaces, Otherwise, enabled.	
<b>Command Modes</b>	WAN Interface Configuration LAN Interface Configuration VLAN Interface Configuration Port-based Bridge Interface Configuration Zone-based Bridge Interface Configuration Cellular Interface Configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable ping response on the WAN interface. router# configure router(config)# interface wan router(config-if)# ip ping-response	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## moxa-utility

To enable Moxa Utility on the router, use the **moxa-utility** global configuration command. To disable Moxa Utility, use the **no** form of this command.

### **Synopsis**

(config)# **moxa-utility**

(config)# **no moxa-utility**

<b>Option Description</b>	N/A	N/A
<b>Defaults</b>	Enabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Moxa's network management software, such as MxConfig, relies on TCP port 443 and UDP port 40404 being open on the device for remote management. If the Moxa utility is disabled, MxConfig will be unable to establish a connection to the device.	
<b>Examples</b>	N/A	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show moxa-utility	



## show ip http-server

To check the HTTP server settings on the router, use the **show ip http-server** command.

### Synopsis

# **show ip http-server**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router# show ip http-server HTTP service is enable HTTP server capability : Present. Port:80 HTTPS secure server capability : Present. Port:443 Auto-logout : disable Maximum Login Users For HTTP+HTTPS : 5
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	ip http-server

## show ip telnet

To check the status of telnet as well as ssh on the router, use the **show ip telnet** command.

### Synopsis

# **show ip telnet**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router# show ip telnet Telnet capability : Present. Port:23 SSH capability : Present. Port:22 Maximum Login Users For Telnet+SSH : 5
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	ip telnet ip ssh

## show moxa-utility

To check the status of Moxa's utility on the router, use the **show moxa-utility** command.

### Synopsis

# **show moxa-utility**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router# show moxa-utility MOXA Utility capability : Present. Port: 4000,4001
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	moxa-utility

## SNMP

### snmp-server version

To enable/disable the Simple Network Management Protocol (SNMP) server and configure the SNMP version, use the **snmp-server version** global configuration command.

### Synopsis

(config)# **snmp-server version** {**v1-v2c-v3** |  
**v1-v2c** |  
**v3** |  
**disable**}

<b>Option Description</b>	v1-v2c-v3	Version 1, 2C and 3 support
	v1-v2c	Version 1 and 2C support
	v3	Only version 3 support
	disable	Disable SNMP service
<b>Defaults</b>	Default version is v1-v2c	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify/modify SNMP version to v3 support. router# configure router(config)# snmp-server version v3 router(config)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	snmp-server community snmp-server user snmp-server host snmp-server trap-mode snmp-server engineid show snmp	

## snmp-server community

To set up the community access string to permit access to the SNMP, use the **snmp-server community** global configuration command.

### Synopsis

```
(config)# snmp-server community <index> <community> {ro |
                                     rw |
                                     no-access}
```

<b>Option Description</b>	index	First or second community: 1 or 2
	community	SNMP community string, max length is 64 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # \$ % & * ( ) . + = { } [ ]   : ; , ~
	ro	Access mode: read-only
	rw	Access mode: read-write
	no-access	Access mode: no-access
<b>Defaults</b>	Public community is ro Private community is rw	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.</li> <li>Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects</li> </ul>	
<b>Examples</b>	Specify/modify rouser as read-only community string. router# configure router(config)# snmp-server community 1 rouser ro router(config)# exit	
<b>Error Messages</b>	% Index must be 1 - 2.	
	Access mode must be rw, ro or no-access.	
	% is over length. It must be 1 - 30.	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	snmp-server version snmp-server user snmp-server host snmp-server trap-mode snmp-server engineid show snmp	

## snmp-server user

In the SNMPv3 application, to configure a user's authentication type and password, use the **snmp-server user** global configuration command.

### Synopsis

```
(config)# snmp-server user {admin | user} auth {no-auth |
                                md5 |
                                sha} [priv {des | aes} <password>]
```

<b>Option Description</b>	admin	System admin group for authentication
	user	User group for authentication
	auth	Specifies which authentication type should be used
	no-auth	Authentication type: no-auth
	md5	Authentication type: MD5
	sha	Authentication type: SHA
	priv	Specifies which encryption algorithm should be used
	des	Encryption algorithm: DES
	aes	Encryption algorithm: AES
	password	Data encryption key, 8 to 64 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # \$ % & * ( ) . + = { } [ ]   : ; , ~
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Length of password must be at least 8 characters.	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Specify/modify data encryption (DES) key to moxamoxa for admin user-group.  <pre>router# configure router(config)# snmp-server user admin auth md5 priv des moxamoxa router(config)# exit</pre> </li> <li>Specify/modify authentication type to sha without altering priv and password arguments.  <pre>router# configure router(config)# snmp-server user admin auth sha router(config)# exit</pre> </li> </ul>	
<b>Error Messages</b>	% SNMP user must be ( admin   user )!!	
	% SNMP authtype must be ( no-auth   md5   sha )!!	
	% Data Encryption must be at least 8 bytes !!!	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	snmp-server community snmp-server version snmp-server host snmp-server trap-mode snmp-server engineid show snmp	

## snmp-server engineid

To enable and configure user-defined SNMP engine ID, use the **snmp-server engineid** global configuration command. To disable and clear user-defined SNMP engine ID, use **no** form of this command.

### Synopsis

(config)# **snmp-server engineid** <hex-string>

(config)# **no snmp-server engineid**

<b>Option Description</b>	hex-string	Specifies the hexadecimal string of user-defined engine ID. The length of this hexadecimal string including the prefix 800021f305 is expected from 12 to 64.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• The length of the hexadecimal string is required to be an even number.</li> <li>• The &lt;hex-string&gt; must use combination of letters from 0-9, a-f, A-F.</li> <li>• The &lt;hex-string&gt; must contain a prefix string <b>800021f305</b>.</li> <li>• In order to use this command, SNMP version is required to be configured as either v1-v2c-v3 or v3.</li> <li>• It is required to re-apply or change the password for every user again to let user-defined Engine ID take effect.</li> </ul>	
<b>Examples</b>	Specify a user-defined engine ID 0x800021f3051234. <pre>router# configure router(config)# snmp-server version v1-v2c-v3 router(config)# snmp-server engineid 800021f3051234 router(config)# exit</pre>	
<b>Error Messages</b>	% Invalid Engine ID : prefix should be 800021f305	
	% The hexadecimal string format is invalid. Please use combination of letters from 0-9, a-f, A-F.	
	% The length of the hexadecimal string is required to be an even number.	
	^Parse error	
<b>Related Commands</b>	^Incomplete command	
	snmp-server community	
	snmp-server user	
	snmp-server host	
	snmp-server trap-mode	
	snmp-server version	
show snmp		

## show snmp

To check the SNMP server settings on the router, use the **show snmp** command.

### Synopsis

# **show snmp**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre> router# show snmp SNMP Read/Write Settings   SNMP Versions           : v1-v2c-v3   SNMP Engine ID          : 800021f3030090e8a9ed13   First Community         : public   Second Community        : private   Admin Auth. Type        : md5   Admin Data Encryption Key : Enable *****   User Auth. Type         : md5   User Data Encryption Key : Disable  Trap Settings   Trap Server 1 IP/Name    : 9.1.1.1   Trap Server 2 IP/Name    : 9.1.1.2   Trap Server 3 IP/Name    : 9.1.1.3   Trap Community           : public  Trap Mode   Mode                     : Trap V3   User                      : trapv3-user   Auth                      : sha   Priv                      : Enable  Private MIB information   Switch Object ID         : enterprise.8691.6.100 </pre>
<b>Error Messages</b>	^Parse error
<b>Related Commands</b>	<pre> snmp-server version snmp-server community snmp-server user snmp-server host snmp-server trap-mode snmp-server engineid snmp-server trap-v3 snmp-server inform-v3 </pre>

## Date and Time

### clock set

Use the **clock set** global configuration command on the router to set the current time.

#### **Synopsis**

(config)# **clock set** <time> <month> <day> <year>

<b>Option</b>	time	hh:mm:ss
<b>Description</b>	month	1 ~ 12
	day	1 ~ 31
	year	2000 ~ 2037
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set system time to Jan 31 , 2022 14:45:30. router# configure router(config)# clock set 14:45:30 1 31 2022 router(config)# exit	
<b>Error Messages</b>	Illegal parameters!	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show clock	

## clock summer-time

Use the **clock summer-time** global configuration command on the router to enable the day light saving time offset and set the duration. Use the **no** form of this command to disable it.

### Synopsis

```
(config)# clock summer-time {start-date <month> <week> <day> <hour> <min> |  
                             end-date <month> <week> <day> <hour> <min> |  
                             offset <offset-hour> [<offset-min>]}
```

```
(config)# no clock summer-time
```

<b>Option Description</b>	start-date	The date when summer time offset start
	end-date	The date when summer time offset end
	month	From 'Jan', 'January' or '1' to 'Dec', 'December', or '12'
	week	From '1st' or '1' to 'Last' or '6'
	day	From 'Sun', 'Sunday' or '1' to 'Sat', 'Saturday' or '7'
	hour	Ranges from 0 to 23
	min	Ranges from 0 to 59
	offset	Summer time offset
	offset-hour	Ranges from 1 to 12
	offset-min	30 to represents half an hour is allowed.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	When configuring the summer time offset, the start-date and end-date must be configured correctly first.	
<b>Examples</b>	Set daylight saving time : start from March, 2nd week, Sunday, 02:00; end at September 1st week, Sunday, 02:00; offset hour: 2. router# configure router(config)# clock summer-time start-date 3 2 1 2 0 router(config)# clock summer-time end-date 9 1 1 2 0 router(config)# clock summer-time offset 2 router(config)# exit	
<b>Error Messages</b>	Invalid parameter Month must be configured as 'Jan', 'January' or a numerical '1'. Week must be configured as '1st', '2nd', '3rd', '4th', '5th' or 'Last' Day must be configured as 'Sun', 'Sunday' or a numerical '1'. Hour must be in the range from 0 to 23. Please input the correct start/end date of the summer time first! Minutes offset is invalid, just only type '30' Hour offset is out of range. ^Parse error ^Incomplete command	
<b>Related Commands</b>	show clock	



## clock timezone

Use the **clock timezone** global configuration command on the router to set the current time zone.

### Synopsis

```
(config)# clock timezone gmt <offset-hour> [{<half-hour> |
city <city-name>}]
```

Option	Value	Description																																																																																																																								
gmt		Greenwich Mean Time																																																																																																																								
offset-hour		-12 ~ 12																																																																																																																								
half-hour		30 to represents half an hour is allowed																																																																																																																								
city		Specifies a city of a timezone																																																																																																																								
city-name		Refers to below list to understand available city names correlated to its offset hour:																																																																																																																								
		<table border="1"> <thead> <tr> <th>Offset-hour</th> <th>city-name</th> <th>Major Cities in the timezone</th> </tr> </thead> <tbody> <tr><td>-12</td><td>Eniwetok</td><td>Eniwetok, Kwajalein</td></tr> <tr><td>-11</td><td>Midway-Island</td><td>Midway Island , Samoa</td></tr> <tr><td>-10</td><td>Hawaii</td><td>Hawaii</td></tr> <tr><td>-9</td><td>Alaska</td><td>Alaska</td></tr> <tr><td>-8</td><td>Pacific-Time</td><td>Pacific Time (US &amp; Canada), Tijuana</td></tr> <tr><td>-7</td><td>Arizona</td><td>Arizona</td></tr> <tr><td>-7</td><td>Mountain-Time</td><td>Mountain Time (US &amp; Canada)</td></tr> <tr><td>-6</td><td>Central-Time</td><td>Central Time (US &amp; Canada)</td></tr> <tr><td>-6</td><td>Mexico-City</td><td>Mexico City, Tegucigalpa</td></tr> <tr><td>-6</td><td>Saskatchewan</td><td>Saskatchewan</td></tr> <tr><td>-5</td><td>Bogota</td><td>Bogota, Lima, Quito</td></tr> <tr><td>-5</td><td>Eastern-Time</td><td>Eastern Time (US &amp; Canada)</td></tr> <tr><td>-5</td><td>Indiana</td><td>Indiana (East)</td></tr> <tr><td>-4</td><td>Atlantic-Time</td><td>Atlantic Time (Canada)</td></tr> <tr><td>-4</td><td>Caracas</td><td>Caracas, La Paz</td></tr> <tr><td>-4</td><td>Santiago</td><td>Santiago</td></tr> <tr><td>-3 30</td><td>Newfoundland</td><td>Newfoundland</td></tr> <tr><td>-3</td><td>Brasilia</td><td>Brasilia</td></tr> <tr><td>-3</td><td>Buenos-Aires</td><td>Buenos Aires, Georgetown</td></tr> <tr><td>-2</td><td>Mid-Atlantic</td><td>Mid-Atlantic</td></tr> <tr><td>-1</td><td>Azores</td><td>Azores, Cape Verde Is.</td></tr> <tr><td>0</td><td>Casablanca</td><td>Casablanca, Monrovia</td></tr> <tr><td>0</td><td>Greenwich</td><td>Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London</td></tr> <tr><td>+1</td><td>Amsterdam</td><td>Amsterdam, Berlin, Bern, Stockholm, Vienna</td></tr> <tr><td>+1</td><td>Belgrade</td><td>Belgrade, Bratislava, Budapest, Ljubljana, Prague</td></tr> <tr><td>+1</td><td>Brussels</td><td>Brussels, Copenhagen, Madrid, Paris, Vilnius</td></tr> <tr><td>+1</td><td>Sarajevo</td><td>Sarajevo, Skopje, Warsaw, Zagreb</td></tr> <tr><td>+2</td><td>Athens</td><td>Athens, Istanbul, Minsk</td></tr> <tr><td>+2</td><td>Bucharest</td><td>Bucharest</td></tr> <tr><td>+2</td><td>Cairo</td><td>Cairo</td></tr> <tr><td>+2</td><td>Harare</td><td>Harare, Pretoria</td></tr> <tr><td>+2</td><td>Helsinki</td><td>Helsinki, Kyiv, Riga, Sofia, Tallinn</td></tr> <tr><td>+2</td><td>Jerusalem</td><td>Jerusalem</td></tr> <tr><td>+3</td><td>Baghdad</td><td>Baghdad, Kuwait, Riyadh</td></tr> <tr><td>+3</td><td>Moscow</td><td>Moscow, St. Petersburg, Volgograd</td></tr> <tr><td>+3</td><td>Nairobi</td><td>Nairobi</td></tr> <tr><td>+3 30</td><td>Tehran</td><td>Tehran</td></tr> <tr><td>+4</td><td>Abu-Dhabi</td><td>Abu Dhabi, Muscat</td></tr> <tr><td>+4</td><td>Baku</td><td>Baku, Tbilisi</td></tr> </tbody> </table>	Offset-hour	city-name	Major Cities in the timezone	-12	Eniwetok	Eniwetok, Kwajalein	-11	Midway-Island	Midway Island , Samoa	-10	Hawaii	Hawaii	-9	Alaska	Alaska	-8	Pacific-Time	Pacific Time (US & Canada), Tijuana	-7	Arizona	Arizona	-7	Mountain-Time	Mountain Time (US & Canada)	-6	Central-Time	Central Time (US & Canada)	-6	Mexico-City	Mexico City, Tegucigalpa	-6	Saskatchewan	Saskatchewan	-5	Bogota	Bogota, Lima, Quito	-5	Eastern-Time	Eastern Time (US & Canada)	-5	Indiana	Indiana (East)	-4	Atlantic-Time	Atlantic Time (Canada)	-4	Caracas	Caracas, La Paz	-4	Santiago	Santiago	-3 30	Newfoundland	Newfoundland	-3	Brasilia	Brasilia	-3	Buenos-Aires	Buenos Aires, Georgetown	-2	Mid-Atlantic	Mid-Atlantic	-1	Azores	Azores, Cape Verde Is.	0	Casablanca	Casablanca, Monrovia	0	Greenwich	Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London	+1	Amsterdam	Amsterdam, Berlin, Bern, Stockholm, Vienna	+1	Belgrade	Belgrade, Bratislava, Budapest, Ljubljana, Prague	+1	Brussels	Brussels, Copenhagen, Madrid, Paris, Vilnius	+1	Sarajevo	Sarajevo, Skopje, Warsaw, Zagreb	+2	Athens	Athens, Istanbul, Minsk	+2	Bucharest	Bucharest	+2	Cairo	Cairo	+2	Harare	Harare, Pretoria	+2	Helsinki	Helsinki, Kyiv, Riga, Sofia, Tallinn	+2	Jerusalem	Jerusalem	+3	Baghdad	Baghdad, Kuwait, Riyadh	+3	Moscow	Moscow, St. Petersburg, Volgograd	+3	Nairobi	Nairobi	+3 30	Tehran	Tehran	+4	Abu-Dhabi	Abu Dhabi, Muscat	+4	Baku	Baku, Tbilisi
Offset-hour	city-name	Major Cities in the timezone																																																																																																																								
-12	Eniwetok	Eniwetok, Kwajalein																																																																																																																								
-11	Midway-Island	Midway Island , Samoa																																																																																																																								
-10	Hawaii	Hawaii																																																																																																																								
-9	Alaska	Alaska																																																																																																																								
-8	Pacific-Time	Pacific Time (US & Canada), Tijuana																																																																																																																								
-7	Arizona	Arizona																																																																																																																								
-7	Mountain-Time	Mountain Time (US & Canada)																																																																																																																								
-6	Central-Time	Central Time (US & Canada)																																																																																																																								
-6	Mexico-City	Mexico City, Tegucigalpa																																																																																																																								
-6	Saskatchewan	Saskatchewan																																																																																																																								
-5	Bogota	Bogota, Lima, Quito																																																																																																																								
-5	Eastern-Time	Eastern Time (US & Canada)																																																																																																																								
-5	Indiana	Indiana (East)																																																																																																																								
-4	Atlantic-Time	Atlantic Time (Canada)																																																																																																																								
-4	Caracas	Caracas, La Paz																																																																																																																								
-4	Santiago	Santiago																																																																																																																								
-3 30	Newfoundland	Newfoundland																																																																																																																								
-3	Brasilia	Brasilia																																																																																																																								
-3	Buenos-Aires	Buenos Aires, Georgetown																																																																																																																								
-2	Mid-Atlantic	Mid-Atlantic																																																																																																																								
-1	Azores	Azores, Cape Verde Is.																																																																																																																								
0	Casablanca	Casablanca, Monrovia																																																																																																																								
0	Greenwich	Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London																																																																																																																								
+1	Amsterdam	Amsterdam, Berlin, Bern, Stockholm, Vienna																																																																																																																								
+1	Belgrade	Belgrade, Bratislava, Budapest, Ljubljana, Prague																																																																																																																								
+1	Brussels	Brussels, Copenhagen, Madrid, Paris, Vilnius																																																																																																																								
+1	Sarajevo	Sarajevo, Skopje, Warsaw, Zagreb																																																																																																																								
+2	Athens	Athens, Istanbul, Minsk																																																																																																																								
+2	Bucharest	Bucharest																																																																																																																								
+2	Cairo	Cairo																																																																																																																								
+2	Harare	Harare, Pretoria																																																																																																																								
+2	Helsinki	Helsinki, Kyiv, Riga, Sofia, Tallinn																																																																																																																								
+2	Jerusalem	Jerusalem																																																																																																																								
+3	Baghdad	Baghdad, Kuwait, Riyadh																																																																																																																								
+3	Moscow	Moscow, St. Petersburg, Volgograd																																																																																																																								
+3	Nairobi	Nairobi																																																																																																																								
+3 30	Tehran	Tehran																																																																																																																								
+4	Abu-Dhabi	Abu Dhabi, Muscat																																																																																																																								
+4	Baku	Baku, Tbilisi																																																																																																																								

		+4 30	Kabul	Kabul
		+5	Ekaterinburg	Ekaterinburg
		+5	Islamabad	Islamabad, Karachi, Tashkent
		+5 30	Bombay	Bombay, Calcutta, Madras, New Delhi
		+6	Astana	Astana, Almaty, Dhaka
		+6	Colombo	Colombo
		+7	Bangkok	Bangkok, Hanoi, Jakarta
		+8	Beijing	Beijing, Chongqing, Hongkong, Urumqi
		+8	Perth	Perth
		+8	Singapore	Singapore
		+8	Taipei	Taipei
		+9	Osaka	Osaka, Sapporo, Tokyo
		+9	Seoul	Seoul
		+9	Yakutsk	Yakutsk
		+9 30	Adelaide	Adelaide
		+9 30	Darwin	Darwin
		+10	Brisbane	Brisbane
		+10	Canberra	Canberra, Melbourne, Sydney
		+10	Guam	Guam, Port Moresby
		+10	Hobart	Hobart
		+10	Vladivostok	Vladivostok
		+11	Magadan	Magadan, Solomon Is., New Caledonia
		+12	Auckland	Auckland, Wellington
		+12	Fiji	Fiji, Kamchatka, Marshall Is.
<b>Defaults</b>	GMT+8			
<b>Command Modes</b>	Global configuration			
<b>Usage Guidelines</b>	N/A			
<b>Examples</b>	Set system time zone to GMT+01:00 Paris (same timezone as Brussels). <pre>router# configure router(config)# clock timezone gmt 1 city Brussels router(config)# exit</pre>			
<b>Error Messages</b>	% Hour offset is out of range.			
	% City Name Error - " "			
	^Parse error			
	^Incomplete command			
<b>Related Commands</b>	show clock			

## ntp remote-server

Use the **ntp remote-server** global configuration command to enable the NTP or SNTP client function and configure the network direction of the remote NTP server. Use the **no** form of this command to return to the default value.

### Synopsis

```
(config)# ntp remote-server <server-addr-1> [<server-addr-2>] [simple]
```

```
(config)# no ntp remote-server
```

<b>Option Description</b>	server-addr-1	IP address or DNS name, max length is 39 characters
	server-addr-2	IP address or DNS name, max length is 39 characters
	simple	Configure Simple Network Time Protocol instead of Network Time Protocol
<b>Defaults</b>	The default configuration contains one time server "time.nist.gov".	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	For the command: no ntp remote-server After revoking the ntp remote server configuration the previously set server information will be kept on the cache and still showing on the clock output. However, the clock source will be set to Local.	
<b>Examples</b>	Set up an NTP server 192.168.1.1 and specify SNTP clock source. router# configure router(config)# ntp remote-server 192.168.1.1 simple router(config)# exit	
<b>Error Messages</b>	^Parse error	
	^Incomplete command	
	% Maximum length of server 1 is 39 % Maximum length of server 2 is 39	
<b>Related Commands</b>	ntp server ntp remote-server-auth ntp authentication-key show ntp-auth-keys	

## ntp server

Use the **ntp server** global configuration command to enable the router as an NTP server. Use the **no** form of this command to return to disable it.

### Synopsis

(config)# **ntp server** [auth]

(config)# **no ntp server** [auth]

<b>Option Description</b>	auth	Specifies to enable/disable client authentication
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Use CLI command <b>ntp authentication-key</b> to create the entry for client's authentication.	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Enable NTP server and client authentication. router# configure router(config)# ntp server router(config)# ntp server auth router(config)# exit</li><li>• Disable NTP server. router# configure router(config)# no ntp server router(config)# exit</li></ul>	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ntp remote-server ntp remote-server-auth ntp authentication-key show ntp-auth-keys	

## ntp remote-server-auth server

Use the **ntp remote-server-auth** global configuration command to specify the key ID to the remote NTP server. Use the **no** form of this command to disable NTP authentication.

### Synopsis

(config)# **ntp remote-server-auth server** {1 | 2} **key** <key-id>

(config)# **no ntp remote-server-auth server** {1 | 2}

<b>Option</b>	1	Specifies NTP Server 1
<b>Description</b>	2	Specifies NTP Server 2
	key	Specifies the authentication key ID
	key-id	The key ID, integer ranges from 1 to 65535
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	To proceed with this command, you need to create at least one authentication key beforehand. The maximum number of Key IDs that can be set is 20.	
<b>Examples</b>	<ul style="list-style-type: none"><li>Specify KeyID(3) to first NTP server. router# configure router(config)# ntp remote-server-auth server 1 key 3 router(config)# exit</li><li>Disable authentication for first NTP server. router# configure router(config)# no ntp remote-server-auth server 1 router(config)# exit</li></ul>	
<b>Error Messages</b>	% Invalid Server, should be (1   2). % Invalid key ID for the server, should be 1~65535. ^Parse error ^Incomplete command	
<b>Related Commands</b>	ntp server ntp remote-server ntp authentication-key show ntp-auth-keys	

## ntp authentication-key

Use the **ntp authentication-key** global configuration command to create a key ID for remote NTP server authentication. Use the **no** form of this command to delete the key for NTP authentication.

### Synopsis

```
(config)# ntp authentication-key <key-id> <key-type> <key>
```

```
(config)# no ntp authentication-key <key-id>
```

<b>Option</b>	key-id	Key ID, integer ranges from 1 to 65535
<b>Description</b>	key-type	Specifies a string for key type: {MD5   SHA512}
	key	Key string. Max. 32 characters
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Create KeyID(3) and key type "SHA512" with key string "moxa1234". router# configure router(config)# ntp authentication-key 3 SHA512 moxa1234 router(config)# exit</li><li>• Delete keyID(3) for NTP server authentication. router# configure router(config)# no ntp authentication-key 3 router(config)# exit</li></ul>	
<b>Error Messages</b>	% Invalid key ID for the server, should be 1~65535.	
	% Invalid Key Type, should be (MD5   SHA512).	
	% Invalid key length (max. 32 characters).	
	% Invalid key ID.	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	ntp server ntp remote-server-auth ntp remote-server show ntp-auth-keys	

## show clock

Use the **show clock** user EXEC command to display the time-related settings.

### **Synopsis**

# **show clock**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show clock Current Time           : Wed Oct 14 11:09:26 2017 Clock Source           : Local Daylight Saving   Start Date           :   End Date              :   Offset                : Time Zone              : GMT+8:00 Time Server             : NTP/SNTP Server        : Disabled NTP Server Auth        : Disabled</pre>
<b>Error Messages</b>	<pre>^Parse error ^Incomplete command</pre>
<b>Related Commands</b>	<pre>clock set clock summer-time clock timezone ntp remote-server ntp server ntp remote-server-auth ntp authentication-key</pre>

## show ntp-auth-keys

Use the **show ntp-auth-keys** user EXEC command to display authentication keys for remote NTP servers.

### **Synopsis**

# **show ntp-auth-keys**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show ntp-auth-keys +-----+   Key ID  Key Type  Key                                 +-----+-----+-----+            1  SHA512  *****                                       2   MD5    *****                                       3  SHA512  *****                            +-----+-----+-----+</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	ntp server ntp remote-server-auth ntp authentication-key ntp remote-server



# Setting Check

## settingcheck

To specify or modify the settingcheck function on the router, use the **settingcheck** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

```
(config)# settingcheck {timer <second> |  
                    l3l7-policy |  
                    nat |  
                    trusted-access}
```

```
(config)# no settingcheck {l3l7-policy |  
                    nat |  
                    trusted-access}
```

<b>Option Description</b>	timer	Specifies a timeout value to wait confirmation from the user.
	second	A timeout in seconds, integer ranges from 10 to 3600 seconds
	l3l7-policy	Enables or disables layer 3-7 policy setting check
	nat	Enables or disables nat setting check
	trusted-access	Enables or disables trusted-access setting check
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Enabling the SettingCheck function will execute these new policy changes temporarily until doubly confirmed by the user. If the user does not click the confirm button, the Industrial Secure Router will revert to the previous setting.	
<b>Examples</b>	Specify a timer (180 seconds) to check firewall policy. router# configure router(config)# settingcheck timer 180 router(config)# settingcheck l3l7-policy router(config)# exit	
<b>Error Messages</b>	% Timer range must be 10 - 3600.	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show settingcheck	

## show settingcheck

To check the settings of settingcheck function, use the **show settingcheck**.

### **Synopsis**

# **show settingcheck**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router# show settingcheck Setting Check Layer 3-7 Policy : Disable NAT Policy : Disable Trusted Access List : Disable Timer : 180 seconds
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	settingcheck

# Security

## Login Policy

### aaa authentication

To set the login banner and fail message, use the **aaa authentication** global configuration command. To return to the default string, use the **no** form of this command.

#### Synopsis

```
(config)# aaa authentication {banner <text-banner> |  
                                fail-message <text-fail-message>}
```

```
(config)# no aaa authentication {banner |  
                                fail-message}
```

<b>Option</b>	banner	Specifies banner
<b>Description</b>	text-banner	A text string to be displayed on banner, max length is 512 characters
	fail-message	Specifies fail message, the max length is 512 characters
	text-fail-message	A text string to be displayed while authentication failure.
<b>Defaults</b>	Empty string.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• Maximum length of text-banner or text-fail-message is 512.</li><li>• The text string comprises characters including <b>a-z, A-Z, 0-9 or . - _ @ ! # \$ % ^ &amp; * ( )</b>. Uses <b>\\</b> instead to represent a whitespace character.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Specify/modify the banner to "Welcome to use MOXA router". router# configure router(config)# aaa authentication banner Welcome\\to\\use\\MOXA\\router router(config)# exit</li><li>• Specify/modify the fail-message to "Login Failed". router# configure router(config)# aaa authentication fail-message Login\\Failed router(config)# exit</li></ul>	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show running config	

## login-lockout

To specify or modify the login lockout function on the router, use the **login-lockout** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

```
(config)# login-lockout [retry-threshold <threshold>|  
                        lockout-time <minute>]
```

```
(config)# no login-lockout [{retry-threshold |  
                             lockout-time}]
```

<b>Option Description</b>	retry-threshold	Specifies the maximum number of login retries before the account is locked out.
	threshold	Integer ranges from 1 to 10 times.
	lockout-time	Specifies the lockout duration (in minutes) during which a locked out account will be unable to log in.
	minute	Integer ranges from 1 to 10 minutes.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	This command applies to telnet, SSH and the web interface.	
<b>Examples</b>	Set Login lockout for 5 attempts and 10 minutes lockout. router# configure router(config)# login-lockout retry-threshold 5 router(config)# login-lockout lockout-time 10 router(config)# exit	
<b>Error Messages</b>	% login lockout threshold should between 1~10	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show running-configuration	

## ip auto-logout

When the user does not touch the web management interface for a defined period of time, the management interface will logout automatically. To specify this feature, use the **ip auto-logout** global configuration command.

### Synopsis

```
(config)# ip auto-logout <minute>
```

<b>Option Description</b>	minute	A time period in minutes, integer ranges from 0 to 1440 minutes
<b>Defaults</b>	The default value is 5 minutes	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<minute>: 0 for disable, or 1 ~ 1440 minutes.	
<b>Examples</b>	Specify Auto Logout for 120 minutes. router# configure router(config)# ip auto-logout 120 router(config)# exit	
<b>Error Messages</b>	% Switch auto-logout interval should be 0(disable) or 1~1440mins !!!	
	^Parse error	
<b>Related Commands</b>	N/A	

# Trusted Access

## interface trusted-access

To specify or modify accessible IP list, use the **interface trusted-access** global configuration command. To disable trusted access, use the **no** form of this command.

### Synopsis

```
(config)# interface trusted-access [lan [<ip> <netmask> [enable | disable]]]
```

```
(config)# no interface trusted-access [lan [<ip> <netmask>]]
```

<b>Option Description</b>	lan	Specifies LAN interface
	ip	IP address
	netmask	Subnet mask for this IP address
	enable	Enables specified accessible IP address
	disable	Disables specified accessible IP address
<b>Defaults</b>	Accessible IP list is enabled by default. Accept all connection from LAN port is enabled by default.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	When the accessible IP list is enabled, only addresses on the list will be allowed access to the router.	
<b>Examples</b>	<ul style="list-style-type: none"><li>Disable trusted-access to allow connection from all IP addresses. router# configure router(config)# no interface trusted-access. router(config)# exit</li><li>Disable "Accept all connection from LAN port" and specify 192.168.127.0/24 can access this router. router# configure router(config)# no interface trusted-access lan router(config)# interface trusted-access lan 192.168.127.0 255.255.255.0 enable router(config)# exit</li></ul>	
<b>Error Messages</b>	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show interfaces trusted-access settingcheck	

## show interfaces trusted-access

Use the **show interfaces trusted-access** EXEC command to display the setting of trusted access function.

### Synopsis

# **show interfaces trusted-access**

<b>Option Description</b>	N/A	
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Display trusted-access settings. router # show interfaces trusted-access Trusted Access List : Enable Severity : <0> Emergency Syslog : Disable Trap : Disable Accept All LAN : Enable Index State IP Netmask ----- 1 Disable 192.168.127.1 255.255.255.255	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	interface trusted-access	

## Certificate Management

### sslcertgen

Use the sslcertgen privileged command to generate a new certificate for web login (HTTPS) and configuration file signatures.

### Synopsis

# **sslcertgen**

<b>Option Description</b>	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	Few minutes may be required. Web will be unavailable temporarily until it finished.	
<b>Examples</b>	N/A	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	N/A	

## sshkeygen

Use the sshkeygen privilege command to generate a new encryption key for SSH connection.

### Synopsis

# sshkeygen

<b>Option Description</b>	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	Few minutes may be required. Web will be unavailable temporarily until it finished.	
<b>Examples</b>	N/A	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	N/A	

## Authentication

### auth mode

To specify or modify authentication protocol, use the **auth mode** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

```
(config)# auth mode {local |  
                    radius [local]}  
                    tacacs [local]}
```

```
(config)# no auth mode
```

<b>Option Description</b>	local	Specifies local authentication
	radius	Specifies RADIUS authentication
	radius local	Specifies to use RADIUS server and, in case of connection failure or no response from the RADIUS server, switches to the local database for authentication.
	tacacs	Specifies TACACS+ authentication
	tacacs local	Specifies to use TACACS+ server and, in case of connection failure or no response from the TACACS+ server, switches to the local database for authentication.
<b>Defaults</b>	local	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	If exclusively relying on remote authentication servers like RADIUS or TACACS+ without a local database as backup, failure or unavailability of the remote server will prevent login through network services (HTTP/HTTPS/Telnet/SSH). The only access method would then be through the console port.	
<b>Examples</b>	Authentication occurs sequentially in RADIUS and then locally. router# configure router(config)# auth mode radius local router(config)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show auth radius auth radius auth tacacs	

## auth radius

To specify or modify the remote RADIUS authentication server, use the **auth radius** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

```
(config)# auth radius {server {primary <server-ip> port <server-port> key <shared-key> |
backup <server-ip> port <server-port> key <shared-key>} |
auth-type {pap |
chap |
peap-mschapv2}}
```

```
(config)# no auth radius server {primary | backup}
```

<b>Option</b>	server	Specifies RADIUS primary or backup servers
<b>Description</b>	primary	Specifies primary RADIUS authentication server
	server-ip	IP address of the RADIUS authentication server
	port	Specifies a port number of the remote RADIUS Server
	server-port	Port of the RADIUS authentication server, integer ranges from 1 to 65535, default value is 1812
	key	Specifies a shared-key of the remote RADIUS Server
	shared-key	Shared key of the RADIUS authentication server, 1 to 64 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # \$ % & * ( ) . + = { } [ ]   : ; , ~.
	backup	Specifies backup RADIUS authentication server
	auth-type	Specifies type of authentication
	pap	PAP
	chap	CHAP
	peap-mschapv2	PEAP-MSCHAPv2
<b>Defaults</b>	N/A	
<b>Command</b>	Global configuration	
<b>Modes</b>		
<b>Usage</b>	N/A	
<b>Guidelines</b>		
<b>Examples</b>	Specify and enable the primary RADIUS,Local server (192.168.1.5), port (2812) and shared key (radius-key). <pre>router# configure router(config)# auth radius server primary 192.168.1.5 port 2812 key radius-key router(config)# auth mode radius local router(config)# exit</pre>	
<b>Error</b>	% Radius index must be 1~2	
<b>Messages</b>	% Must be greater than 0 and smaller than 65536	
	% The length of Shared Key must be greater than 0 and smaller than 65.	
	^Parse error	
	^Incomplete command	
<b>Related</b>	show auth radius	
<b>Commands</b>	auth mode	



## show auth radius

To check the settings of RADIUS server, use the **show auth radius** command.

### Synopsis

# **show auth radius**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show auth radius  Radius information:   Authentication Type      : Local   Type                     : EAP-PEAP MSCHAPv2   Primary Auth server     : 192.168.1.5   Primary Server Port     : 2812   Primary Shared key      : *****   Backup Auth server      :   Backup Server Port     : 1812   Backup Shared key       : *****</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	auth mode auth radius

## auth tacacs

To specify or modify the remote TACACS+ authentication server, use the auth tacacs global configuration command. To return to the default, use the no form of this command.

### Synopsis

```
(config)# auth tacacs server {primary | backup} <server-ip> port <server-port>
key <shared-key> timeout <second> retransmit <times>
auth-type {pap |
chap |
ascii}}
```

```
(config)# no auth tacacs server {primary | backup}
```

<b>Option Description</b>	server	Specifies TACACS+ primary or backup servers
	primary	Specifies primary TACACS+ authentication server
	server-ip	IP address of the TACACS+ authentication server
	port	Specifies a port number of the remote TACACS+ Server
	server-port	Port of the TACACS+ authentication server. Integer ranges from 1 to 65535. Default value is 49.
	key	Specifies a shared-key of the remote TACACS+ Server
	shared-key	Shared key of the TACACS+ authentication server. Valid ranges are 1 to 64 characters and must consist of the characters a-z, A-Z, 0-9 or - @ ! # \$ % & * ( ) . + = { } [ ]   : ; , ~.
	timeout	Specifies a time period (in seconds) until which a client waits for a response from the server before re-transmitting the request.
	second	Integer value ranges from 5 to 120 seconds. Default value is 5.
	retransmit	Specifies the maximum number of attempts the client undertakes to contact the server.
	times	Integer value ranges from 0 to 5. Default value is 1.
	backup	Specifies backup TACACS+ authentication server
	auth-type	Specifies the type of authentication (default is CHAP)
	pap	PAP
	chap	CHAP
	ascii	ASCII
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify and enable the primary TACACS+, Local server (192.168.1.6), port (49), shared key (tacacs-key), timeout(5), retransmission (3) and auth-type (CHAP). <pre>router# configure router(config)# auth tacacs server primary 192.168.1.6 port 49 key tacacs-key timeout 5 retransmit 3 authtype chap router(config)# auth mode tacacs local router(config)# exit</pre>	
<b>Error Messages</b>	% Invalid parameter!	
	% Port must be greater than 0 and smaller than 65536	
	% The length of Shared Key must be greater than 0 and smaller than 65.	
	% Timeout must be 5~120	
	% Retransmit must be 0~5	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show auth tacacs auth mode	

## show auth tacacs

To check the settings of TACACS+ server, use the show auth tacacs command.

### Synopsis

#### # show auth tacacs

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show auth tacacs  TACACS+ information:   Primary Auth server       : 192.168.1.6   Primary Server Port      : 49   Primary Shared key       : *****   Primary Type              : CHAP   Primary Timeout          : 5 (sec)   Primary Retransmit       : 3   Backup Auth server       : 0.0.0.0   Backup Server Port       : 49   Backup Shared key        : *****   Backup Type               : CHAP   Backup Timeout           : 5 (sec)   Backup Retransmit        : 1</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	auth mode auth tacacs

## Port-based access control (IEEE 802.1X)

### interface ethernet dot1x

To enable 802.1x port-based access control function, use the **interface ethernet** global configuration command and **dot1x** sub-level configuration command set. To disable this function, use the **no** form of this command.

#### Synopsis

```
(config)# interface ethernet <mod-port>
(config-if)# dot1x {auth |
                   reauth}
```

```
(config-if)# no dot1x
```

<b>Option</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
<b>Description</b>	dot1x	Specifies 802.1x settings.
	auth	Enables 802.1x port authentication function
	reauth	802.1x port re-authenticate immediately
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify PORT3 to enable port-based access control. router# configure router(config)# interface ethernet 1/3 router(config-if)# dot1x auth router(config-if)# exit	
<b>Error Messages</b>	% Illegal parameter % Port doesn't enable 802.1x ^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces ethernet show dot1x	

## dot1x radius

To specify or modify the RADIUS server settings for 802.1X port access control, use the **dot1x radius** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

```
(config)# dot1x radius {1st-server | 2nd-server} {server-ip <ip> |
                                server-port <port> |
                                shared-key <key>}
```

```
(config)# no dot1x radius {both |
                                1st-server |
                                2nd-server}
```

<b>Option Description</b>	1st-server	Specifies first RADIUS authentication server.
	2nd-server	Specifies second RADIUS authentication server.
	server-ip	Specifies IP address of the RADIUS authentication server
	ip	IP address
	server-port	Specifies port of the RADIUS authentication server
	port	Port number, integer ranges from 1 to 65535
	shared-key	Specifies the shared key of the RADIUS authentication server
	key	Shared key, 1 to 64 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # \$ % & * ( ) . + = { } [ ]   : ; , ~.
	both	Disables both first and second RADIUS servers
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify the first RADIUS server (192.168.1.6), port (3812) and shared key (rad-ser-key). <pre>router# configure router(config)# dot1x radius 1st-server server-ip 192.168.1.6 router(config)# dot1x radius 1st-server server-port 3812 router(config)# dot1x radius 1st-server shared-key rad-ser-key router(config)# exit</pre>	
<b>Error Messages</b>	% Must be greater than 0 and smaller than 65536	
	% The length of Shared Key must be greater than 0 and smaller than 65.	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	<pre>show dot1x show dot1x all show dot1x interfaces show dot1x local-userdb show dot1x radius</pre>	

## dot1x auth

To specify or modify the RADIUS server settings for 802.1X port access control, use the **dot1x radius** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

```
(config)# dot1x auth {local |  
                    radius |  
                    radius-local}
```

<b>Option Description</b>	local	Specifies local database as user account database for 802.1X authentication.
	radius	Specifies RADIUS authentication server.
	radius-local	Specifies RADIUS as the first authentication sever; local database as the second priority.
<b>Defaults</b>	Local	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify Radius server as database for authentication. router# configure router(config)# dot1x auth radius router(config)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show dot1x show dot1x all show dot1x interfaces show dot1x local-userdb show dot1x radius	

## dot1x local-userdb

To add or modify local user for 802.1X authentication, use the **dot1x local-userdb** global configuration command. To delete a local user from the local database, use the **no** form of this command.

### Synopsis

(config)# **dot1x local-userdb username** <user-name> **password** <pwd>

(config)# **no dot1x local-userdb username** <user-name>

<b>Option Description</b>	username	Specifies user name in local database
	user-name	User name in a local database, it can have a maximum length of 32 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # \$ % ^ & * ( ) . / .
	password	Specifies user password
	pwd	User password, it can have a maximum length of 64 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # \$ % & * ( ) . + = { } [ ]   : ; , ~ .
<b>Defaults</b>	Local	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify a user name (locusr1) with password (locusrpwd) in a database for authentication. router# configure router(config)# dot1x local-userdb username locusr1 password locusrpwd router(config)# exit	
<b>Error Messages</b>	Username is not in database	
	Username or password exceed maximum length	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show dot1x show dot1x all show dot1x interfaces show dot1x local-userdb show dot1x radius	

## dot1x reauth

To enable or configure re-auth period for 802.1X authentication, use the **dot1x reauth** global configuration command. To disable re-auth or return period to the default setting, use the **no** form of this command.

### Synopsis

(config)# **dot1x reauth** [period <second>]

(config)# **no dot1x reauth** [period]

<b>Option</b>	period	Specify the re-authentication period (in seconds).
<b>Description</b>	second	Ranges from 60 to 65535 seconds
<b>Defaults</b>	3600	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Enables re-auth before specifies re-authentication period.	
<b>Examples</b>	Specify a re-auth period (1800 seconds) for 802.1X authentication and enable it. router# configure router(config)# dot1x reauth period 1800 router(config)# exit	
<b>Error Messages</b>	% Invalid Re-Auth Period!!! Must not be smaller than 60 or greater than 65535 ^Parse error ^Incomplete command	
<b>Related Commands</b>	show dot1x show dot1x all show dot1x interfaces show dot1x local-userdb show dot1x radius	



## show dot1x

To check the 802.1X settings on the router, use the **show dot1x** command.

### Synopsis

```
# show dot1x [{all |
               interfaces ethernet <mod-port> |
               local-userdb |
               radius}]
```

<b>Option Description</b>	all	Specifies to display 802.1X all interface information
	interfaces ethernet	Specifies to display 802.1X specific interface information
	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	local-userdb	Specifies to display current local database
	radius	Specifies to display 802.1x radius settings
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router # show dot1x Dot1x Info  Database Option : Local Re-Auth          : Enable Re-Auth Period  : 3600  1st Auth server ----- IP/name          : 192.168.127.253 Port             : 1812 Shared key       : 11111111112222222222333333333333  2nd Auth server ----- IP/name          : Port             : 1812 Shared key       :  Port 802.1X Enable ----- 1/1  Disabled 1/2  Disabled 1/3  Disabled 1/4  Disabled 1/5  Disabled 1/6  Disabled 1/7  Disabled 1/8  Disabled</pre>	
<b>Error Messages</b>	<pre>^Parse error ^Incomplete command % Illegal parameter % Unavailable module</pre>	
<b>Related Commands</b>	<pre>dot1x radius dot1x auth dot1x local-userdb dot1x reauth</pre>	

# Security Notification

## security-notification

To enable MXview Alert Notification features on the router, use the **security-notification** global configuration command. To disable the feature, use the **no** form of this command.

### Synopsis

```
(config)# security-notification {event-accessviolation |  
                                event-loginfail |  
                                event-firewall |  
                                event-dosattack}
```

```
(config)# no security-notification {event-accessviolation |  
                                    event-loginfail |  
                                    event-firewall |  
                                    event-dosattack}
```

<b>Option Description</b>	event-accessviolation	Specifies access violation event notification
	event-loginfail	Specifies login fail event notification
	event-firewall	Specifies firewall event notification
	event-dosattack	Specifies DoS attack event notification
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable security notification for Login fail event. router# configure router(config)# security-notification event-loginfail router(config)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show security-notification	

## clear security-notification

To clear MXView Alert Notification and status, use the **clear security-notification** global configuration command.

### Synopsis

```
(config)# clear security-notification [status]
```

<b>Option Description</b>	status	Specifies to clear security notification information status
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	N/A	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show security-notification security-notification	

## show security-notification

To check the security-notification settings on the router, use the **show security-notification** command.

### Synopsis

```
# show security-notification {setting |
                             status}
```

<b>Option</b>	setting	Specifies to display security notification settings
<b>Description</b>	status	Specifies to display security notification status
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# show security-notification setting ===== Security Notification Configuration =====   Firewall Event Notification           : Enable   DoS Attack Event Notification         : Enable   Access Violation Event Notification   : Enable   Login Fail Event Notification         : Enable router# show security-notification status ===== Security Notification Status =====   Firewall Event Notification           : Safe   DoS Attack Event Notification         : Safe   Access Violation Event Notification   : Safe   Login Fail Event Notification         : Safe =====</pre>	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	security-notification	

## Diagnostics

### System Status

#### show usage

To check the CPU usage and memory utilization on the router, use the **show usage** command.

### Synopsis

```
# show usage
```

<b>Option</b>	N/A	
<b>Description</b>		
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# show usage CPU:  2.79% Mem: 328056K used, 1703484K free, 117036K shrd, 996K buff, 117344K cached</pre>	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	^Incomplete command	

<b>Related Commands</b>	N/A
-------------------------	-----

## Network Status

### show interfaces counters

To check the packet counter information for all ports including trunk ports, use the **show interfaces counters** command.

#### Synopsis

# **show interfaces counters**

<b>Option Description</b>	N/A																																																			
<b>Defaults</b>	N/A																																																			
<b>Command Modes</b>	Privileged EXEC / User EXEC																																																			
<b>Usage Guidelines</b>	N/A																																																			
<b>Examples</b>	<p>Display packet counter information for all ports.</p> <pre>router# show interfaces counters</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>Tx Packets</th> <th>Rx Packets</th> </tr> <tr> <th colspan="3">-----</th> </tr> </thead> <tbody> <tr> <td>1/ 1</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/ 2</td> <td>442490</td> <td>673826</td> </tr> <tr> <td>1/ 3</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/ 4</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/ 5</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/ 6</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/ 9</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/10</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/11</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/12</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/13</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/14</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/15</td> <td>0</td> <td>0</td> </tr> <tr> <td>1/16</td> <td>0</td> <td>0</td> </tr> <tr> <td>Trk1</td> <td>7273</td> <td>6897</td> </tr> </tbody> </table>	Port	Tx Packets	Rx Packets	-----			1/ 1	0	0	1/ 2	442490	673826	1/ 3	0	0	1/ 4	0	0	1/ 5	0	0	1/ 6	0	0	1/ 9	0	0	1/10	0	0	1/11	0	0	1/12	0	0	1/13	0	0	1/14	0	0	1/15	0	0	1/16	0	0	Trk1	7273	6897
Port	Tx Packets	Rx Packets																																																		
-----																																																				
1/ 1	0	0																																																		
1/ 2	442490	673826																																																		
1/ 3	0	0																																																		
1/ 4	0	0																																																		
1/ 5	0	0																																																		
1/ 6	0	0																																																		
1/ 9	0	0																																																		
1/10	0	0																																																		
1/11	0	0																																																		
1/12	0	0																																																		
1/13	0	0																																																		
1/14	0	0																																																		
1/15	0	0																																																		
1/16	0	0																																																		
Trk1	7273	6897																																																		
<b>Error Messages</b>	^Parse error ^Incomplete command																																																			
<b>Related Commands</b>	show interfaces ethernet show interfaces trunk																																																			

## lldp

Use the **lldp enable** global configuration command to enable LLDP. To stop LLDP or disable LLDP Ring bypass, use the **no** form of this command.

### Synopsis

```
(config)# lldp {enable |  
                timer <seconds> |  
                enable-bypass}
```

```
(config)# no lldp {enable | timer | enable-bypass}
```

<b>Option</b>	enable	Enables/disables LLDP feature
<b>Description</b>	timer	Specifies a Message Transmit Interval
	seconds	Ranges from 5 to 32768 seconds.
	enable-bypass	Specifies to enable or disable the LLDP Ring port bypass feature
<b>Defaults</b>	LLDP is enabled in factory default. Transmission frequency of LLDP updates is 30 seconds.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	In the case of TN router acts as a member of the Ring topology and Moxa Auto-Config mechanism is required, it's vital to enable "enable-bypass" to ensure the entire Auto-Config process is completed.	
<b>Examples</b>	Enable LLDP and specify timer (60 seconds) and enable Ring bypass feature. router# configure router(config)# lldp timer 60 router(config)# lldp enable router(config)# lldp enable-bypass router(config)# exit	
<b>Error Messages</b>	^Parse error	
	^Incomplete command	
	% Time interval must be 5 - 32768	
<b>Related Commands</b>	show lldp	

## show lldp

Use the **show lldp** command to display the LLDP settings and the LLDP neighbor information.

### Synopsis

# **show lldp** [entry]

<b>Option Description</b>	entry	LLDP entries
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# show lldp LLDP Enable : Enable LLDP Ring Port Bypass : Enable Message Transmit Interval : 60  router# show lldp entry  Port 3 Neighbor ID : 00:90:e8:0a:0a:0a Neighbor Port 3 Neighbor Port Descript : 100TX,RJ45. Neighbor System : Managed Redundant Router 00000  Port 4 Neighbor ID : 00:90:e8:0a:0a:0a Neighbor Port 2 Neighbor Port Descript : 100TX,RJ45. Neighbor System : Managed Redundant Router 00000	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	lldp	

## show arp

To check the ARP cache on the router, use the **show arp** command.

### Synopsis

# **show arp**

<b>Option Description</b>	N/A	
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# show arp Address                      Hardware Addr                      Interface 192.168.127.1                      50:7b:9d:e1:82:5a                      LAN20	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	N/A	

## Event Logs and Notifications

### copy event-log

To export different types of event-logs to a storage device or a remote file server, use the **copy event-log** privileged command on the router.

#### Synopsis

```
# copy event-log <event-db> <method> [<ip> [<account> <password>]]
```

<b>Option Description</b>	event-db	Specifies the integer of the event log type. The following types are available: {System(0)   VPN(1)   Trust-Access(2)   Malformed-Packets(3)   DOS-Policy(4)   L3L7-Policy(6)   Protocol-Filter-Policy(7)   ADP(8)   IPS(9)   Session-Control(10)   L2-policy(11)}
	method	Specifies an integer for below method: {TFTP(1)   USB(2)   SCP(3)   SFTP(4)}
	ip	IP address of the file server
	account	Specifies the user name to login remote SCP or SFTP file server
	password	Specifies the password for authentication.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>When selecting method "TFTP(1)", there is no need for &lt;account&gt; and &lt;password&gt; to complete the command.</li> <li>When selecting method "USB(2)", there is no need for &lt;ip&gt;, &lt;account&gt; and &lt;password&gt; to complete the command.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Export System event-logs to USB storage device. router# copy event-log 0 2 Exported Event Log File: system.json Event Log File is exporting now, please wait. Event Log File Exporting is Complete. router#</li> <li>Export System event-logs to a remote SCP server. router# copy event-log 0 3 192.168.127.102 moxa moxa Server IP: 192.168.127.102 Exported Event Log File: system.json Event Log File is exporting now, please wait. Event Log File Exporting is Complete. router#</li> </ul>	
<b>Error Messages</b>	% The event log DB only allows 0 ~ 11	
	% Only method 1 ~ 4 are supported	
	% TFTP/SCP/SFTP needs host IP address!	
	No USB Device	
	Event Log File Exporting Failed!	
	% SCP/SFTP needs to key-in username!	
	^Parse error	
^Incomplete command		
<b>Related Commands</b>	auto-backup event-log	

## warning-notification system-event

To specify or modify warning notification for system events, use the **warning-notification system-event** global configuration command. To return to default settings, use the **no** form of this command.

### Synopsis

```
(config)# warning-notification system-event <events> {action <action-index> |  
                                         severity <severity-level> |  
                                         active}
```

```
(config)# no warning-notification system-event <events> active
```

<b>Option Description</b>	events	Specifies one of below event names: { <b>cold-start</b>   <b>warm-start</b>   <b>config-changed</b>   <b>pwr1-trans-on</b>   <b>pwr2-trans-on</b>   <b>pwr1-trans-off</b>   <b>pwr2-trans-off</b>   <b>auth-fail</b>   <b>topology-changed</b>   <b>coupling-changed</b>   <b>master-changed</b>   <b>vrrp-state-changed</b>   <b>dot1x-auth-fail</b>   <b>poe-pd-on</b>   <b>poe-pd-off</b>   <b>poe-exceed-system-threshold</b>   <b>poe-fetbad</b>   <b>poe-over-temperature</b>   <b>poe-vee-uvlo</b>   <b>poe-pd-over-current</b>   <b>poe-pd-check-fail</b>   <b>poe-exceed-power-budget</b>   <b>vpn-connected</b>   <b>vpn-disconnected</b>   <b>firewall-policy-changed</b>   <b>firmware-upgrade-success</b>   <b>firmware-upgrade-failure</b>   <b>log-service-ready</b> }
	action	Configure actions of events
	action-index	Specifies an integer for: {Trap only(1)   Email only(2)   Trap+Email(3)   Syslog only(4)   Trap+Syslog(5)   Email+Syslog(6)   Trap+Email+Syslog(7)   Relay1 only(8)   Trap+Relay1(9)   Email+Relay1(10)   Trap+Email+Relay1(11)   Syslog+Relay1(12)   Trap+Syslog+Relay1(13)   Email+Syslog+Relay1(14)   Trap+Email+Syslog+Relay1(15)   None(0)}
	severity	Configure event severity
	severity-level	Specifies an integer for: {Emergency(0)   Alert(1)   Critical(2)   Error(3)   Warning(4)   Notice(5)   Information(6)   Debug(7)}
	active	Activate event waring
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>Configure SNMP Trap in advance when taking action of events { Trap only(1)   Trap+Email(3)   Trap+Syslog(5)   Trap+Email+Syslog(7)   Trap+Relay1(9)   Trap+Email+Relay1(11)   Trap+Syslog+Relay1(13)   Trap+Email+Syslog+Relay1(15) }</li> <li>Configure Email server in advance when taking action of events { Email only(2)   Trap+Email(3)   Email+Syslog(6)   Trap+Email+Syslog(7)   Email+Relay1(10)   Trap+Email+Relay1(11)   Email+Syslog+Relay1(14)   Trap+Email+Syslog+Relay1(15) }</li> <li>Configure Syslog server in advance when taking action of events { Syslog only(4)   Trap+Syslog(5)   Email+Syslog(6)   Trap+Email+Syslog(7)   Syslog+Relay1(12)   Trap+Syslog+Relay1(13)   Email+Syslog+Relay1(14)   Trap+Email+Syslog+Relay1(15) }</li> </ul>	
<b>Examples</b>	Enable "warm start" event notification and send warning message to the Syslog server with severity DEBUG. <pre>router# configure router(config)# warning-notification system-event warm-start action 4 router(config)# warning-notification system-event warm-start severity 7 router(config)# warning-notification system-event warm-start active router(config)# exit</pre>	
<b>Error Messages</b>	% Invalid severity type	
	% Invalid action value or non-support this combination action	
	^Parse error	



	^Incomplete command
<b>Related Commands</b>	snmp-server host snmp-server trap-mode email-warning logging <ip-addr>

## warning-notification system-event topology-changed

Set topology change event configuration including enabling, notification targets, and event severity.

### Synopsis

```
(config)# warning-notification system-event topology-changed { action <combination> | severity <type> | active }
```

```
(config)# no warning-notification system-event topology-changed active
```

Option	action	Enable Action setting
<b>Description</b>	combination	<ul style="list-style-type: none"> <li>• SNMP Trap Server only(1)</li> <li>• Email only(2)</li> <li>• SNMP Trap Server+Email(3)</li> <li>• Syslog only(4)</li> <li>• SNMP Trap Server+Syslog Server(5)</li> <li>• Email+Syslog Server(6)</li> <li>• SNMP Trap Server+Email+Syslog Server(7)</li> <li>• Relay1 only(8)</li> <li>• SNMP Trap Server+Relay1(9)</li> <li>• Email+Relay1(10)</li> <li>• SNMP Trap Server+Email+Relay1(11)</li> <li>• Syslog+Relay1(12)</li> <li>• SNMP Trap Server+Syslog Server+Relay1(13)</li> <li>• Email+Syslog Server+Relay1(14)</li> <li>• SNMP Trap Server+Email+Syslog Server+Relay1(15)</li> <li>• SMS(32)</li> <li>• SNMP Trap Server+SMS(33)</li> <li>• Email+SMS(34)</li> <li>• SNMP Trap Server+Email+SMS(35)</li> <li>• Syslog Server+SMS(36)</li> <li>• SNMP Trap Server+Syslog Server+SMS(37)</li> <li>• Email+Syslog Server+SMS(38)</li> <li>• SNMP Trap Server+Email+Syslog Server+SMS(39)</li> <li>• Relay1+SMS(40)</li> <li>• SNMP Trap Server+Relay1+SMS(41)</li> <li>• Email+Relay1+SMS(42)</li> <li>• SNMP Trap Server+Email+Relay1+SMS(43)</li> <li>• Syslog Server+Relay1+SMS(44)</li> <li>• SNMP Trap Server+Syslog Server+Relay1+SMS(45)</li> <li>• Email+Syslog Server+Relay1+SMS(46)</li> <li>• SNMP Trap Server+Email+Syslog Server+Relay1+SMS(47)</li> <li>• None(0)</li> </ul>
	severity	Severity setting
	type	<ul style="list-style-type: none"> <li>• Emergency(0)</li> <li>• Alert(1)</li> <li>• Critical(2)</li> <li>• Error(3)</li> <li>• Warning(4)</li> <li>• Notice(5)</li> <li>• Information(6)</li> <li>• Debug(7)</li> </ul>
	active	Activate
	no	Negate command or set to default

<b>Defaults</b>	N/A
<b>Command Modes</b>	Configuration mode
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre> Firewall/VPN Router 00000# configure Firewall/VPN Router 00000(config)# warning-notification system-event topology-changed action 0 Firewall/VPN Router 00000(config)# warning-notification system-event topology-changed severity 4 Firewall/VPN Router 00000(config)# warning-notification system-event topology-changed active Firewall/VPN Router 00000(config)# no warning-notification system- event topology-changed active </pre>
<b>Error messages</b>	% Invalid action value or non-support this combination action % Invalid severity type
<b>Related Commands</b>	N/A

## interface ethernet warning-notification port-event

To specify or modify warning notification for port events, use the **interface ethernet** global configuration command and **warning-notification port-event** sub-level configuration command set. To return to default settings, use the **no** form of this command.

### Synopsis

```

(config)# interface ethernet <mod-port>
(config-if)# warning-notification port-event {active |
severity <severity-level>|
event {link-on | link-off} |
action <action-index>}

(config-if)# no warning-notification port-event {active |
event {link-on | link-off}}

```

<b>Option Description</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	port-event	Specifies port events for notification.
	active	Enables port event notification
	severity	Specifies event severity.
	severity-level	Specifies an integer for: {Emergency(0)   Alert(1)   Critical(2)   Error(3)   Warning(4)   Notice(5)   Information(6)   Debug(7)}
	event	Specifies link on/off events
	link-on	Link on
	link-off	Link off
	action	Specifies actions for port event notification
	action-index	Specifies an integer for: {Trap only(1)   Email only(2)   Trap+Email(3)   Syslog only(4)   Trap+Syslog(5)   Email+Syslog(6)   Trap+Email+Syslog(7)   Relay1 only(8)   Trap+Relay1(9)   Email+Relay1(10)   Trap+Email+Relay1(11)   Syslog+Relay1(12)   Trap+Syslog+Relay1(13)   Email+Syslog+Relay1(14)   Trap+Email+Syslog+Relay1(15)   None(0)}
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>Configure SNMP Trap in advance when taking action of events { Trap only(1)   Trap+Email(3)   Trap+Syslog(5)   Trap+Email+Syslog(7)   Trap+Relay1(9)  </li> </ul>	

	<pre>Trap+Email+Relay1(11)   Trap+Syslog+Relay1(13)   Trap+Email+Syslog+Relay1(15) }</pre> <ul style="list-style-type: none"> <li>• Configure Email server in advance when taking action of events { Email only(2)   Trap+Email(3)   Email+Syslog(6)   Trap+Email+Syslog(7)   Email+Relay1(10)   Trap+Email+Relay1(11)   Email+Syslog+Relay1(14)   Trap+Email+Syslog+Relay1(15) }</li> <li>• Configure Syslog server in advance when taking action of events { Syslog only(4)  Trap+Syslog(5)   Email+Syslog(6)   Trap+Email+Syslog(7)   Syslog+Relay1(12)   Trap+Syslog+Relay1(13)   Email+Syslog+Relay1(14)   Trap+Email+Syslog+Relay1(15) }</li> </ul>
<b>Examples</b>	<pre>Enable Port-3 link-on event notification and send warning message to the Syslog server with severity DEBUG. router# configure router(config)# interface ethernet 1/3 router(config-if)# warning-notification port-event event link-on router(config-if)# warning-notification port-event action 4 router(config-if)# warning-notification port-event severity 7 router(config-if)# warning-notification port-event active router(config-if)# exit</pre>
<b>Error Messages</b>	<pre>% Invalid severity type % Invalid action value or non-support this combination action ^Parse error ^Incomplete command</pre>
<b>Related Commands</b>	<pre>show interfaces ethernet snmp-server host snmp-server trap-mode email-warning logging &lt;ip-addr&gt;</pre>

## logging-capacity

To specify or modify the logging capacity and oversize action on the router, use the **logging-capacity** global configuration command. To disable warning notification, use the **no** form of this command.

### Synopsis

```
(config)# logging-capacity {<threshold> |
                        snmp-trap-warning |
                        email-warning |
                        over-size-action {overwrite-oldest |
                        stop-recording }} {<category-name>}

(config)# no logging-capacity [snmp-trap-warning | email-warning] {<category-name>}
```

<b>Option Description</b>	threshold	The threshold to trigger a warning notification. Ranges from 50 to 100.
	category-name	Specifies the function event category to configure logging capacity parameters for. The following function event categories are available: {system   vpn   trusted-access   malformed-packets   dos-policy   layer-3-7-policy   protocol-filter-policy   adp   ips   session-control   layer2-filter }
	snmp-trap-warning	Specifies notification via SNMP Trap.
	email-warning	Specifies notification via email.
	over-size-action	Specifies action when the log threshold is exceeded.
	overwrite-oldest	Specifies to overwrite the oldest log.
	stop-recording	Specifies to stop record event logs.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	

<b>Examples</b>	Specify and enable threshold to 60 % for System events and send a warning via SNMPT Trap. Overwrite the oldest log when log threshold is exceeded. <pre>router# configure router(config)# logging-capacity 60 system router(config)# logging-capacity snmp-trap-warning system router(config)# no logging-capacity email-warning system router(config)# logging-capacity over-size-action overwrite-oldest system router(config)# exit</pre>
<b>Error Messages</b>	^Parse error
	^Incomplete command
	% Event log capacity threshold should between 50~100
<b>Related Commands</b>	% Error Name:
	show logging-capacity

## email-warning

To specify or modify email server for warning notification, use the **email-warning** global configuration command. To return to default settings, use the **no** form of this command.

### Synopsis

```
(config)# email-warning {server <ip> <port> |
mail-address <mail-index> <rcv-email> |
account <name> [<password>]
sender <sender-email>}
```

```
(config)# no email-warning {server |
account |
sender |
mail-address <mail-index>}
```

<b>Option Description</b>	server	Specifies the email server.
	ip	IP address of the email server
	port	SMTP port of the email server, integer ranges from 1 to 65535
	mail-address	Specifies recipient's email address
	mail-index	Ranges from 1 to 4
	rcv-email	Recipient's email address
	account	Specifies sender's email account
	name	Sender's email account, 1 to 64 characters
	password	Sender's email password, 1 to 64 characters
	sender	Specifies sender's email
	sender-email	Sender's email address
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify E-mail server IP (192.168.1.1), port (2525) with account name (user1) and password (user1-password). Sender email is user1@example.com; recipient email is worker1@example.com. <pre>router# configure router(config)# email-warning server 192.168.1.1 2525 router(config)# email-warning mail-address 1 worker1@example.com router(config)# email-warning account user1 user1-password router(config)# email-warning sender user1@example.com router(config)# exit</pre>	
<b>Error Messages</b>	^Parse error ^Incomplete command % Invalid Port % Invalid Mail Index % Invalid Email Address % Invalid User Name Length	
<b>Related Commands</b>	show email-warning config	

## logging

To specify or modify logging events for DoS/IPsec/Trusted-Access/Firewall functions, use the **logging** global configuration command sets. To return to default settings, use the **no** form of this.

### Synopsis

```
(config)# logging {dos [{severity <severity-level> |
                        flash |
                        syslog |
                        trap}] |
                 ipsec [{syslog |
                        flash |
                        trap}] |
                 trusted-access [{severity <severity-level> |
                        flash |
                        syslog |
                        trap}] |
                 firewall |
                 I317-policy}
```

```
(config)# no logging [{dos [{flash |
                        syslog |
                        trap}] |
                    ipsec [{syslog |
                        flash |
                        trap}] |
                    trusted-access [{flash |
                        syslog |
                        trap}] |
                    firewall |
                    I317-policy }]
```

<b>Option Description</b>	dos	Enables/disables event logging for DoS function
	severity	Specifies severity of logging for DoS function
	severity-level	Specifies an integer for: {Emergency(0)   Alert(1)   Critical(2)   Error(3)   Warning(4)   Notice(5)   Information(6)   Debug(7)}
	flash	Specifies writing event logs into flash.
	syslog	Specifies sending event logs to syslog server
	trap	Specifies sending event logs via SNMP trap
	ipsec	Enables/disables event logging for IPsec function
	trusted-access	Enables/disables event logging for Trusted-Access function
	I317-policy	Enables/disables event logging for Layer 3-7 policy
firewall	Enables/disables event logging for Firewall function ( <b>No longer supported after version 3.0.</b> )	
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>Configure SNMP Trap in advance when sending event logs via SNMP trap.</li> <li>Configure Syslog server in advance when sending event logs to syslog server.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Enable logging for Trusted-Access function. Specify the severity to DEBUG and write logs into internal Flash storage.</li> </ul> <pre>router# configure router(config)# logging trusted-access severity 7 router(config)# logging trusted-access flash router(config)# logging trusted-access router(config)# exit</pre>	

	<ul style="list-style-type: none"> <li>Disable logging for Layer 3-7 policy function.  <pre>router# configure router(config)# no logging l3l7-policy</pre> </li> </ul>
<b>Error Messages</b>	% Severity level is out of range!
	% The firewall configuration is not compatible with firmware versions prior to V2.0.
	^Parse error ^Incomplete command
<b>Related Commands</b>	<pre>logging-capacity show logging event-log show logging event-log snmp-server host snmp-server trap-mode logging &lt;ip-addr&gt;</pre>

## Syslog server settings

To specify or modify syslog server settings, use the **logging** global configuration command. To delete a specified syslog server, use the **no** form of this command.

### Synopsis

```
(config)# logging <ip-addr> [{<port> [{<server-index> [authentication tls <local-cert>] |
                                enable |
                                disable}] |
                             authentication tls <local-cert>}]
```

```
(config)# no logging {<ip-addr> | enable <server-index>}
```

<b>Option Description</b>	ip-addr	IP address of the syslog server
	port	Port of the syslog server. Ranges from 1 to 65535.
	server-index	Ranges from 1 to 3.
	enable	Enables specified syslog server
	disable	Disables specified syslog server
	authentication tls	Specifies TLS authentication
	local-cert	Previously imported certificate
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>Max. number of Syslog server is 3.</li> <li>If necessary, the certificate must be installed via web GUI when utilizing TLS authentication with the Syslog server.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Specify the first Syslog server (192.168.1.2), port (5145) and enable it.  <pre>router# configure router(config)# logging 192.168.1.2 5145 1 router(config)# exit</pre> </li> <li>Disable the first Syslog server entry.  <pre>router# configure router(config)# no logging enable 1 router(config)# exit</pre> </li> </ul>	
<b>Error Messages</b>	% This server is not existed in the list.	
	% Server list is full.	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	<pre>logging warning-notification system-event interface ethernet warning-notification</pre>	

## clear logging

To clear event logs including of VPN/System/Firewall, use the **clear logging event-log** privileged command.

### Synopsis

```
# clear logging event-log [{vpn |  
                           system |  
                           trusted-access |  
                           malformed |  
                           dos |  
                           l3l7-policy |  
                           dpi |  
                           adp |  
                           ips |  
                           session-control |  
                           l2-policy }]
```

<b>Option</b>	vpn	VPN event logs
<b>Description</b>	system	System event logs
	trusted-access	Trust Access Event Logs
	malformed	Malformed Packets Event Logs
	dos	DoS Policy Event Logs
	l3l7-policy	Layer 3-7 Event Logs
	dpi	Protocol Filter Policy Event Logs
	adp	ADP Event Logs
	ips	IPS Event Logs
	session-control	Session Control Event Logs
	l2-policy	Layer 2 Event Logs
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Clear all system event logs. router# clear logging event-log system router#	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show logging event-log	



## auto-backup event-log

Use the **auto-backup** global configuration commands on the router to enable auto-backup event logs to the local storage. Use the **no** form of this command to disable auto-backup function.

### Synopsis

```
(config)# auto-backup {enable |  
                        event-log}
```

```
(config)# no auto-backup {enable |  
                          event-log}
```

<b>Option Description</b>	enable	Specifies to enable hardware interface (USB) to allow the router to export event logs
	event-log	Specifies to automatically back up event logs to ABC-02
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• A local storage (ABC-02) has to be plugged in advance.</li><li>• Hardware interface (USB) has to be enabled in advance.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Enable auto-backup to export event-logs to the USB storage device. router# configure router(config)# auto-backup enable router(config)# auto-backup event-log router(config)# exit</li><li>• Disable auto-backup to export event-logs to the USB storage device. router# configure router(config)# no auto-backup event-log router(config)# no auto-backup enable router(config)# exit</li></ul>	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	show auto-backup auto-backup config	

## snmp-server host

To set up a target IP address for SNMP trap notification, use the **snmp-server host** global configuration command. To remove SNMP trap target IP address, use the **no** form of this command.

### Synopsis

(config)# **snmp-server host** <trap-ip> [<trap-community>]

(config)# **no snmp-server host** [<trap-ip> <trap-community>]

<b>Option</b>	trap-ip	IP address for SNMP trap notification
<b>Description</b>	trap-community	SNMP trap community string, 1 to 64 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # \$ % & * ( ) . + = { } [ ]   : ; , ~.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>This command can add one trap IP at a time. Maximum number of target trap IP is 3. In the case of replacing one target IP among existing 3 IP, delete one trap IP and then add a new one is required.</li> <li>When Specify/modify trap community, {trap-community} should come after {trap-ip}.</li> <li>With the no form of this command, in the case of {trap-ip} and {trap-community} are not presented, all target IP will be cleared.</li> <li>With the no form of this command, in the case of both correct {trap-ip} and {trap-community} are provided correctly, a specific {trap-ip} will be cleared.</li> </ul>	
<b>Examples</b>	Specify a trap target IP address and modify the trap community string to "newTrap". <pre>router# configure router(config)# snmp-server host 192.168.127.10 newTrap router(config)# exit</pre>	
<b>Error Messages</b>	% Invalid IP Address. % Host or Community is incorrect!!! % Trap servers are full, please remove at least one first. ^Parse error ^Incomplete command	
<b>Related Commands</b>	snmp-server community snmp-server user snmp-server version snmp-server trap-mode snmp-server engineid show snmp	

## snmp-server trap-mode

To enable all SNMP notifications (traps or informs) available on your system, use the **snmp-server trap-mode** global configuration command. To return to the default, use **no** form of this command.

### Synopsis

```
(config)# snmp-server trap-mode {trap-v1 |
                                trap-v2c |
                                trap-v3 |
                                inform [{retry <times> timeout <second> |
                                        v3}]}
```

```
(config)# no snmp-server trap-mode
```

<b>Option</b>	trap-v1	SNMP v1 trap notification
<b>Description</b>	trap-v2c	SNMP v2c trap notification
	trap-v3	SNMP v3 trap notification
	inform	SNMP v2c inform request
	retry	Specifies inform retries
	times	Inform retry times. Ranges from 1 to 99.
	timeout	Specifies inform timeout
	second	Second, ranges from 1 to 300.
	v3	Specifies SNMP inform V3
<b>Defaults</b>	The default mode is "trap-v1"	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify/modify SNMP v2c trap notification. router# configure router(config)# snmp-server trap-mode trap-v2c router(config)# exit	
<b>Error Messages</b>	% Invalid Retries Value. It must be 1 - 99.	
	% Invalid Timeout Value. It must be 1 - 300.	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	snmp-server community snmp-server user snmp-server host snmp-server version snmp-server engineid show snmp	

## snmp-server {trap-v3 | inform-v3}

To create a SNMP trap / inform account on your system, use the **snmp-server {trap-v3 | inform-v3}** global configuration command.

### Synopsis

```
(config)# snmp-server {trap-v3 | inform-v3} {user <name> auth <authtype> [<authpass> [priv <enc-key>]]}
```

<b>Option</b>	trap-v3	Specifies SNMP v3 trap notifications
<b>Description</b>	inform-v3	Specifies SNMP v3 inform requests
	user	Specifies to create the SNMP Trap/Inform user.
	name	User name. Max. string length is 32.
	auth	Specifies authentication type
	authtype	Specifies one of the strings {no-auth   md5   sha}
	authpass	Authentication key. String length ranges from 8 to 64.
	priv	Specifies to use AES encryption
	enc-key	AES encryption key. String length ranges from 8 to 64.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Only one user is permitted. Executing the command again will overwrite the existing settings.	
<b>Examples</b>	Create a SNMP trap-v3 account. router# configure router(config)# snmp-server trap-v3 user trapv3-user auth sha moxa1234 priv 1234moxa router(config)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command % SNMP authtype must be ( no-auth   md5   sha )!!	
<b>Related Commands</b>	snmp-server community snmp-server user snmp-server host snmp-server version snmp-server engineid show snmp	

## show logging event-log

Use the **show logging** user EXEC command to display the setting of the syslog server.

### Synopsis

# **show logging event-log** [{**vpn** | **system** | **I317-policy** | **trust-access** | **malformed** | **dos** | **dpi** | **adp** | **ips** | **session-control** | **I2-policy**}] [**severity** <level-range>]

<b>Option</b>	vpn	Specifies all VPN event logs
<b>Description</b>	system	Specifies all System event logs
	I317-policy	Specifies all Layer 3 to 7 event logs
	trust-access	Specifies Trusted Access event logs
	malformed	Specifies Malformed Packet event logs
	dos	Specifies DoS event logs
	dpi	Specifies protocol filter policy logs
	adp	Specifies ADP logs
	ips	Specifies IPS logs
	session-control	Specifies session control event logs
	I2-policy	Specifies Layer 2 policy event logs
	severity	Specifies to display a specific range of severity levels
	level-range	Severity level ranges 0 to 7. Specifies a range of level. E.g. 1-1, 5-7, ...
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# show logging event-log system severity 0-0 System Log:  2  message lines logged, ----- Index Date          Time          Severity Event -----  - 1      2017/10/14 12:04:14 &lt;0&gt;          [Configuration Change] DHCP Relay Agent, Bootup:132, Startup:0d5h20m48s ----- 2      2017/10/14 12:04:11 &lt;0&gt;          [Configuration Change] DHCP Relay Agent, Bootup:132, Startup:0d5h20m44s</pre>	
<b>Error Messages</b>	Severity level is out of range!	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	logging event-log	

## show email-warning config

Use the **show email-warning config** command to display the settings of the email warning.

### Synopsis

# **show email-warning config**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC /User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre># show email-warning config Mail Server and Email Setup SMTP Server IP/Name      : SMTP Port                25 Account Name             : Account Password         :  1st email address : 2nd email address : 3rd email address : 4th email address :</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	email-warning

## show logging-capacity

To check the logging capacity thresholds on the router, use the **show logging-capacity** command.

### Synopsis

# **show logging-capacity**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router # show logging-capacity Logging Capacity Threshold: 0% Logging Capacity Threshold Warning by Trap: On Logging Capacity Threshold Warning by Email: On Logging Capacity Oversize Action: Overwrite Oldest</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	logging-capacity

## Tools

### Port Mirror

Use **monitor** global configuration commands to enable the monitoring of data transmitted/received by a specific port. Use **no** form of this command to disable the monitoring.

#### Synopsis

```
(config)# monitor {source interface <mod-port> [{both |  
                                     tx |  
                                     rx}] |  
                destination interface <port-id>}
```

```
(config)# no monitor {source interface |  
                    destination interface}
```

<b>Option Description</b>	source	Specifies monitored port(s)
	interface	Specifies which port is mirrored from or mirrored to.
	destination	Specifies the mirror port
	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	port-id	Port ID (consists of module/port-number)
	both	Specifies this option to monitor data packets both coming into, and being sent out
	tx	Specifies this option to monitor only those data packets being sent out
	rx	Specifies this option to monitor only those data packets coming into
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>Traffic send/receive by a source port (Monitored port) will be mirrored to the destination port (Mirror port)</li><li>Multiple port selection is acceptable.</li></ul>	
<b>Examples</b>	Specify PORT8 and PORT9 to be monitored for both directions. All packets will be mirrored to PORT4: router# configure router(config)# monitor source interface 1/8-9 both router(config)# monitor destination interface 1/4 router(config)# exit	
<b>Error Messages</b>	Monitored Port is the same with Mirror Port !!!	
	Invalid parameter	
	Warning !!! Mirror Port don't set !	
	Warning !!! Monitored Port don't set !	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show port monitor	

## show port monitor

Use the **show port monitor** EXEC command to display the setting of the port mirror.

### Synopsis

# **show port monitor**

<b>Option Description</b>	N/A	
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# show port monitor Port Being Monitored           Direction  Mirror Port ----- 1/8  1/9                        both       1/4</pre>	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	monitor	

## ping

Use the **ping** user EXEC command on the router to detect if the remote host is still alive.

### Synopsis

# **ping** <ip-address>

<b>Option Description</b>	ip-address	Ex. 192.168.127.1
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# ping 192.168.127.1 PING 192.168.127.1, Send/Recv/Lost = 4/4/0</pre>	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## tcpdump

Use the **tcpdump** privileged command on the router to capture layer-3 packets and display on the terminal.

### Synopsis

# **tcpdump**

[-c <count> | -i <interface> | -n ] [<expression>]

<b>Option Description</b>	-c <count>	Exit after receiving count packets
	-i <interface>	Network interface to be used to capture packets. E.g. <b>eth0</b>
	-n	Do't convert host addresses to names.
	expression	Common pcap-filter syntax
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	



<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• Typing <b>tcpdump</b> command and pressing enter will get a prompt message and then type applicable arguments.</li> <li>• Only incoming packets will be displayed on the terminal console.</li> </ul>
<b>Examples</b>	<p>Capture and display incoming icmp packets.</p> <pre>router# tcpdump Please set tcpdump parsing parameter -i eth0 icmp</pre> <p>Press ESC or q to exit tcpdump</p> <pre>tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes 01:15:50.760091 IP 192.168.127.1 &gt; 192.168.127.254: ICMP echo request, id 1, seq 2282, length 40 01:15:50.760035 IP 192.168.127.1 &gt; 192.168.127.254: ICMP echo request, id 1, seq 2283, length 40</pre>
<b>Error Messages</b>	<p>^Parse error</p> <p>^Incomplete command</p>
<b>Related Commands</b>	N/A

## Netflow

To specify or modify netflow configurations, use the following configuration command sets.

### ip flow-export

Use **ip flow-export** command to configure netflow global settings.

#### Synopsis

(config)# **ip flow-export** {enable | disable | destination <host> [port] | version <ver>}

<b>Option Description</b>	enable	Enable netflow
	disable	Disable netflow
	destination	Collector setting
	host	Collector's IP
	port	Collector's port
	version	Specifies NetFlow version
	ver	NetFlow version
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable Netflow and set collector ip, mask. router# configure router(config)# ip flow-export enable router(config)# ip flow-export destination 172.21.0.1 9996 router(config)# exit	
<b>Error Messages</b>	Invalid Collector %ip:%port. It has been set on Primary Collector.	
	Invalid IP/Hostname	
	Invalid Port	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show ip flow export	

### no ip flow-export destination

Use the **no ip flow-export destination** command to disable connector settings.

#### Synopsis

(config)# **no ip flow-export destination** [host]

<b>Option Description</b>	host	Collector's IP
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Disable Netflow and set collector ip, mask. router# configure router(config)# no ip flow-export destination 172.21.0.1 router(config)# exit	
<b>Error Messages</b>	% is not exist.	
	^Parse error	
	^Incomplete command	

<b>Related Commands</b>	show ip flow export
-------------------------	---------------------

**Synopsis**

(config)# **ip flow-cache timeout** {active <a-time> | inactive <i-time>}

<b>Option Description</b>	active	Configure NetFlow active timeout
	a-time	active timeout time
	inactive	Configure NetFlow inactive timeout
	i-time	inactive timeout time
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable Netflow and set collector ip, mask. router# configure router(config)# ip flow-cache timeout 5 router(config)# exit	
<b>Error Messages</b>	Inactive Timeout must be 1 - 3600. Active Timeout must be 1 - 60. ^Parse error ^Incomplete command	
<b>Related Commands</b>	show ip flow export	

**Synopsis**

(config-if)# **interface** <if-name>

(config-if)# **ip flow** {both | egress | ingress}

<b>Option Description</b>	both	Bidirectional traffic data
	egress	Egress traffic data
	ingress	Ingress traffic data
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set Netflow cache direction on interface router# configure router(config)#interface lan router(config-if)# ip flow both router(config-if)# exit	
<b>Error Messages</b>	Can not enable NetFlow on this interface ^Parse error ^Incomplete command	
<b>Related Commands</b>	show ip flow export	

### **Synopsis**

(config-if)# **ip route-cache flow {enable | disable}**

<b>Option</b>	enable	Enable netflow
<b>Description</b>	disable	Disable netflow
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable Netflow on Interface. router# configure router(config)#interface lan router(config-if)# ip route-cache flow enable router(config-if)# exit	
<b>Error Messages</b>	Can not enable NetFlow on this interface ^Parse error ^Incomplete command	
<b>Related Commands</b>	show ip flow export	

### **Synopsis**

(config-if)# **no ip route-cache flow**

<b>Option</b>	no	Reset or disable configuration
<b>Description</b>	enable	Enable netflow
	disable	Disable netflow
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Delete Interface Netflow Setting. router# configure router(config)#interface lan router(config-if)# no ip route-cache flow router(config-if)# exit	
<b>Error Messages</b>	Can not enable NetFlow on this interface Rate must be 0-65535 ^Parse error ^Incomplete command	
<b>Related Commands</b>	show ip flow export	

(config-if)# **netflow-mode {basic [rate] |filtered}**

<b>Option Description</b>	basic	Basic mode
	rate	Specifies the sampling rate
	filtered	Filter mode
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable Netflow and set collector ip, mask. router# configure router(config)# netflow-mode basic 1 router(config)# exit	
<b>Error Messages</b>	Can not enable NetFlow on this interface	
	Rate must be 0-65535	
	^Parse error	
<b>Related Commands</b>	^Incomplete command	
	show ip flow export	

## Synopsis

(config)# **configure**

(config)# **interface lan**

(config-if)# **netflow-mode filtered**

(config-filter)# {**src-ip** <s-ip> <s-mask> | **src-port** <s-port> | **dst-ip** <d-ip> <d-mask> | **dst-port** <d-port> | **protocol tcp** | **protocol udp** }

<b>Option Description</b>	src-ip	Filter Source IP Address
	s-ip	Source IP Address
	s-mask	Source IP Mask
	src-port	Filter Source Port
	s-port	Source Port
	dst-ip	Filter Destination IP Address
	d-ip	Destination IP Address
	d-mask	Destination IP mask
	dst-port	Filter Destination Port
	d-port	Destination Port
	protocol	Protocol type
	tcp	TCP
udp	UDP	
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable Netflow and set collector ip, mask. router# configure router(config)#interface lan router(config-if)#netflow-mode filtered router(config-filter)#src-ip 192.168.127.0 255.255.255.0 router(config-filter)#src-port 80 router(config-filter)#protocol tcp router(config-filter)#exit router(config-if)#exit router(config)#exit	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show ip flow export	

## Synopsis

(config-filter)# **no** {protocol | no src-ip | no dst-ip | no src-port | no dst-port}

<b>Option</b>	no	Reset or disable configuration
<b>Description</b>	src-ip	Filter Source IP Address
	src-port	Filter Source Port
	dst-ip	Filter Destination IP Address
	dst-port	Filter Destination Port
	protocol	Protocol type
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set Netflow filter mode. router# configure router(config)#interface lan router(config-if)#netflow-mode filtered router(config-filter)#no protocol router(config-filter)#exit router(config-if)#exit router(config)#exit	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show ip flow export	

# Network Services

## DHCP

### service dhcp

To enable the DHCP service, use the **service dhcp** global configuration command. To disable the DHCP service, use **no** form of this command.

#### Synopsis

(config)# **service dhcp** [**auto-assign**]

(config)# **no service dhcp**

<b>Option Description</b>	auto-assign	Enables DHCP server mode as Port-based IP assignment
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Command service dhcp enables DHCP server mode as DHCP/MAC-based assignment.	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Enable DHCP server mode to Port-based IP assignment. router# configure router(config)# service dhcp auto-assign router(config)# exit</li><li>• Enable DHCP server mode to DHCP/MAC-based assignment. router# configure router(config)# service dhcp router(config)# exit</li><li>• Disable DHCP server mode. router# configure router(config)# no service dhcp router(config)# exit</li></ul>	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show ip dhcp show ip dhcp static show ip auto-assign show ip dhcp-relay ip dhcp pool ip dhcp static pool ip dhcp-relay interface ethernet	



## ip dhcp pool

To create a DHCP pool for dynamic IP assignment, use the **ip dhcp pool** global configuration command and related sub-level configuration command sets. To remove the DHCP pool, use **no** form of this command.

### Synopsis

#### Create / Remove a DHCP pool

```
(config)# ip dhcp pool <index>
(config)# no ip dhcp pool <index>
```

#### Set IP addresses in the pool

```
(dhcp-config)# network <first-ip> <last-ip> <netmask>
```

#### Set lease time

```
(dhcp-config)# lease <minutes>
```

#### Set DNS Server

```
(dhcp-config)# dns-server <dns-ip1><dns-ip2>
```

#### Set Default Gateway

```
(dhcp-config)# default-router <dr-ip>
```

#### Set NTP Server

```
(dhcp-config)# ntp-server <ntp-ip>
```

#### Save and Exit DHCP pool configuration

```
(dhcp-config)# exit
```

#### Enable / Disable the DHCP pool

```
(config)# ip dhcp pool <index> {enable |
                               disable}
```

<b>Option Description</b>	index	Index of DHCP pools. This value should be created in sequence, the maximum number of pools is 32.
	lease	Specifies DHCP lease time.
	minutes	A number, ranges from 5 to 527039. Default is 60.
	network	Specifies a range of IP addresses in a DHCP pool.
	first-ip	The first IP address in a DHCP pool. Default is 0.0.0.0
	last-ip	The last IP address in a DHCP pool. Default is 0.0.0.0
	netmask	Netmask of a DHCP pool. Default is 0.0.0.0
	dns-server	Specifies DNS servers.
	dns-ip1	The IP address of the first DNS server. Default is 0.0.0.0
	dns-ip2	The IP address of the second DNS server. Default is 0.0.0.0
	default-router	Specifies the default router.
	dr-ip	The IP address of the default router. Default is 0.0.0.0
	ntp-server	Specifies the NTP server.
	ntp-ip	The IP address of the NTP server Default is 0.0.0.0
	exit	Commit new settings and exit sub-level configuration mode.
	enable	Enable specified <index> in the DHCP pool
disable	Disable specified <index> in the DHCP pool	
<b>Defaults</b>	Enabled.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>Maximum number of pools is 32.</li><li>No modification function is provided. In case modification on a specific index is required, remove it first and then add a new setting.</li></ul>	

	<ul style="list-style-type: none"> <li>• Type a valid index to enter sub-level configuration mode.</li> <li>• Specify <b>network</b> &lt;first-ip&gt; &lt;last-ip&gt; &lt;netmask&gt; first before setting <b>lease</b>, <b>dns-server</b>, <b>default-router</b> or <b>ntp-server</b>. Otherwise, error message <b>% Please configure offered network first</b> will be displayed.</li> <li>• Static IP assignment takes precedence over the dynamic IP assignment as well as DHCP relay agent.</li> <li>• Exit the sub-level configuration mode to let settings take effect.</li> </ul>
<b>Examples</b>	<p>Create a DHCP pool for dynamic IP assignment:</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>• TN router: <ul style="list-style-type: none"> <li>- Interface LAN5: static IP = 192.168.5.254/24, VLAN ID=5;</li> <li>- PORT5: VLAN ID=5</li> <li>- DHCP server mode: Dynamic/Static IP assignment</li> </ul> </li> <li>• Device(A) connected on PORT5: <ul style="list-style-type: none"> <li>- IP: DHCP client</li> </ul> </li> </ul> <p>Scenario:</p> <p>a) TN router DHCP pool settings:</p> <ol style="list-style-type: none"> <li>IP addresses: from 192.168.5.1 to 192.168.5.10</li> <li>Netmask: 255.255.255.0</li> <li>Lease time: 2880 minutes</li> <li>Default gateway: 192.168.5.254</li> <li>DNS server 1: 8.8.8.8</li> <li>DNS server 2: 192.168.8.8</li> <li>NTP server: 192.168.8.9</li> </ol> <p>b) Device(A) can get an DHCP IP: 192.168.5.1 through PORT5.</p> <p>Commands:</p> <pre>router# configure router(config)# ip dhcp pool 1 router(dhcp-config)# network 192.168.5.1 192.168.5.10 255.255.255.0 router(dhcp-config)# lease 2880 router(dhcp-config)# default-router 192.168.5.254 router(dhcp-config)# dns-server 8.8.8.8 192.168.8.8 router(dhcp-config)# ntp-server 192.168.8.9 router(dhcp-config)# exit</pre>
<b>Error Messages</b>	<p>% Invalid parameter!</p> <p>% Invalid Index</p> <p>% Please configure offered network first.</p> <p>^Parse error</p> <p>^Incomplete command</p>
<b>Related Commands</b>	<pre>service dhcp ip dhcp static pool ip dhcp-relay interface ethernet show ip dhcp show ip dhcp static show ip auto-assign show ip dhcp binding show ip dhcp-relay</pre>

## ip dhcp static pool

To assign a static DHCP IP address to a client device with a specific MAC address, use the **ip dhcp static pool** global configuration command. To remove the static IP assignment, use **no** form of this command.

### Synopsis

#### Create / Remove a DHCP static IP

```
(config)# ip dhcp static pool <name>
(config)# no ip dhcp static pool <name>
```

#### Set the static IP address in the pool

```
(dhcp-config)# host <ip-addr> <netmask>
```

#### Set lease time

```
(dhcp-config)# lease <minutes>
```

#### Set MAC address

```
(dhcp-config)# hardware-address <mac-addr>
```

#### Set DNS Server

```
(dhcp-config)# dns-server <dns-ip1> <dns-ip2>
```

#### Set Default Gateway

```
(dhcp-config)# default-router <dr-ip>
```

#### Set NTP Server

```
(dhcp-config)# ntp-server <ntp-ip>
```

#### Save and Exit DHCP static configuration

```
(dhcp-config)# exit
```

#### Enable / Disable DHCP static IP configuration

```
(config)# ip dhcp static pool <name> {enable |
                                     disable}
```

Option Description	name	A name of the static IP assignment in the DHCP pool. Maximum length is 63.
	lease	Specifies DHCP lease time
	minutes	The lease duration. Ranges from 5 to 527039. Default is 60.
	host	Specifies the static IP address.
	ip-addr	Assigned IP address. Default is 0.0.0.0
	netmask	Netmask of the assigned IP address. Default is 0.0.0.0
	hardware-address	Specifies the MAC address
	mac-addr	The MAC address of the selected device. Default is 00:00:00:00:00:00
	dns-server	Specifies the DNS servers.
	dns-ip1	The IP address of the first DNS server. Default is 0.0.0.0
	dns-ip2	The IP address of the second DNS server. Default is 0.0.0.0
	default-router	Specifies the default router.
	dr-ip	The IP address of the default router. Default is 0.0.0.0
	ntp-server	Specifies the NTP server.
	ntp-ip	The IP address of the NTP server. Default is 0.0.0.0
	exit	Commit new settings and exit sub-level configuration mode.
	enable	Enable specified <name> in the DHCP pool
	disable	Disable specified <name> in the DHCP pool
Defaults		Enabled.

<b>Command Modes</b>	Global configuration, sub-level configuration
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• Maximum number of static IP in the DHCP pool is 256.</li> <li>• Types a valid name to enter sub-level configuration mode to modify IP assignment settings.</li> <li>• Specify host &lt;ip-addr&gt; &lt;netmask&gt; first before setting <b>lease</b>, <b>hardware-address</b>, <b>dns-server</b>, <b>default-router</b> or <b>ntp-server</b>. Otherwise, error message <b>% Please configure host IP and netmask first</b> will be displayed.</li> <li>• Static IP assignment takes precedence over the dynamic IP assignment as well as DHCP relay agent.</li> <li>• Exits the sub-level configuration mode to let settings take effect.</li> </ul>
<b>Examples</b>	<p>Create a static IP assignment:</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>• TN router: <ul style="list-style-type: none"> <li>- Interface LAN6: static IP = 192.168.6.254/24, VLAN ID=6</li> <li>- PORT6: VLAN ID=6</li> <li>- DHCP server mode: Dynamic/Static IP assignment</li> </ul> </li> <li>• Device(A) connected on PORT6: <ul style="list-style-type: none"> <li>- IP: DHCP client</li> </ul> </li> </ul> <p>Scenario:</p> <p>a) TN router DHCP static IP settings:</p> <ol style="list-style-type: none"> <li>Name: P6-static</li> <li>IP addresses: from 192.168.6.1</li> <li>Netmask: 255.255.255.0</li> <li>MAC address: 00:90:e8:00:f2:ac</li> <li>Lease time: 2880 minutes</li> <li>Default gateway: 192.168.6.254</li> <li>DNS server 1: 8.8.8.8</li> <li>DNS server 2: 192.168.8.8</li> <li>NTP server: 192.168.8.9</li> </ol> <p>b) Device(A) can get an DHCP IP: 192.168.6.1 through PORT6.</p> <p>Commands:</p> <pre>router# configure router(config)# ip dhcp static pool P6-static router(dhcp-config)# host 192.168.6.1 255.255.255.0 router(dhcp-config)# lease 2880 router(dhcp-config)# hardware-address 00:90:e8:00:f2:ac router(dhcp-config)# default-router 192.168.6.254 router(dhcp-config)# dns-server 8.8.8.8 192.168.8.8 router(dhcp-config)# ntp-server 192.168.8.9 router(dhcp-config)# exit</pre>
<b>Error Messages</b>	<p>^Parse error</p> <p>^Incomplete command</p> <p>% Please configure host IP and netmask first.</p>
<b>Related Commands</b>	<pre>service dhcp ip dhcp static pool ip dhcp-relay interface ethernet show ip dhcp show ip dhcp static show ip auto-assign show ip dhcp binding show ip dhcp-relay</pre>

## ip dhcp-relay

To enable a DHCP relay agent, use the **ip dhcp-relay** global configuration command. To disable DHCP relay agent, use **no** form of this command.

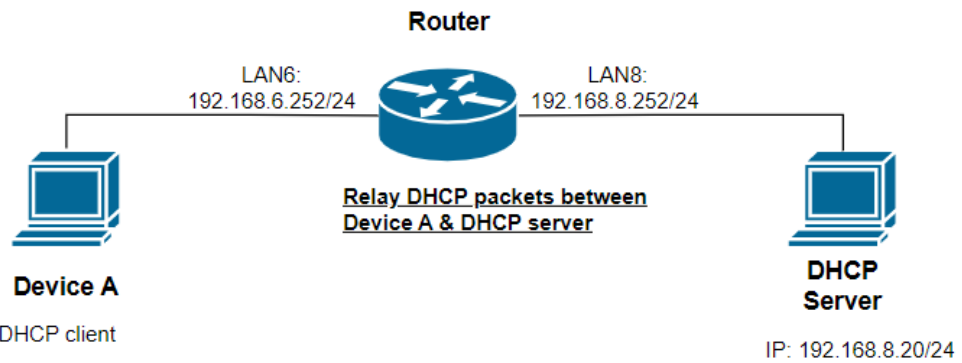
### Synopsis

```
(config)# ip dhcp-relay {server {interface <if-name> |
                           <server-index> <server-ip>} |
                           option82 [{remote-id-type {ip |
                                                    interface <if-name>}
                                         mac |
                                         client-id |
                                         other}] |
                           man-id <manual-id>}}
```

```
(config)# no ip dhcp-relay {server {interface |
                                   <server-index1>} |
                             option82}
```

<b>Option Description</b>	server	Specifies an interface to relay DHCP message to a DHCP server or DHCP servers
	interface	Specifies an interface to relay DHCP message to a DHCP server
	if-name	Valid interface name, if-name is case-sensitive
	server-index	Index ranges from 1 to 4
	server-ip	IP addresses of DHCP server.
	option82	Specifies DHCP option 82
	remote-id-type	Specifies one of WAN-IP/LAN/MAC/Client-ID/Other types
	ip	(Deprecated) WAN interface IP address
	mac	MAC address
	client-id	Uses a combination of the switch's MAC address and IP address as the remote ID
	other	Uses string specified by <manual-id>
	man-id	Specifies the user-designated ID
	manual-id	User-designated ID. Maximum length is 32.
server-index1	Index ranges from 0 to 3	
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>If dynamic/static IP assignment or IP-port binding is specified, DHCP relay agent will not take effect in this case.</li> <li>Static IP assignment takes precedence over the dynamic IP assignment as well as DHCP relay agent.</li> <li>For DHCP option 82 feature, the CLI command (config)# ip dhcp-relay option82 remote-id-type <b>ip</b> is replaced with (config)# ip dhcp-relay option82 remote-id-type <b>interface WAN</b>.</li> </ul>	
<b>Examples</b>	DHCP relay agent:  Prerequisites: <ul style="list-style-type: none"> <li>TN router:               <ul style="list-style-type: none"> <li>LAN6: 192.168.6.252/24, VLAN ID=6, interface used for DHCP clients</li> <li>LAN8: 192.168.8.252/24, VLAN ID=8, interface used for the DHCP server</li> </ul> </li> <li>Device(A) on subnet 192.168.6.0/24:               <ul style="list-style-type: none"> <li>IP: DHCP client</li> </ul> </li> <li>DHCP Server on subnet 192.168.8.0/24:               <ul style="list-style-type: none"> <li>IP: 192.168.8.20/24</li> <li>Server settings:                   <ol style="list-style-type: none"> <li>IP pool: 192.168.6.11 to 192.168.6.15</li> <li>Circuit-ID: 0x01000606</li> <li>Remote-ID: 0x31323334</li> </ol> </li> </ul> </li> </ul>	

Network topology:



Scenario:

- a) Device(A) send DHCP DISCOVER packet to the router. Then the router will add a relay agent IP address and replace source IP and destination IP to the packet and forward it to the DHCP server.
- b) A DHCP server replies DHCP OFFER packet to the router and the router sends the packet to Device(A).

Commands:

```
router# configure
router(config)# ip dhcp-relay server interface LAN8
router(config)# ip dhcp-relay server 1 192.168.8.20
router(config)# ip dhcp-relay option82
router(config)# ip dhcp-relay option82 remote-id-type other
router(config)# ip dhcp-relay option82 man-id 1234
router(config)# interface ethernet 1/6
router(config-if)# ip dhcp-relay
router(config-if)# exit
router(config)#
```

<b>Error Messages</b>	% Invalid parameter!
	% Invalid outbound Interface Name.
	% Invalid interface!
	% Please configure offered network first.
	^Parse error
<b>Related Commands</b>	^Incomplete command
	service dhcp
	ip dhcp static pool
	ip dhcp pool
	interface ethernet
	show ip dhcp
	show ip dhcp static show ip auto-assign show ip dhcp binding show ip dhcp-relay

## interface ethernet ip

To assign a static DHCP IP address to a client device by using IP-port binding function, use the **interface ethernet** global configuration command and **ip** sub-level configuration command sets. To remove IP-port binding settings or disable dhcp-relay, use the **no** form of this command.

### Synopsis

#### Enter into the sub-level command mode to configure IP-port binding related settings

```
(config)# interface ethernet <mod-port>
```

#### Set the IP address of the specified Port / Remove the IP address

```
(config-if)# ip auto-assign <ip-addr> <netmask>
```

```
(config-if)# no ip auto-assign
```

#### Set DNS Server

```
(config-if)# ip dns-server <dns-ip1> <dns-ip2>
```

#### Set Default Gateway

```
(config-if)# ip default-router <dr-ip>
```

#### Set NTP Server

```
(config-if)# ip ntp-server <ntp-ip>
```

#### Set lease time

```
(config-if)# ip lease <minutes>
```

#### Enable / Disable Option-82 for DHCP relay agent on specified Port

```
(config-if)# ip dhcp-relay
```

```
(config-if)# no ip dhcp-relay
```

<b>Option</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
<b>Description</b>	Ip	Specifies IP-port binding or enables dhcp-relay function
	auto-assign	Specifies IP address and netmask for the connected device
	ip-addr	The IP address to be assigned to the device.
	netmask	Netmask
	dns-server	Specifies DNS servers.
	dns-ip1	The IP address of the first DNS server.
	dns-ip2	The IP address of the second DNS server.
	default-router	Specifies the default router.
	dr-ip	The IP address of the default router.
	ntp-server	Specifies the NTP server.
	ntp-ip	The IP address of the NTP server
	lease	Specifies DHCP lease time
	minutes	A number, ranges from 5 to 527039
	dhcp-relay	Specifies to enable/disable dhcp-relay function.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• Maximum number of port-based IP pool is 16.</li><li>• IP-port binding takes precedence over DHCP relay agent.</li></ul>	
<b>Examples</b>	Create a port-based IP assignment:  Prerequisites: <ul style="list-style-type: none"><li>• TN router:<ul style="list-style-type: none"><li>- Interface LAN7: static IP = 192.168.7.252/24, VLAN ID=7</li><li>- PORT7: VLAN ID=7</li><li>- DHCP server mode: IP-port binding</li></ul></li></ul>	

	<ul style="list-style-type: none"> <li>• Device(A) connected on PORT7: - IP: DHCP client</li> </ul> <p>Scenario:</p> <p>a) TN router DHCP port-based IP settings:</p> <ol style="list-style-type: none"> <li>i. IP addresses: from 192.168.7.22</li> <li>ii. Netmask: 255.255.255.0</li> <li>iii. Lease time: 1440 minutes</li> <li>iv. Default gateway: 192.168.7.252</li> <li>v. DNS server 1: 8.8.8.8</li> <li>vi. DNS server 2: 192.168.8.8</li> <li>vii. NTP server: 192.168.8.9</li> </ol> <p>b) Device(A) can get an DHCP IP: 192.168.7.22 through PORT7.</p> <p>Commands:</p> <pre>router# configure router(config)# interface ethernet 1/7 router(config-if)# ip auto-assign 192.168.7.22 255.255.255.0 router(config-if)# ip lease 1440 router(config-if)# ip ntp-server 192.168.8.9 router(config-if)# ip default-router 192.168.7.252 router(config-if)# ip dns-server 8.8.8.8 192.168.8.8 router(config-if)# exit</pre>
<b>Error Messages</b>	<pre>% Illegal parameter ^Parse error ^Incomplete command</pre>
<b>Related Commands</b>	<pre>service dhcp ip dhcp pool ip dhcp static pool ip dhcp-relay interface ethernet show ip dhcp show ip dhcp static show ip auto-assign show ip dhcp binding show ip dhcp-relay</pre>



## show ip dhcp

To check the DHCP static or dynamic client list on the router, use the **show ip dhcp** command.

### Synopsis

```
# show ip dhcp [{static |  
                binding}]
```

<b>Option</b>	static	Specifies to display static DHCP client list
<b>Description</b>	binding	Specifies to display dynamic DHCP client list
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<ul style="list-style-type: none"><li>Display static DHCP client list. router # show ip dhcp static Static DHCP Pool List ----- Name : P6-static State : Enable Host IP Address : 192.168.6.1 Host Netmask : 255.255.255.0 MAC Address : 00:90:E8:00:F2:AC Lease Time(min): 2880 Default Gateway : 192.168.6.254 NTP Server : 192.168.8.9 DNS Server 1 : 8.8.8.8 DNS Server 2 : 192.168.8.8 -----</li><li>Display dynamic DHCP client list. router # show ip dhcp binding Name MAC Address IP Address Time Left ----- Moxa-1 00:90:e8:00:00:41 192.168.5.1 44 h: 34 m: 25 s</li></ul>	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	ip dhcp static pool interface ethernet ip	

## show ip auto-assign

To check the port-based IP pool list information on the router, use the **show ip auto-assign** command.

### Synopsis

```
# show ip auto-assign
```

<b>Option</b>	N/A	
<b>Description</b>		
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# show ip auto-assign Port-based IP Pool List ----- Port : 7 State : Enable Static IP Address : 192.168.7.22 Netmask : 255.255.255.0 Lease Time(min) : 1440 Default Gateway : 192.168.7.252 NTP Server : 192.168.8.9 DNS Server 1 : 8.8.8.8 DNS Server 2 : 192.168.8.8 -----	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	^Incomplete command	

<b>Related Commands</b>	ip dhcp static pool interface ethernet ip
-------------------------	----------------------------------------------

## show ip dhcp-relay

To check the DHCP relay settings on the router, use the **show ip dhcp-relay** command.

### Synopsis

# **show ip dhcp-relay**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show ip dhcp-relay DHCP Relay Agent Setting   Interface      : LAN8   1st server IP : 192.168.8.20   2nd server IP : 0.0.0.0   3rd server IP : 0.0.0.0   4th server IP : 0.0.0.0 DHCP Relay Option 82: Enable   Remote ID type   : Other   Remote ID value  : 1234 (null)            : 31323334 DHCP Fucntion Table Port  Circuit-ID      Option 82 ----- 1/1   01000801          Disable 1/2   01000102          Disable 1/3   01000503          Disable 1/4   01000804          Disable 1/5   01000505          Disable 1/6   01000606          Enable 1/7   01000107          Disable 1/8   01000808          Disable 1/9   01000109          Disable 1/10  0100010A          Disable 1/11  0100080B          Disable 1/12  0100010C          Disable 1/13  0100010D          Disable 1/14  0100010E          Disable 1/15  0100010F          Disable 1/16  01000110          Disable</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	interface ethernet ip

# Dynamic DNS

## ip ddns

To enable the DDNS service, use the **ip ddns** global configuration command. To disable DDNS service, use the **no** form of this command.

### Synopsis

```
(config)# ip ddns {service {freedns |  
                 3322 |  
                 dyndns |  
                 no-ip} |  
                 username <user-name> |  
                 password <pwd> |  
                 domain <domain-name>}
```

```
(config)# no ip ddns
```

<b>Option</b>	service	Specifies a DDNS service
<b>Description</b>	freedns	DDNS service: freedns
	3322	DDNS service: 3322
	dyndns	DDNS service: dyndns
	no-ip	DDNS service: no-ip
	username	Specifies the DDNS server's user name
	user-name	DDNS server's user name, 1 to 45 characters
	password	Specifies the DDNS server's password
	pwd	DDNS server's password, 1 to 45 characters
	domain	Specifies domain name for DDNS service
	domain-name	DDNS server's domain name, 1 to 45 characters
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Configure freedns ddns service. router# configure router(config)# ip ddns service freedns router(config)# ip ddns username demo-user router(config)# ip ddns password demo-password router(config)# ip ddns domain domain-name router(config)# exit	
<b>Error Messages</b>	% Password Length should <= 45	
	% Server Name Error	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show ip ddns	

## show ip ddns

To check the Dynamic DNS settings on the router, use the **show ip ddns** command.

### Synopsis

# **show ip ddns**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router # show ip ddns DDNS Service : no-ip Server Name : User Name : demo-user Password : ***** Domain Name :
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	ip ddns

## Other Commands

### terminal

Use the **terminal** privileged command on the router to configure terminal page length.

### Synopsis

# **terminal** {length <number> |  
default}

<b>Option Description</b>	length	Specifies terminal page length
	number	0 or 20-100, 0: Unlimited
	default	Resets the Terminal Length to Default, default length: 20
<b>Defaults</b>	20	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	N/A	
<b>Error Messages</b>	Page Length should be between 20 and 100 ^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## package

Use the **package** privileged command on the router to install/upgrade packages such as Network Security Package or MXsecurity Agent Package.

### Synopsis

# **package** {**install** | **upgrade**} <pkg-name> {**firmware** | **tftp** <ip> <filename>}

<b>Option</b>	install	Specifies to install designated package
<b>Description</b>	upgrade	Specifies to upgrade designated package
	pkg-name	One of the package names {security   mxsecurity}
	firmware	Specifies to use the package prebuilt in the firmware
	tftp	Specifies to use the package located on a remote TFTP server
	ip	IP address
	filename	The filename of the designated package
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• &lt;pkg-name&gt; is case-sensitive.</li> <li>• If the package is already present, utilize the "upgrade" command instead of the "install" command.</li> <li>• Given that firmware and packages are handled separately, if the current package is incompatible with the new firmware, the existing package will be unloaded. You'll then need to download a new package and install it on the router.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>• Upgrade security package via TFTP           <pre>router# package upgrade security tftp 192.168.127.102 Security_TN-4900_V7.0.12_Build_23081018.pkg Upgrade security package(Security_TN-4900_V7.0.12_Build_23081018.pkg) from TFTP Server IP 192.168.127.102 Package transferring... Verified OK Checking Package...Package is importing now, please wait! All checking are ok.  Package upgrade successfully. router#</pre> </li> <li>• Upgrade security package via built-in firmware           <pre>router# package upgrade security firmware Upgrade to security buildin package  Buildin package upgrade successfully. router#</pre> </li> </ul>	
<b>Error Messages</b>	% You do not have admin privilege Buildin package install failed.(ERROR CODE: 1) Upgrade failed.(ERROR CODE: 1) Uninstall failed, package is not support uninstall. Buildin package install failed, package is already installed. ^Parse error ^Incomplete command	
<b>Related Commands</b>	show package	

## show package status

Use the **show package status** command on the router to display the status of installed packages.

### Synopsis

# **show package status**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	Display status of installed packages. router# show package status  Package security is enable.(v7.0.0011)  Package mxsecurity is enable.(v2.0.0012) router#
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	package

## moxasupport

Use the **moxasupport** command on the router to activate engineering mode for troubleshooting when it is necessary. To disable moxasupport, use the **no** form of this command.

### Synopsis

# **moxasupport** <secret-seed>

# **no moxasupport**

<b>Option Description</b>	secret-seed	A set of characters without a whitespace. The length must range from 4 to 8.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• This command is exclusively intended for troubleshooting by Moxa staff.</li><li>• The engineering mode will be disabled after system reboot.</li><li>• The &lt;secret-seed&gt; will become invalid after the next reboot .</li><li>• CLI command "show moxasupport" displays default status.</li></ul>	
<b>Examples</b>	Instructions for setting up the environment for remote troubleshooting by Moxa's staff.  Step 1: Enter CLI Privileged EXEC mode and issue below command. Please be aware that "1234" followed by "moxasupport" is a temporary one-time seed passphrase for login purposes. router# moxasupport 1234 router#  Step 2: Arrange a remote session to allow Moxa staff to troubleshoot the router through either the console port or SSH.	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## show integrity

Use the **show integrity** command on the router to check configuration and application integrity.

### Synopsis

# **show integrity**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	Whenever configuration or application changes in a normal operation, the router will calculate the hash and keep it as a record. Users can verify the integrity status of configurations or applications by entering this CLI command. The router will recalculate the hash and compare it against the previously recorded value.
<b>Examples</b>	Display status of integrity check. router # show integrity Application: OK Configuraion: OK router #
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	N/A

## license activation

Use the **license activation** privileged command to activate a specific function such as IPS on the router.

### Synopsis

(config)# **license activation** <code>

<b>Option Description</b>	code	Activation code
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC	
<b>Usage Guidelines</b>	Apply and download the activation code from Moxa's site in advance.	
<b>Examples</b>	N/A	
<b>Error Messages</b>	% cparser_cmd_config_license_activation_code: L43 Invalid activation code! ^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## show license

Use the **show license** command on the router to provide an overview of installed license and historical information.

### Synopsis

# **show license** {**overview** | **history**} <feature-id>

<b>Option</b>	overview	Specifies to display overview information
<b>Description</b>	history	Specifies to display historical information
	feature-id	Feature ID starting from 1
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	Whenever configuration or application changes in a normal operation, the router will calculate the hash and keep it as a record. Users can verify the integrity status of configurations or applications by entering this CLI command. The router will recalculate the hash and compare it against the previously recorded value.	
<b>Examples</b>	Display license overview information router# show license overview 1	
	License Overview: Name : IPS-DEVICE Valid Duration : 11066 days Start Date : 2022-04-01 08:20:00 End Date : 2053-12-08 02:06:40 Status : Valid	
<b>Error Messages</b>	% Invalid feature ID!	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	N/A	



## 2. Interface and Routing Functions

---

This chapter describes the interface and routing functions of the Ethernet switches.

### Command Modes

Refer to the following table for the command mode descriptions.

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your router by using a normal user account and password.	#	Enter <b>exit</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"><li>• Change terminal settings.</li><li>• Perform basic tests.</li><li>• Display system information.</li></ul>
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter <b>exit</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"><li>• Change terminal settings.</li><li>• Perform basic tests.</li><li>• Display system information.</li><li>• Enter configuration mode.</li></ul>
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	(config)#	To exit to privileged EXEC mode, enter <b>exit</b> .	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example <b>interface lan</b> command and press enter	(config-if)#	To exit to global configuration mode, enter <b>exit</b> .	A sub-level to configure for example LAN interface related arguments.

# Command Sets

## Interfaces

### LAN (using management VLAN)

Information described in this chapter is only applied to the LAN interface which management VLAN belongs to. For all other LAN interface configuration, refer to LAN (using non-management VLAN)) on page 114.

#### interface lan name

To change the name of this LAN interface, use the **interface lan** global configuration command and **name** sub-level configuration command. To exit sub-level configuration mode, use **exit** command.

##### Synopsis

```
(config)# interface lan  
(config-if)# {name <if-name> |  
              exit}
```

<b>Option</b>	name	Specifies the name of LAN interface
<b>Description</b>	if-name	The name of LAN interface, 1 to 12 characters.
	exit	Commit new settings and exit sub-level configuration mode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	This command only applies to LAN interface using the management VLAN.	
<b>Examples</b>	Change interface name to LAN-M. router# configure router(config)# interface lan router(config-if)# name LAN-M router(config-if)# exit	
<b>Error Messages</b>	% is over length. It must be 1 - 12.	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces lan	

## interface lan ip address

To configure static IP address or a secondary IP address for LAN interface, use the **interface lan** global configuration command and **ip address static** sub-level configuration command. To return to default settings or remove a secondary IP address, use the **no** form of this command.

### Synopsis

(config)# **interface lan**

(config-if)# **ip address static** <lan-ip> <netmask> [**secondary**]

(config-if)# **no ip address** [**static** <ip> <netmask> **secondary**]

	no	Disable
<b>Option Description</b>	static	Specifies static IP address
	lan-ip	IP address
	netmask	Netmask of the static IP address
	secondary	Specifies a secondary IP address
<b>Defaults</b>	IP address of default LAN is 192.168.127.254	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• This command only applies to LAN interface using the management VLAN..</li><li>• DHCP option is not applicable to this entry LAN interface.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Change the IP address (192.168.127.253) and netmask (255.255.255.0) of the interface. router# configure router(config)# interface lan router(config-if)# ip address static 192.168.127.254 255.255.255.0 router(config-if)# exit</li><li>• Return the LAN interface to default IP 192.168.127.254. router# configure router(config)# interface lan router(config-if)# no ip address router(config-if)# exit</li><li>• Remove a secondary IP 192.168.127.9/24 on LAN interface. router# configure router(config)# interface lan router(config-if)# no ip address static 192.168.127.9 255.255.255.0 secondary router(config-if)# exit</li></ul>	
<b>Error Messages</b>	% No match entry for Secondary IP, mask for LAN	
<b>Related Commands</b>	show interface lan	

## interface lan ip ospf

To configure dynamic routing with OSPF interface settings and auth type for LAN, use the **interface lan** global configuration command and **ip ospf** sub-level configuration command sets. To return to the default settings, use the **no** form of this command.

### Synopsis

```
(config)# interface lan
(config-if)# ip ospf {cost <metric> |
                    priority <pri-number> |
                    hello-interval <h-second> |
                    dead-interval <d-second> |
                    auth {simple auth-key <key-string>|
                        md5 <key-id> auth-key <md5-key-string>} |
                    area <area-id>}

(config-if)# no ip ospf [{cost |
                        priority |
                        hello-interval |
                        dead-interval |
                        auth}]
```

<b>Option Description</b>	cost	Specifies Metric/Cost of OSPF
	metric	Metric/Cost of OSPF. Ranges from 1 to 65535.
	priority	Specifies router's priority
	pri-number	Priority. Ranges from 0 to 255.
	hello-interval	Specifies Hello packets which are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors.
	h-second	Interval of hello packets. Ranges from 1 to 65535 seconds.
	dead-interval	Specifies the dead-interval
	d-second	Interval of dead packets. Ranges from 1 to 65535 seconds.
	auth	Enables or disables auth function
	simple auth-key	Specifies simple auth type
	key-string	A key string for simple auth type. Maximum string length is 8.
	md5	Specifies MD5 auth type
	key-id	A key ID for MD5 hash calculation. Ranges from 1 to 255.
	auth-key	Specifies MD5 key for hash
	md5-key-string	A key string for MD5 auth type. Maximum string length is 8.
area	Specifies the area ID	
area-id	An area ID	
<b>Defaults</b>	<ul style="list-style-type: none"> <li>metric : 1</li> <li>h-interval : 10</li> <li>d-interval : 40</li> <li>pri-number : 1</li> </ul>	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	This command only applies to LAN interface using the management VLAN.	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Specify Auth type to "none".  <pre>router# configure router(config)# interface lan router(config-if)# no ip ospf auth router(config-if)# exit router(config)# exit</pre> </li> <li>Delete OSPF LAN interface.  <pre>router# configure router(config)# interface lan router(config-if)# no ip ospf router(config-if)# exit router(config)# exit</pre> </li> </ul>	

	<ul style="list-style-type: none"> <li>Return hello interval to default.  <pre>router# configure router(config)# interface lan router(config-if)# no ip ospf hello-interval router(config-if)# exit router(config)# exit</pre> </li> </ul> <p>* An illustrative example can be found in the chapter "Unicast Route".</p>
<b>Error Messages</b>	% Priority must be 0 - 255
	% MD5 Key ID must be 1 - 255
	% Please bind WAN VLAN ID first.
	% Metric must be 1 - 65535
	% Hello Interval must be 1 - 65535
	% Dead Interval must be 1 - 65535
	% Auth Key lengths up to 8 characters
	^Parse error
	^Incomplete command
<b>Related Commands</b>	<pre>route ospf show interfaces lan</pre>

## interface lan ip directed-broadcast

To enable directed broadcast for LAN interface, use the **interface lan** global configuration command and **ip directed-broadcast** sub-level configuration command. To disable directed broadcast, use the **no** form of this command.

### Synopsis

```
(config)# interface lan
```

```
(config-if)# ip directed-broadcast [source-ip]
```

```
(config-if)# no ip directed-broadcast
```

<b>Option Description</b>	source-ip	Specifies to overwrite source IP
<b>Defaults</b>	Directed broadcast is disabled by default.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>This command only applies to LAN interface using the management VLAN.</li> <li>This feature supports directed broadcast for UDP packets only; ICMP is not included.</li> </ul>	
<b>Examples</b>	Enable directed broadcast. <pre>router# configure router(config)# interface lan router(config-if)# ip directed-broadcast router(config-if)# exit</pre>	
<b>Error Messages</b>	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show ip directed-broadcast	

## interface lan ip proxy-arp

To enable Proxy ARP for LAN interface, use the **interface lan** global configuration command and **ip proxy-arp** sub-level configuration command. To disable Proxy ARP, use the **no** form of this command.

### Synopsis

```
(config)# interface lan
```

```
(config-if)# ip proxy-arp
```

```
(config-if)# no ip proxy-arp
```

<b>Option Description</b>	N/A
<b>Defaults</b>	Disabled
<b>Command Modes</b>	Global configuration, sub-level configuration
<b>Usage Guidelines</b>	This command only applies to LAN interface using the management VLAN. Make sure the VLAN ID is created in advance before using it.
<b>Examples</b>	Enable Proxy ARP on interface LAN router# configure router(config)# interface lan router(config-if)# ip proxy-arp router(config-if)# exit
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	show ip proxy-arp

## interface lan bind vlan

To specify/modify the management VLN for LAN interface, use the **interface lan** global configuration command and **bind vlan** sub-level configuration command. To return management VLAN to default value, use the **no** form of this command.

### Synopsis

```
(config)# interface lan
```

```
(config-if)# bind vlan <vlan-id>
```

```
(config-if)# no bind vlan
```

<b>Option Description</b>	vlan-id	Ranges from 1 to 4094.
<b>Defaults</b>	Default management VLAN ID is 1.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• This command only applies to LAN interface using the management VLAN.</li><li>• Make sure the VLAN ID is created in advance before using it.</li></ul>	
<b>Examples</b>	Specify management VLAN ID (2). router# configure router(config)# interface lan router(config-if)# bind vlan 2 router(config-if)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces lan	

## interface lan mac-address

To configure virtual MAC address to LAN interface, use the **interface lan** global configuration command and **mac-address** sub-level configuration command. To return virtual MAC address to default, use the **default** argument of this command.

### Synopsis

```
(config)# interface lan  
(config-if)# mac-address {<mac-addr> |  
                        default}
```

<b>Option</b>	mac-addr	The virtual MAC address.
<b>Description</b>	default	Return to default value 00:00:00:00:00:00
<b>Defaults</b>	00:00:00:00:00:00	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	This command only applies to LAN interface using the management VLAN.	
<b>Examples</b>	Specify the virtual MAC (00:90:e8:12:34:56) to the interface using management VLAN. router# configure router(config)# interface lan router(config-if)# mac-address 00:90:e8:12:34:56 router(config-if)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces lan	

## show interfaces lan

To check the status of the default LAN interface, use the **show interfaces lan** command.

### Synopsis

```
# show interfaces lan
```

<b>Option</b>	N/A	
<b>Description</b>		
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# show interfaces lan Management VLAN ID : 1 LAN IP : 192.168.127.254 LAN Netmask : 255.255.255.0	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	interface lan	

## ip ping-response

When an ICMP echo request is received on the network interface, the command determines whether or not to send an ICMP echo response.

To disable this feature, use the **no** form of this command.

### **Synopsis**

(config-if)# **ip ping-response**

(config-if)# **no ip ping-response**

<b>Option</b>	ip	Configure IP Parameter
<b>Description</b>	ping-response no	Enable Ping Response/Disable Ping Response Negate Command
<b>Defaults</b>	Disabled on all WAN interfaces, otherwise, enabled.	
<b>Command Modes</b>	WAN Interface Configuration LAN Interface Configuration VLAN Interface Configuration Port-based Bridge Interface Configuration Zone-based Bridge Interface Configuration Cellular Interface Configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable ping response on the LAN interface. router# configure router(config)# interface lan router(config-if)# ip ping-response	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	



## show ip directed-broadcast

To check the directed broadcast settings of LAN or WAN interfaces on the router, use the **show ip directed-broadcast** command.

### Synopsis

# **show ip directed-broadcast**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	This command displays the settings of "Directed Broadcast" and "Source IP Overwrite" for all interfaces.
<b>Examples</b>	<pre>router# show ip directed-broadcast Interface          Directed Broadcast  Source IP Overwrite ----- WAN                Disable             Disable LAN20              Enable              Disable</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	interface lan ip directed-broadcast interface vlan ip directed-broadcast interface wan ip directed-broadcast

## show ip proxy-arp

To check the Proxy ARP settings of LAN or WAN interfaces on the router, use the **show ip proxy-arp** command.

### Synopsis

# **show ip proxy-arp**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	This command displays the settings of Proxy ARP for all interfaces.
<b>Examples</b>	<pre>router# show ip proxy-arp Interface          Proxy ARP ----- WAN                Disable LAN                Enable LAN8               Disable LAN6               Disable LAN7               Disable</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	interface lan ip proxy-arp interface vlan ip proxy-arp interface wan ip proxy-arp

## LAN (using non-management VLAN)

Information described in this chapter is only applied to the LAN interface which non-management VLAN belongs to. For the interface configured with the management VLAN, please refer to the chapter LAN (using management VLAN).

### interface vlan shutdown

To change the name of this LAN interface, use the **interface vlan** global configuration command and **name** sub-level configuration command. To exit sub-level configuration mode, use **exit** command.

#### Synopsis

```
(config)# interface vlan <vlan-id>
(config-vif)# {name <if-name> |
               exit |
               shutdown}
```

```
(config-vif)# no shutdown
```

<b>Option</b>	vlan-id	Ranges from 1 to 4094.
<b>Description</b>	name	Specifies the name of LAN interface
	if-name	The name of LAN interface, 1 to 12 characters.
	exit	Commit new settings and exit sub-level configuration mode.
	shutdown	Disables the LAN interface with selected VLAN ID.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• This command only applies to LAN interface using the non-management VLAN.</li><li>• The IP address of the LAN interface should be configured before using this command.</li><li>• Make sure the VLAN ID is created in advance before using it.</li></ul>	
<b>Examples</b>	Modify existing interface name from LAN2 to LAN2a and disable it for now. router# configure router(config)# interface vlan 2 router(config-vif)# name LAN2a router(config-vif)# shutdown router(config-vif)# exit	
<b>Error Messages</b>	% is over length. It must be 1 - 12.	
	vlan id does not exist!!	
	% Interface not exist! Please create interface and set ip and netmask first	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show interface vlan	

## no interface vlan

To remove a specific LAN interface with a specific VLAN ID, use the **no interface vlan** global configuration command.

### **Synopsis**

(config)# **no interface vlan** <vlan-id>

<b>Option Description</b>	vlan-id	VLAN ID to be removed.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• Range of VLAN ID is 1 to 4094.</li><li>• Make sure the VLAN ID has been assigned to a LAN interface in advance, otherwise, the error message '% interface vlan is not exist' will be displayed.</li></ul>	
<b>Examples</b>	Remove the interface which binds VLAN ID (5) from the router. router# configure router(config)# no interface vlan 5 router(config)# exit	
<b>Error Messages</b>	% interface vlan is not exist ^Parse error ^Incomplete command	
<b>Related Commands</b>	show interface vlan	

## interface vlan ip address

To configure a static IP address or a secondary IP address for LAN interface, use the **interface vlan** global configuration command and **ip address** sub-level configuration command. To disable dhcp option66/67 or remove a secondary IP address, use the **no** form of this command.

### Synopsis

```
(config)# interface vlan <vlan-id>
(config-vif)# ip address {<ip> <netmask> [secondary] |
                        dhcp [option66-67] }
```

```
(config-vif)# no ip address {<ip> <netmask> secondary |
                             dhcp option66-67}
```

<b>Option Description</b>	vlan-id	Ranges from 1 to 4094.
	ip	IP address
	netmask	Netmask of the static IP address
	secondary	Specifies a secondary IP address
	dhcp	Specifies dynamic IP type
	option66-67	Specifies DHCP option 66/67
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>This command only applies to LAN interface using the non-management VLAN.</li> <li>Make sure the LAN interface is created in advance before using it.</li> <li>The maximum number of secondary IPs allowed is 640.</li> <li>When deleting the non-management VLAN directly, any associated secondary IP addresses will be automatically removed.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Create LAN3's interface IP 30.0.0.1 and secondary IP addresses 30.0.0.2 and 20.0.0.2. <pre>router# configure router(config)# interface vlan 3 router(config-vif)# ip address 30.0.0.1 255.255.255.0 router(config-vif)# ip address 30.0.0.2 255.255.255.0 secondary router(config-vif)# ip address 20.0.0.2 255.255.255.0 secondary router(config-vif)# name LAN3 router(config-vif)# no shutdown router(config-vif)# exit router(config)# exit</pre> </li> <li>Remove secondary IP 30.0.0.2 of LAN3. <pre>router# configure router(config)# interface vlan 3 router(config-vif)# no ip address 30.0.0.2 255.255.255.0 secondary router(config-vif)#</pre> </li> <li>Remove the static IP address as well as all the secondary IP addresses of LAN3. <pre>router# configure router(config)# no interface vlan 3 router(config)# exit</pre> </li> </ul>	
<b>Error Messages</b>	% Invalid parameter!	
	vlan id does not exist!!	
	% Interface is not dynamic IP mode	
	% No match entry for Secondary IP, mask in the VLAN	
	% Interface not exist! Please create interface and set ip and netmask first	
	^Parse error	
<b>Related Commands</b>	^Incomplete command	
	show interface vlan	

## interface vlan ip ospf

To configure dynamic routing with OSPF interface settings and auth type for LAN, use the **interface vlan** global configuration command and **ip ospf** sub-level configuration command. To return to the default settings, use the **no** form of this command.

### Synopsis

```
(config)# interface vlan <vlan-id>
(config-vif)# ip ospf {cost <metric> |
                    priority <pri-number> |
                    hello-interval <h-second> |
                    dead-interval <d-second> |
                    auth {simple auth-key <key-string>|
                        md5 <key-id> auth-key <md5-key-string>} |
                    area <area-id>}

(config-vif)# no ip ospf [{cost |
                        priority |
                        hello-interval |
                        dead-interval |
                        auth}]
```

<b>Option Description</b>	vlan-id	Ranges from 1 to 4094.
	cost	Specifies Metric/Cost of OSPF
	metric	Metric/Cost of OSPF. Ranges from 1 to 65535.
	priority	Specifies router's priority
	pri-number	Priority. Ranges from 0 to 255.
	hello-interval	Specifies Hello packets which are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors.
	h-second	Interval of hello packets. Ranges from 1 to 65535 seconds.
	dead-interval	Specifies the dead-interval
	d-second	Interval of dead packets. Ranges from 1 to 65535 seconds.
	auth	Enables or disables auth function
	simple auth-key	Specifies simple auth type
	key-string	A key string for simple auth type. Maximum string length is 8.
	md5	Specifies MD5 auth type
	key-id	A key ID for MD5 hash calculation. Ranges from 1 to 255.
	auth-key	Specifies MD5 key for hash
	md5-key-string	A key string for MD5 auth type. Maximum string length is 8.
	area	Specifies the area ID
area-id	An area ID	
<b>Defaults</b>	<ul style="list-style-type: none"> <li>metric : 1</li> <li>h-interval : 10</li> <li>d-interval : 40</li> <li>pri-number : 1</li> </ul>	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>This command only applies to LAN interface using the non-management VLAN.</li> <li>Make sure the VLAN ID is created in advance before using it.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Specify Auth type to "none" with LAN interface (VLAN ID=3). <pre>router# configure router(config)# interface vlan 3 router(config-vif)# no ip ospf auth router(config-vif)# exit router(config)# exit</pre> </li> <li>Delete OSPF WAN interface. <pre>router# configure router(config)# interface vlan 3 router(config-vif)# no ip ospf</pre> </li> </ul>	

	<pre>router(config-vif)# exit router(config)# exit</pre> <ul style="list-style-type: none"> <li>Return hello interval to default. <pre>router# configure router(config)# interface vlan 3 router(config-vif)# no ip ospf hello-interval router(config-vif)# exit router(config)# exit</pre> </li> </ul> <p>* An illustrative example can be found in the chapter "Unicast Route".</p>
<b>Error Messages</b>	% Priority must be 0 - 255
	% MD5 Key ID must be 1 - 255
	% this IF is not existed in OSPF Interface list.
	% Metric must be 1 - 65535
	% Hello Interval must be 1 - 65535
	% Dead Interval must be 1 - 65535
	% Auth Key lengths up to 8 characters
<b>Related Commands</b>	route ospf
	show interface vlan

## interface vlan ip directed-broadcast

To enable directed broadcast for LAN interface, use the **interface vlan** global configuration command and **ip directed-broadcast** sub-level configuration command. To disable directed broadcast, use the **no** form of this command.

### Synopsis

```
(config)# interface vlan <vlan-id>
```

```
(config-vif)# ip directed-broadcast [source-ip]
```

```
(config-vif)# no ip directed-broadcast
```

<b>Option Description</b>	vlan-id	Ranges from 1 to 4094.
	directed-broadcast	Enables directed broadcast feature.
	source-ip	Specifies to overwrite source IP
<b>Defaults</b>	Directed broadcast is disabled by default.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>This command only applies to LAN interface using the non-management VLAN.</li> <li>Make sure the VLAN ID is created in advance before using it.</li> <li>This feature supports directed broadcast for UDP packets only; ICMP is not included.</li> </ul>	
<b>Examples</b>	Enable directed broadcast. <pre>router# configure router(config)# interface vlan 10 router(config-vif)# ip directed-broadcast router(config-vif)# exit</pre>	
<b>Error Messages</b>	^Parse error	
	vlan id does not exist!!	
<b>Related Commands</b>	^Incomplete command	
	show ip directed-broadcast	

## interface vlan ip proxy-arp

To enable Proxy ARP for LAN interface, use the **interface vlan** global configuration command and **ip proxy-arp** sub-level configuration command. To disable Proxy ARP, use the **no** form of this command.

### Synopsis

```
(config)# interface vlan <vlan-id>
```

```
(config-vif)# ip proxy-arp
```

```
(config-vif)# no ip proxy-arp <vlan-id>
```

<b>Option Description</b>	vlan-id	Ranges from 1 to 4094.
<b>Defaults</b>	Proxy ARP is disabled by default.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>This command only applies to LAN interface using the non-management VLAN.</li><li>Make sure the VLAN ID is created in advance before using it.</li></ul>	
<b>Examples</b>	Enable Proxy ARP on interface LAN6 which VLAN ID=6. router# configure router(config)# interface vlan 6 router(config-vif)# ip proxy-arp router(config-vif)# exit	
<b>Error Messages</b>	^Parse error vlan id does not exist!! ^Incomplete command	
<b>Related Commands</b>	show ip proxy-arp	

## interface vlan mac-address

To configure virtual MAC address to LAN interface, use the **interface vlan** global configuration command and **mac-address** sub-level configuration command. To return virtual MAC address to default, use the **default** argument of this command.

### Synopsis

```
(config)# interface vlan <vlan-id>
```

```
(config-vif)# mac-address {<mac-addr> |  
                        default}
```

<b>Option Description</b>	vlan-id	Ranges from 1 to 4094.
	mac-addr	The virtual MAC address.
	default	Return to default value 00:00:00:00:00:00
<b>Defaults</b>	00:00:00:00:00:00	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>This command only applies to LAN interface using the non-management VLAN.</li><li>Make sure the VLAN ID is created in advance before using it.</li></ul>	
<b>Examples</b>	Specify the virtual MAC (00:90:e8:12:34:57) to the interface using non-management VLAN. router# configure router(config)# interface vlan 2 router(config-vif)# mac-address 00:90:e8:12:34:57 router(config-vif)# exit	
<b>Error Messages</b>	vlan id does not exist!! ^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## show interfaces vlan

To check the status of the VLAN interfaces, use the **show interfaces vlan** command.

### **Synopsis**

# **show interfaces vlan** [<vlan-id>]

<b>Option Description</b>	vlan-id	Specifies a specific VLAN ID
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	Make sure the VLAN ID is created in advance before using it.	
<b>Examples</b>	router# show interfaces vlan 2  Interface Name: LAN2 State: Enable IP Address: 192.168.2.254 Subnet Mask: 255.255.255.0 VLAN ID: 2	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	interface vlan	



## LAN (EDF Series only)

Information described in this chapter only applies to LAN interfaces for the EDF Series.

Please note that settings and available options will vary between product models.

### interface lan name

To configure lan interface name, use the **interface lan** global configuration command and name sub-level configuration command sets.

#### Synopsis

```
(config)# interface lan
```

```
(config-if)# name <name>
```

<b>Option Description</b>	name	Interface name
<b>Defaults</b>	BRG_LAN	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Configure lan interface name. router# configure router(config)# interface lan router(config-if)# name LAN router(config-if)# exit router(config)# exit	
<b>Error Messages</b>	^Incomplete command  ^Parse error	
<b>Related Commands</b>	show interface lan	

### interface lan ip address static

To configure lan interface ip, use the **interface lan** global configuration command and **ip address static** sub-level configuration command sets. Please note that there is no secondary IP address for the EDF series.

#### Synopsis

```
(config)# interface lan
```

```
(config-if)# ip address static <ip> <mask> [<gateway>]
```

<b>Option Description</b>	interface	Interface setting
	lan	LAN setting
	ip address static	Settings for IP address, mask and gateway
<b>Defaults</b>	IP: 192.168.127.254 Mask: 255.255.255.0 Gateway: 0.0.0.0	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Configure lan interface ip. router# configure router(config)# interface lan router(config-if)# ip address static 192.168.127.254 255.255.255.0 (without setting gateway)	

	<pre>router(config-if)# ip address static 192.168.127.254 255.255.255.0 192.168.127.1      (with setting gateway) router(config-if)# exit router(config)# exit</pre>
<b>Error Messages</b>	% Configured IP Address is in the subnet of interface MGMT
	% Invalid parameter!
	^Incomplete command
	^Parse error
<b>Related Commands</b>	show interface lan

## interface lan ip name-server

To configure lan interface dns server ip, use the **interface lan** global configuration command and **ip name-server** sub-level configuration command sets. Up to 3 sets of IP addresses can be set. Please note that the EDF series only supports LAN.

### Synopsis

(config)# **interface lan**

(config-if)# **ip name-server <ipaddr1> [<ipaddr2> [<ipaddr3>]]**

<b>Option</b>	ipaddr1	IP address
<b>Description</b>	ipaddr2	IP address
	ipaddr3	IP address
<b>Defaults</b>	0.0.0.0	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>Configure lan interface dns server ip. router# configure router(config)# interface lan router(config-if)# ip name-server 1.1.1.1 1.1.1.2 1.1.1.3 router(config-if)# exit router(config)# exit</pre>	
<b>Error Messages</b>	% Invalid parameters!	
	^Parse error	
	% Incomplete command	
<b>Related Commands</b>	show interface lan	

## interface lan no ip address

To reset lan interface ip, use the **interface lan** global configuration command and **no ip address** sub-level configuration command sets.

### Synopsis

(config)# **interface lan**

(config-if)# **no ip address**

<b>Option</b>	N/A
<b>Description</b>	
<b>Defaults</b>	N/A
<b>Command Modes</b>	Global configuration, sub-level configuration

<b>Usage Guidelines</b>	N/A
<b>Examples</b>	Reset lan interface ip to default. router# configure router(config)# interface lan router(config-if)# no ip address router(config-if)# exit router(config)# exit
<b>Error Messages</b>	N/A
<b>Related Commands</b>	show interface lan

## show interface lan

To show lan interface, use **show interface lan** command.

### **Synopsis**

# **show interface lan**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Global configuration, sub-level configuration
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	Show lan interface. router# show interface lan Interface Name : BRG_LAN IP Address : 192.168.127.254 Subnet Mask : 255.255.255.0 Gateway : 0.0.0.0 DNS Server : 0.0.0.0 0.0.0.0 0.0.0.0
<b>Error Messages</b>	^Incomplete command ^Parse error
<b>Related Commands</b>	interface lan

## ip ping-response

When an ICMP echo request is received on the network interface, the command determines whether or not to send an ICMP echo response.

To disable this feature, use the **no** form of this command.

### **Synopsis**

(config-if)# **ip ping-response**

(config-if)# **no ip ping-response**

<b>Option</b>	ip	Configure IP Parameter
<b>Description</b>	ping-response no	Enable Ping Response/Disable Ping Response Negate Command
<b>Defaults</b>	Disabled on all WAN interfaces, otherwise, enabled.	
<b>Command Modes</b>	WAN Interface Configuration LAN Interface Configuration VLAN Interface Configuration Port-based Bridge Interface Configuration Zone-based Bridge Interface Configuration Cellular Interface Configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable ping response on the LAN interface. router# configure router(config)# interface lan router(config-if)# ip ping-response	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

# WAN

## interface wan shutdown

To disable WAN interface connection mode, use the **interface wan** global configuration command and **shutdown** sub-level configuration command. To enable WAN interface connection mode, use the **no** form of this command.

### Synopsis

```
(config)# interface wan  
(config-if)# {shutdown |  
              exit}
```

```
(config-if)# no shutdown
```

<b>Option</b>	shutdown	Specifies "Connection Mode" to Disable
<b>Description</b>	exit	Commit new settings and exit sub-level configuration mode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify "Connection Mode" to Enable. router# configure router(config)# interface wan router(config-if)# no shutdown router(config-if)# exit router(config)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces wan	

## interface wan ip address

To configure static/dhcp/pppoe for WAN interface, use the **interface wan** global configuration command and **ip address** sub-level configuration command sets. To disable dhcp option66/67 or remove a secondary IP address, use the **no** form of this command.

### Synopsis

```
(config)# interface wan
(config-if)# ip address {static <wan-ip> <netmask> [<gateway> | secondary] |
                        dhcp [option66-67] |
                        pppoe <user-name> <password> <hostname>}

(config-if)# no ip address {static <ip> <netmask> secondary |
                           dhcp option66-67}
```

<b>Option Description</b>	static	Specifies static IP type
	wan-ip	IP address
	netmask	Netmask of the static IP address
	gateway	Gateway IP address
	dhcp	Specifies dynamic IP type
	secondary	Specifies a secondary IP address
	option66-67	Specifies DHCP option 66/67
	pppoe	Specifies PPPoE type
	user-name	The User Name for logging in to the PPPoE server. Maximum string length is 30.
	password	The login password for the PPPoE server. Maximum string length is 30.
	hostname	User-defined Host Name of this PPPoE server. Maximum string length is 30.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify DHCP type and enable DHCP option 66/67. router# configure router(config)# interface wan router(config-if)# ip address dhcp option66-67 router(config-if)# exit router(config)# exit	
<b>Error Messages</b>	% is over length. It must be 1 - 30.	
	% Interface is not dynamic IP mode	
	% No match entry for Secondary IP, mask for WAN	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show interfaces wan	

## interface wan ip pptp

To configure PPTP dialup when using dynamic IP type for WAN interface, use the **interface wan** global configuration command and **ip pptp** sub-level configuration command sets. To disable PPTP, use the **no** form of this command.

### Synopsis

```
(config)# interface wan  
(config-if)# ip pptp {<pptp-ip> <user-name> <password> |  
                mppe}
```

```
(config-if)# no ip pptp [mppe]
```

<b>Option Description</b>	pptp-ip	The PPTP service IP address
	user-name	The Login username when dialing up to PPTP service. Maximum string length is 30.
	password	The password for dialing the PPTP service. Maximum string length is 30.
	mppe	Enables or disables the MPPE encryption
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify the PPTP server IP (192.168.1.100), user name (demo-usr) and password (demo-pwd). router# configure router(config)# interface wan router(config-if)# ip pptp 192.168.1.100 demo-usr demo-pwd router(config-if)# exit	
<b>Error Messages</b>	% is over length. It must be 1 - 30.	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces wan	

## interface wan ip name-server

To configure DNS servers for WAN interface, use the **interface wan** global configuration command and **ip name-server** sub-level configuration command.

### Synopsis

```
(config)# interface wan
(config-if)# ip name-server <dns1> [<dns2> [<dns3>]]
```

<b>Option Description</b>	dns1	1st The DNS IP address
	dns2	2nd The DNS IP address
	dns3	3rd The DNS IP address
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	The priority of a manually configured DNS will be higher than the DNS from the PPPoE or DHCP server.	
<b>Examples</b>	Specify the DNS server 1 IP (8.8.8.8) and DNS server 2 IP (9.9.9.9). router# configure router(config)# interface wan router(config-if)# ip name-server 8.8.8.8 9.9.9.9 router(config-if)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces wan	

## interface wan ip ospf

To configure dynamic routing with OSPF interface settings and auth type for WAN, use the **interface wan** global configuration command and **ip ospf** sub-level configuration command sets. To return to the default settings, use the **no** form of this command.

### Synopsis

```
(config)# interface wan
(config-if)# ip ospf {cost <metric> |
    priority <pri-number> |
    hello-interval <h-second> |
    dead-interval <d-second> |
    auth {simple auth-key <key-string>|
        md5 <key-id> auth-key <md5-key-string>} |
    area <area-id>}
(config-if)# no ip ospf [{cost |
    priority |
    hello-interval |
    dead-interval |
    auth}]
```

<b>Option Description</b>	cost	Specifies Metric/Cost of OSPF
	metric	Metric/Cost of OSPF. Ranges from 1 to 65535.
	priority	Specifies router's priority
	pri-number	Priority. Ranges from 0 to 255.
	hello-interval	Specifies Hello packets which are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors.
	h-second	Interval of hello packets. Ranges from 1 to 65535 seconds.
	dead-interval	Specifies the dead-interval
	d-second	Interval of dead packets. Ranges from 1 to 65535 seconds.
	auth	Enables or disables auth function
	simple auth-key	Specifies simple auth type



	key-string	A key string for simple auth type. Maximum string length is 8.
	md5	Specifies MD5 auth type
	key-id	A key ID for MD5 hash calculation. Ranges from 1 to 255.
	auth-key	Specifies MD5 key for hash
	md5-key-string	A key string for MD5 auth type. Maximum string length is 8.
	area	Specifies the area ID
	area-id	An area ID
<b>Defaults</b>		<ul style="list-style-type: none"> <li>metric : 1</li> <li>h-interval : 10</li> <li>d-interval : 40</li> <li>pri-number : 1</li> </ul>
<b>Command Modes</b>		Global configuration, sub-level configuration
<b>Usage Guidelines</b>		N/A
<b>Examples</b>		<ul style="list-style-type: none"> <li>Specify Auth type to "none".  <pre>router# configure router(config)# interface wan router(config-if)# no ip ospf auth router(config-if)# exit router(config)# exit</pre> </li> <li>Delete OSPF WAN interface.  <pre>router# configure router(config)# interface wan router(config-if)# no ip ospf router(config-if)# exit router(config)# exit</pre> </li> <li>Return hello interval to default.  <pre>router# configure router(config)# interface wan router(config-if)# no ip ospf hello-interval router(config-if)# exit router(config)# exit</pre> </li> </ul> <p>* An illustrative example can be found in the chapter "Unicast Route".</p>
<b>Error Messages</b>		% Priority must be 0 - 255
		% MD5 Key ID must be 1 - 255
		% Please bind WAN VLAN ID first.
		% Metric must be 1 - 65535
		% Hello Interval must be 1 - 65535
		% Dead Interval must be 1 - 65535
		% Auth Key lengths up to 8 characters
		^Parse error
		^Incomplete command
<b>Related Commands</b>		route ospf show interfaces wan

## interface wan ip directed-broadcast

To enable directed broadcast for WAN interface, use the **interface wan** global configuration command and **ip directed-broadcast** sub-level configuration command. To disable directed broadcast, use the **no** form of this command.

### Synopsis

(config)# **interface wan**

(config-if)# **ip directed-broadcast** [**source-ip**]

(config-if)# **no ip directed-broadcast**

<b>Option Description</b>	source-ip	Specifies to overwrite source IP
<b>Defaults</b>	Directed broadcast is disabled by default.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	This feature supports directed broadcast for UDP packets only; ICMP is not included.	
<b>Examples</b>	Enable directed broadcast. router# configure router(config)# interface wan router(config-if)# ip directed-broadcast router(config-if)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces wan show ip directed-broadcast	

## interface wan ip proxy-arp

To enable Proxy ARP for WAN interface, use the **interface wan** global configuration command and **ip proxy-arp** sub-level configuration command. To disable Proxy ARP, use the **no** form of this command.

### Synopsis

```
(config)# interface wan
```

```
(config-if)# ip proxy-arp
```

```
(config-if)# no ip proxy-arp
```

<b>Option Description</b>	N/A
<b>Defaults</b>	Proxy ARP is disabled by default.
<b>Command Modes</b>	Global configuration, sub-level configuration
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	Enable Proxy ARP on interface WAN. router# configure router(config)# interface wan router(config-if)# ip proxy-arp router(config-if)# exit
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	show ip proxy-arp

## interface wan bind vlan

To bind VLAN to WAN interface, use the **interface wan** global configuration command and **bind vlan** sub-level configuration command. To remove VLAN from WAN interface, use the **no** form of this command.

### Synopsis

```
(config)# interface wan
```

```
(config-if)# bind vlan <vlan-id>
```

```
(config-if)# no bind vlan
```

<b>Option Description</b>	vlan-id	Ranges from 1 to 4094.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	Make sure the VLAN ID is created in advance before using it.	
<b>Examples</b>	Specify VLAN ID (2) for WAN interface. router# configure router(config)# interface wan router(config-if)# bind vlan 2 router(config-if)# exit	
<b>Error Messages</b>	vlan id does not exist!! ^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces wan	

## interface wan mac-address

To configure virtual MAC address to WAN interface, use the **interface wan** global configuration command and **mac-address** sub-level configuration command. To return virtual MAC address to default, use the **default** argument of this command.

### Synopsis

```
(config)# interface wan  
(config-if)# mac-address {<mac-addr> |  
                        default}
```

<b>Option</b>	mac-addr	The virtual MAC address.
<b>Description</b>	default	Return to default value 00:00:00:00:00:00
<b>Defaults</b>	00:00:00:00:00:00	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify the virtual MAC (00:90:e8:12:34:58) to the WAN interface. router# configure router(config)# interface wan router(config-if)# mac-address 00:90:e8:12:34:58 router(config-if)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces wan	

## show interfaces wan

To check the settings of WAN interface or status of the WAN interface, use the **show interfaces wan** command.

### Synopsis

# **show interfaces wan** [**status** | <wan-id>]

<b>Option</b>	status	Specifies to display WAN interface information
<b>Description</b>	wan-id	Integer value starting from 1. This option is only valid for the product which supports multi-WAN interfaces.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>If the connection type is "Static IP", suggest use #show interfaces wan to display the settings.</li> <li>If the connection type is "Dynamic IP" or "PPPoE", suggest use #show interfaces wan status to display the status.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>When the connection type is Static IP, display current settings.  <pre>router# show interfaces wan WAN Vlan ID           : 3 Connect Mode      : Enable Connect Type      : Static IP Address        : 192.168.3.154 Netmask           : 255.255.255.0 Gateway           : 0.0.0.0 PPTP Connection   : Disable PPTP IP Address   : 0.0.0.0 PPTP User Name    : PPTP Password     : ***** PPTP MPPE Encryption: Disable DNS Server        : 0.0.0.0 0.0.0.0 0.0.0.0</pre> </li> <li>When the connection type is Dynamic IP, display current status.  <pre>router# show interfaces wan status WAN Connect Type      : DHCP IP Address        : 10.123.24.12 Netmask           : 255.255.252.0 Gateway           : 10.123.24.1 DNS Server        : 10.123.200.11 10.123.200.12 0.0.0.0</pre> </li> </ul>	
<b>Error Messages</b>	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	interface wan	

## ip ping-response

When an ICMP echo request is received on the network interface, the command determines whether or not to send an ICMP echo response.

To disable this feature, use the **no** form of this command.

### **Synopsis**

(config-if)# **ip ping-response**

(config-if)# **no ip ping-response**

<b>Option</b>	ip	Configure IP Parameter
<b>Description</b>	ping-response	Enable Ping Response/Disable Ping Response
	no	Negate Command
<b>Defaults</b>	Disabled on all WAN interfaces, otherwise, enabled.	
<b>Command Modes</b>	WAN Interface Configuration LAN Interface Configuration VLAN Interface Configuration Port-based Bridge Interface Configuration Zone-based Bridge Interface Configuration Cellular Interface Configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable ping response on the WAN interface. router# configure router(config)# interface wan router(config-if)# ip ping-response	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## WAN2/DMZ

### interface wan dmz

To enable DMZ on specific WAN interface, use the **interface wan dmz** command.

#### Synopsis

(config-if)# **dmz**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Sub-level configuration
<b>Usage Guidelines</b>	There is only one WAN interface supporting DMZ: the WAN2 on the EDR-G9004 models.
<b>Examples</b>	<pre>router(config)# interface wan 2 router(config-if)# dmz router(config-if)# exit</pre>
<b>Error Messages</b>	% DMZ mode can only be enabled on WAN2. % DMZ mode can only be enabled on interface with static IP. % Only one of WAN Redundancy and DMZ functionality can be enabled.
<b>Related Commands</b>	no dmz show interface wan <wanid>

### interface wan no dmz

To disable DMZ on specific WAN interface, use the **interface wan no dmz** command

#### Synopsis

(config-if)# **no dmz**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Sub-level configuration
<b>Usage Guidelines</b>	There is only one WAN interface supporting DMZ: the WAN2 on the EDR-G9004 models.
<b>Examples</b>	<pre>router(config)# interface wan 2 router(config-if)# no dmz router(config-if)# exit</pre>
<b>Error Messages</b>	% DMZ mode can only be enabled on WAN2.
<b>Related Commands</b>	dmz show interface wan <wanid>

# Maximum Transmission Unit

## mtu

To specify or modify maximum transmission unit (MTU) on an interface, use the **mtu** global configuration command set.

### Synopsis

(config)# **mtu** <if-name> <size>

<b>Option</b>	if-name	The name of LAN/WAN interface, if-name is case-sensitive.
<b>Description</b>	size	MTU size in bytes. Ranges from 68 to 1578.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify MTU of interface (LAN10) to 1512. router# configure router(config)# mtu LAN10 1512	
<b>Error Messages</b>	% Invalid MTU size . (68~1578) % Invalid Input Interface Name ^Parse error ^Incomplete command	
<b>Related Commands</b>	show mtu	

## show mtu

To check maximum transmission unit (MTU) settings on the router, use the **show mtu** command.

### Synopsis

# **show mtu**

<b>Option</b>	N/A	
<b>Description</b>		
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router # show mtu MTU Adjustment Interface                    MTU -----                    --- WAN                            1500 LAN20                          1500 LAN10                          1512	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	mtu	



# Bridge Group Interface

## interface bridge

To configure a port-based bridge interface, use the **interface bridge** global configuration command and related sub-level configuration command sets. To exit sub-level configuration mode, use **exit** command.

### Synopsis

#### Enable / Disable a port-based bridge interface

```
(config)# interface bridge
```

```
(config-brg)# no shutdown
```

```
(config-brg)# shutdown
```

#### Set IP address of port-based bridge interface

```
(config-brg)# ip address <brg-ip> <netmask>
```

#### Set name of the bridge interface

```
(config-brg)# name <brg-name>
```

#### Save and Exit port-based bridge interface configuration

```
(config-brg)# exit
```

<b>Option</b>	ip address	Specifies IP address of the bridge interface
<b>Description</b>	brg-ip	IP address
	netmask	Netmask of the static IP address
	name	Specifies the name of the bridge interface
	brg-name	The name of bridge interface, 1 to 12 characters.
	exit	Commit new settings and exit sub-level configuration mode.
	shutdown	Disables the bridge interface.
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• Bridge member ports can be configured via <b>interface ethernet</b> and its sub-level <b>bridge group</b> commands.</li><li>• Maximum number of bridge interface is one which means either a port-based bridge or a zone-based bridge interface can be configured.</li><li>• Enabling the '<b>no shutdown</b>' command when the zone-based bridge is already active will switch to port-based bridge mode while disabling the zone-based bridge simultaneously.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Specify PORT5, PORT6, PORT7 as port-based bridge members.<pre>router# configure router(config)# interface ethernet 1/5 router(config-if)# bridge group router(config-if)# exit router(config)# interface ethernet 1/6 router(config-if)# bridge group router(config-if)# exit router(config)# interface ethernet 1/7 router(config-if)# bridge group router(config-if)# exit router(config)#</pre></li><li>• Specify the IP address and netmask of the port-based bridge interface.<pre>router# configure router(config)# interface bridge router(config-brg)# ip address 192.168.57.254 255.255.255.0 router(config-brg)# exit router(config)#</pre></li><li>• Specify the name of the port-based bridge interface.<pre>router# configure router(config)# interface bridge router(config-brg)# name BRG_LAN</pre></li></ul>	

	<pre>router(config-brg)# exit router(config)#</pre> <ul style="list-style-type: none"> <li>• Enable the port-based bridge interface. <pre>router# configure router(config)# interface bridge router(config-brg)# no shutdown router(config-brg)# exit router(config)#</pre> </li> </ul>
<b>Error Messages</b>	<pre>% is over length. It must be 1 - 12. ^Parse error ^Incomplete command</pre>
<b>Related Commands</b>	<pre>show interfaces bridge interface ethernet bridge</pre>

## interface ethernet bridge

To select the Ethernet interface as a member port of the port-based bridge interface, use the **interface ethernet** global configuration command and related sub-level configuration command sets. To remove Ethernet interface from bridge member ports, use **no** form of this command.

### Synopsis

(config)# **interface ethernet** <mod-port>

(config-if)# **bridge group**

(config-if)# **no bridge group**

<b>Option</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
<b>Description</b>	bridge group	Adds/removes the Ethernet interface to/from bridge member ports
<b>Defaults</b>	Unselected.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• If bridge member is empty, remember to disable the bridge interface by using <b>interface bridge</b> and <b>shutdown</b> command.</li> <li>• Once all member ports have been specified, use <b>interface bridge</b> and <b>no shutdown</b> command to let settings take effect.</li> <li>• When the sub-level command '<b>bridge group</b>' is specified, an additional VLAN ID will be created automatically.</li> <li>• If you're discontinuing the use of a VLAN ID linked to a bridge interface, ensure the bridge interface is disabled and remove all associated VLAN IDs by using 'no vlan create' command.</li> <li>• At least two member ports are selected before using this bridge interface.</li> <li>• Maximum number of bridge member of TN-4908 series is 8.</li> <li>• Maximum number of bridge member of TN-4916 series is 16.</li> </ul>	
<b>Examples</b>	Specify PORT5, PORT6, PORT7 as port-based bridge members. (A comprehensive example can be found in the command " <b>interface bridge</b> ") <pre> router# configure router(config)# interface ethernet 1/5 router(config-if)# bridge group router(config-if)# exit router(config)# interface ethernet 1/6 router(config-if)# bridge group router(config-if)# exit router(config)# interface ethernet 1/7 router(config-if)# bridge group router(config-if)# exit router(config)# interface bridge router(config-brg)# no shutdown router(config-brg)# exit           </pre>	
<b>Error Messages</b>	% Illegal parameter. ^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces bridge	

## interface zone-base-bridge

To configure a zone-based bridge interface, use the **interface zone-base-bridge** global configuration command and related sub-level configuration command sets. To exit sub-level configuration mode, use **exit** command.

### Synopsis

#### Enable / Disable a zone-based bridge interface

```
(config)# interface zone-base-bridge
(config-brg)# no shutdown
(config-brg)# shutdown
```

#### Set IP address of zone -based bridge interface

```
(config-brg)# ip address <brg-ip> <netmask>
```

#### Set name of the bridge interface

```
(config-brg)# name <brg-name>
```

#### Save and Exit zone -based bridge interface configuration

```
(config-brg)# exit
```

<b>Option Description</b>	ip address	Specifies IP address of the bridge interface
	brg-ip	IP address
	netmask	Netmask of the static IP address
	name	Specifies the name of the bridge interface
	brg-name	The name of bridge interface, 1 to 12 characters.
	exit	Commit new settings and exit sub-level configuration mode.
	shutdown	Disables the bridge interface.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• Bridge member ports can be configured via <b>interface vlan zone-base-bridge</b> commands.</li><li>• Maximum number of bridge interface is one which means either a port-based bridge or a zone-based bridge interface can be configured.</li><li>• Enabling the 'no shutdown' command when the port-based bridge is already active will switch to zone-based bridge mode while disabling the port-based bridge simultaneously.</li><li>• Ensure to designate the PVID for the ports allocated to the zone-based bridge interface.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Assign VLAN(5) to PORT5 and PORT6 and VLAN(8) to PORT7 and PORT8. Specify VLAN(5), VLAN(8) as zone-based bridge members.<pre>router# configure router(config)# interface ethernet 1/5 router(config-if)# switchport access vlan 5 router(config-if)# exit router(config)# interface ethernet 1/6 router(config-if)# switchport access vlan 5 router(config-if)# exit router(config)# interface ethernet 1/7 router(config-if)# switchport access vlan 8 router(config-if)# exit router(config)# interface ethernet 1/8 router(config-if)# switchport access vlan 8 router(config-if)# exit router(config)# interface vlan 5 zone-base-bridge 1 z1 router(config)# interface vlan 8 zone-base-bridge 2 z2 router(config)# exit</pre></li><li>• Specify the IP address and netmask of the zone-based bridge interface.<pre>router# configure router(config)# interface zone-base-bridge router(config-brg)# ip address 192.168.58.254 255.255.255.0</pre></li></ul>	

	<pre>router(config-brg)# exit</pre> <ul style="list-style-type: none"> <li>Specify the name of the zone-based bridge interface. <pre>router# configure router(config)# interface zone-base-bridge router(config-brg)# name BRG_LAN router(config-brg)# exit</pre> </li> <li>Enable the zone-based bridge interface. <pre>router# configure router(config)# interface zone-base-bridge router(config-brg)# no shutdown router(config-brg)# exit</pre> </li> </ul>
<b>Error Messages</b>	% is over length. It must be 1 - 12. ^Parse error ^Incomplete command
<b>Related Commands</b>	show interfaces zone-base-bridge

## interface vlan zone-base-bridge

To configure bridge members of the zone-based interface, use the **interface vlan** global configuration command and **name** sub-level configuration command.

### Synopsis

(config)# **interface vlan** <vlan-id> **zone-base-bridge** <zone-index> <zone-name>

<b>Option Description</b>	vlan-id	VLAN ID to be selected into a zone-based bridge. Ranges from 1 to 4094.
	zone-base-bridge	Specifies the a zone-based bridge
	zone-index	Ranges from 1 to 4.
	zone-name	Name of specified zone-based bridge, 1 to 12 characters.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>This command only applies to LAN interface using the non-management VLAN.</li> <li>Once all member ports have been specified, use <b>interface zone-base-bridge</b> and <b>no shutdown</b> command to let settings take effect.</li> <li>At least two member ports are selected before using this bridge interface.</li> <li>Only one VLAN segment (VID) is allowed in each zone.</li> <li>Eligible VIDs should be configured before selecting the bridge member.</li> <li>Maximum number of bridge member of TN-4900 series is 4.</li> </ul>	
<b>Examples</b>	Specify VLAN(5), VLAN(8) as zone-based bridge members. (A comprehensive example can be found in the command " <b>interface zone-base-bridge</b> ") <pre>router# configure router(config)# interface vlan 5 zone-base-bridge 1 z1 router(config)# interface vlan 8 zone-base-bridge 2 z2 router(config)# exit</pre>	
<b>Error Messages</b>	% is over length. It must be 1 - 12. vlan id does not exist!! ^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## show interfaces bridge

To check the status of the port-based bridge interface, use the **show interfaces bridge** command.

### Synopsis

# **show interfaces bridge**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router# show interfaces bridge Interface Name: BRG_LAN State: Enable IP Address: 192.168.57.254 Subnet Mask: 255.255.255.0
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	interface bridge interface zone-base-bridge interface vlan zone-base-bridge

## show interfaces zone-base-bridge

To check the status of the zone-based bridge interface, use the **show interfaces zone-base-bridge** command.

### Synopsis

# **show interfaces zone-base-bridge**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	router # show interfaces zone-base-bridge Interface Name: BRG_LAN State: Enable IP Address: 191.168.58.254 Subnet Mask: 255.255.255.0
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	interface bridge interface zone-base-bridge interface vlan zone-base-bridge

## ip ping-response

When an ICMP echo request is received on the network interface, the command determines whether or not to send an ICMP echo response.

To disable this feature, use the **no** form of this command.

### **Synopsis**

(config-if)# **ip ping-response**

(config-if)# **no ip ping-response**

<b>Option</b>	ip	Configure IP Parameter
<b>Description</b>	ping-response	Enable Ping Response/Disable Ping Response
	no	Negate Command
<b>Defaults</b>	Disabled on all WAN interfaces, otherwise, enabled.	
<b>Command Modes</b>	WAN Interface Configuration LAN Interface Configuration VLAN Interface Configuration Port-based Bridge Interface Configuration Zone-based Bridge Interface Configuration Cellular Interface Configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable ping response on the Bridge interface. router# configure router(config)# interface bridge router(config-if)# ip ping-response	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	N/A	

## LAN Bypass Gen 3 (EDF-G1002 only)

These commands are available for EDF-G1002 only.

### bypass lan shutdown/bypass lan shutdown halted

To configure LAN bypass, specify the conditions under which bypass will be activated with **bypass lan shutdown** or **bypass lan shutdown halted**.

#### Synopsis

(config)# **bypass lan shutdown**

(config)# **bypass lan shutdown halted**

(config)# **no bypass lan**

<b>Option</b>	no	Disable
<b>Description</b>	shutdown	LAN bypass during power off
	halted	LAN bypass during system halts, including power off
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Firewall/VPN Router 00019(config)# bypass lan shutdown halted Firewall/VPN Router 00019(config)# exit	
<b>Error Messages</b>	^Incomplete command	
	^Parse error	
<b>Related Commands</b>	show bypass	



## show bypass

To show LAN bypass status, use **show bypass** command.

### Synopsis

# **show bypass**

<b>Option</b>	show	Show configuration
<b>Description</b>	bypass	Display LAN bypass configuration
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Firewall/VPN Router 00019# show bypass GEN3 LAN Bypass: Mode : Disabled  Runtime Status: Enable : Disable Auto Recovery Time : 5 (Minute) Remain time to timeout : 43200 (Second)	
<b>Error Messages</b>	^Incomplete command ^Parse error	
<b>Related Commands</b>	N/A	

## bypass lan runtime start/duration/stop

To configure runtime LAN bypass settings, use these commands. Runtime LAN bypass settings are not stored in configuration files, and are not persistent.

### Synopsis

(config)# **bypass lan runtime start**

(config)# **bypass lan runtime duration** <minutes>

(config)# **bypass lan runtime stop**

<b>Option</b>	runtime	Runtime bypass is an action and will not be set to configuration file
<b>Description</b>	start	Start bypass
	stop	Stop bypass
	duration	Set duration time of auto recovery
	minutes	0 to 43200 minutes. (0 is forever)
<b>Defaults</b>	minutes: 0	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Set how to act bypass in runtime.	
<b>Examples</b>	Firewall/VPN Router 00019(config)# bypass lan runtime start Firewall/VPN Router 00019(config)# bypass lan runtime duration 10 Firewall/VPN Router 00019(config)# exit	
<b>Error Messages</b>	Must be 0~43200. (0 is forever) ^Incomplete command ^Parse error	
<b>Related Commands</b>	show bypass	

## Virtual Interface (Loopback Interface)

### interface loopback

To specify or modify virtual interface, use the **interface loopback** configuration command set.

#### Synopsis

```
(config)# interface loopback <id>\
```

```
(config-if)# name <name>
```

<b>Option Description</b>	name	Loopback interface name
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set loopback interface name router# configure router(config)# interface loopback 0 router(config-vir_if)# name aaa router(config-vir_if)# exit	
<b>Error Messages</b>	Same interface name with other interface	
	%s is an invalid system symbol	
	^Incomplete command	
	^Parse error	
<b>Related Commands</b>	N/A	

### loopback ip/mask

To configure loopback interface IP address and mask, use the **loopback ip/mask** command.

#### Synopsis

```
(config-if)# ip address {ip} {mask}
```

<b>Option Description</b>	ip	Loopback interface IP address
	mask	Loopback interface IP mask
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set loopback interface ip/mask router# configure router(config)# interface loopback 0 router(config-vir_if)# ip address 172.21.1.1 255.255.255.0 router(config-vir_if)# exit	
<b>Error Messages</b>	N/A	
<b>Related Commands</b>	show interface loopback	



## shutdown/no shutdown

To disable or enable loopback interface, use the **shutdown** or **no shutdown** command.

### Synopsis

<b>Option</b>	shutdown	Enable loopback interface
<b>Description</b>	no shutdown	Disable loopback interface
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set loopback interface name router# configure router(config)# interface loopback 0 router(config-vir_if)# shutdown router(config-vir_if)# exit  Set loopback interface ip/mask router# configure router(config)# interface loopback 0 router(config-vir_if)# no shutdown router(config-vir_if)# exit	
<b>Error Messages</b>	N/A	
<b>Related Commands</b>	show interface loopback	

## Out of Band Management (EDF-G1002 only)

Please note that the following commands are for EDF-G1002 only.

### interface mgmt ip address static

To configure the out of band management interface IP address, use the **interface mgmt** global configuration command and ip sub-level configuration command sets.

#### Synopsis

(config)# **interface mgmt**

(config-mgmt)# **ip address static** <ip> <mask>

<b>Option</b>	ip	Interface IP address
<b>Description</b>	mask	Mask IP address
<b>Defaults</b>	IP: 192.168.1.1 Mask: 255.255.255.0	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Configure mgmt interface ip. router# configure router(config)# interface mgmt router(config-mgmt)# ip address static 192.168.1.1 255.255.255.0 router(config-mgmt)# exit router(config)# exit	
<b>Error Messages</b>	% Configured IP Address is in the subnet of interface BRG_LAN % Invalid parameter! ^Incomplete command ^Parse error	
<b>Related Commands</b>	show ip oob management	

### hardware-interface oob

To enable Othe out of band management interface, use the **hardware-interface oob** command.

#### Synopsis

(config)# **hardware-interface oob**

(config)# **no hardware-interface oob**

<b>Option</b>	no	Disable
<b>Description</b>		
<b>Defaults</b>	Enabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable OOB mgmt interface router# configure router(config)# hardware-interface oob router(config)# exit	
<b>Error Messages</b>	^Incomplete command ^Parse error	
<b>Related</b>	show hardware-interface	

## show oob status

To show the out of band management port information, use the **show oob status** command.

### Synopsis

# **show oob status**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Global configuration
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	Show OOB mgmt port information router# show oob status Link Status 1G-Full
<b>Error Messages</b>	^Incomplete command ^Parse error
<b>Related Commands</b>	show hardware-interface show ip oob management show system

## show hardware-interface

To show the out of band management interface status, use the **show hardware-interface** command.

### Synopsis

# **show hardware-interface**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Global configuration
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	Show OOB mgmt interface status router# show hardware-interface Out of Band Management: Enabled
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	show ip oob management show oob status show system hardware-interface oob

## show ip oob management

To show IP address information for the out of band management interface, use **show ip oob management** command.

### **Synopsis**

# **show ip oob management**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Global configuration
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	Show OOB mgmt interface information. router# show ip oob management IPv4 IP Address: 192.168.1.1 Netmask   : 255.255.255.0
<b>Error Messages</b>	^Incomplete command ^Parse error
<b>Related Commands</b>	show hardware-interface show oob status show system interface mgmt ip address static

## show system

To show out-of-band management port MAC information, use **show system** command.

### **Synopsis**

# **show system**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Global configuration
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	Show OOB mgmt port mac information router# show system System Information System Name : Industrial NGFW 00001 System Location : Device Location System Description : Maintainer Information : Host Name : Industrial-NGFW-00001 MAC Address : 00:90:E8:00:00:01 OOB MAC Address : 00:90:E8:00:00:02 Serial No. : MOXA00000001 System Uptime : 0d2h44m4s CPU Frequency : 1600 MHz
<b>Error Messages</b>	^Incomplete command ^Parse error
<b>Related Commands</b>	show hardware-interface show ip oob management show oob status



## Link Fault Passthrough

Please note that settings and available options will vary by product model.

### interface lfp

To enable Link Fault Passthrough, use **interface lfp** command.

#### **Synopsis**

(config)# **interface lfp**

(config)# **no interface lfp**

<b>Option Description</b>	no	Disable
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	If LFP ports are illegal (not the member of the port-based bridge), then enable operations will be rejected.	
<b>Examples</b>	router(config)# interface lfp router(config)# exit	
<b>Error Messages</b>	When LFP ports are not member of the port-based bridge % LFP ports should be members of the bridge.	
<b>Related Commands</b>	show interface lfp	

### interface lfp ports

Use this command to configure Link Fault Passthrough ports. The availability of LFP port configuration is contingent on product settings. LFP ports are not configurable on the EDR-G9004.

#### **Synopsis**

(config)# **interface lfp ports** <port1> <port2>

<b>Option Description</b>	port1	The name of the first LFP port
	port2	The name of the second LFP port
<b>Defaults</b>	N/A	
<b>Command Modes</b>	By product: the default LFP ports for EDR-G9004 are 1/3 & 1/4 and not configurable.	
<b>Usage Guidelines</b>	If LFP ports are configurable, any ethernet port name could be configured. If the LFP ports are illegal (not bridge port), the LFP state will be disabled.	
<b>Examples</b>	Configure ethernet port 1/3 & 1/4 as LFP ports router# configure router(config)# interface lfp port 1/3 1/4 router(config)# exit	
<b>Error Messages</b>	When LFP ports are not configurable. % LFP ports are fixed and not configurable When LFP ports name is wrong % Invalid port1 name % Invalid port2 name When LFP ports name is the same % LFP port1 and port2 should be different	
<b>Related Commands</b>	show interface lfp	

## show interfaces lfp

To show Link Fault Passthrough information, use the **show interfaces lfp** command.

### Synopsis

# **show interfaces lfp**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Global configuration
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	# show interfaces lfp Link Fault Passthrough Setting State : Disable Ports : 1/3, 1/4
<b>Error Messages</b>	N/A
<b>Related Commands</b>	interface lfp no interface lfp interface lfp ports

## Fault LED (TN-4900 only)

This command is used to configure the fault LED for different settings. To set up the default configuration, use **no led mode** command. This command is for TN-4900 series only.

### led mode

#### Synopsis

(config)# **[no] led mode { 0 | 1 }**

<b>Option Description</b>	0	Moxa default/System default alarm
	1	Advanced/Configuration change alarm
<b>Defaults</b>	0	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify/modify Fault LED behavior with 0. router# configure router(config)# led mode 0 router(config)# exit	
<b>Error Messages</b>	% Mode must be 0 or 1. ^Parse error ^Incomplete command	
<b>Related Commands</b>	warning-notification port-event activewarning-notification port-event event warning-notification system-event pwr1-trans-off active warning-notification system-event pwr2-trans-off active warning-notification system-event pwr1-trans-on active warning-notification system-event pwr2-trans-on active reload factory-defaultcopy tftp <IPV4ADDR:tftp_ip> config-file <STRING:filename>	

# Routing

## Unicast Route

### ip route static

To create a static route entry, use the **ip route static** global configuration command. To delete the static route entry, use the **no** form of this command.

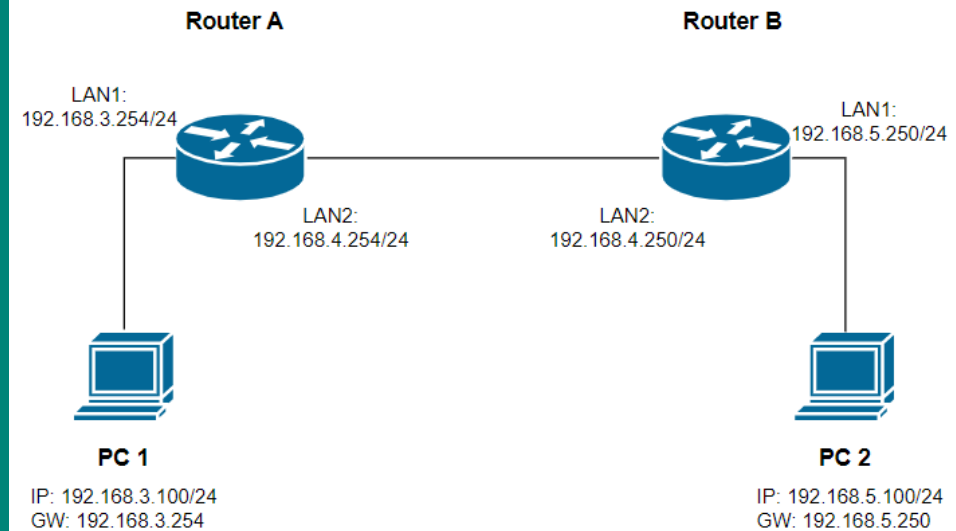
#### Synopsis

```
(config)# ip route static <entry-name> {<ip> <netmask> <nexthop-ip> <metric> |  
                                     enable |  
                                     disable}
```

```
(config)# no ip route static <entry-name>
```

<b>Option Description</b>	entry-name	The entry name in this static route table, 1 to 10 characters.
	ip	Destination IP address
	netmask	Subnet mask for this IP address
	nexthop-ip	The next router along the path to the destination
	metric	A "cost" for accessing the neighboring network, integer ranges from 1 to 255.
	enable	Enables this static route entry
	disable	Disables this static route entry
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• Maximum number of static multicast route entries is 512</li><li>• Network interfaces related to this routing feature must be created in advance.</li></ul>	
<b>Examples</b>	Static route function:  Prerequisites: <ul style="list-style-type: none"><li>• TN router A:<ul style="list-style-type: none"><li>- LAN1: 192.168.3.254/24, VLAN ID=3</li><li>- LAN2: 192.168.4.254/24, VLAN ID=4</li></ul></li><li>• TN router B:<ul style="list-style-type: none"><li>- LAN1: 192.168.5.250/24, VLAN ID=5</li><li>- LAN2: 192.168.4.250/24, VLAN ID=4</li></ul></li><li>• PC (1):<ul style="list-style-type: none"><li>- IP: 192.168.3.100/24</li><li>- Gateway: 192.168.3.254</li></ul></li><li>• PC (2):<ul style="list-style-type: none"><li>- IP: 192.168.5.100/24</li><li>- Gateway: 192.168.5.250</li></ul></li></ul>	

Network topology:



Scenario:

- When the network topology is fixed, no router is expected to be removed or added, configuring static route on each router is considered.
- PC1 can communicate with PC2 via its gateway: 192.168.3.254.
- PC2 can communicate with PC1 via its gateway: 192.168.5.250.

Commands:

[On Router A]

```
router# configure
router(config)# ip route static routerB 192.168.5.0 255.255.255.0
192.168.4.250 10
router(config)# exit
```

[On Router B]

```
router# configure
router(config)# ip route static routerA 192.168.3.0 255.255.255.0
192.168.4.254 10
router(config)# exit
```

<b>Error Messages</b>	% is existed in Static Route list
	% is over length. It must be 1 - 10.
	Invalid Metric. It must be 1 - 255
	^Parse error
<b>Related Commands</b>	^Incomplete command
	show ip route static

## router rip

To enable RIP function on the router, use the **router rip** global configuration command and related sub-level configuration command sets. To disable RIP function, use the **no** form of this command.

### Synopsis

#### **Enable / Disable RIP**

```
(config)# router rip
(config)# no router rip
```

#### **Set interface name to enable RIP**

```
(config-rip)# network <if-name>
```

#### **Set version of RIP**

```
(config-rip)# version {1 | 2}
```

#### **Enable / Disable Redistribute entries**

```
(config-rip)# redistribute {connected |
static |
ospf}
```

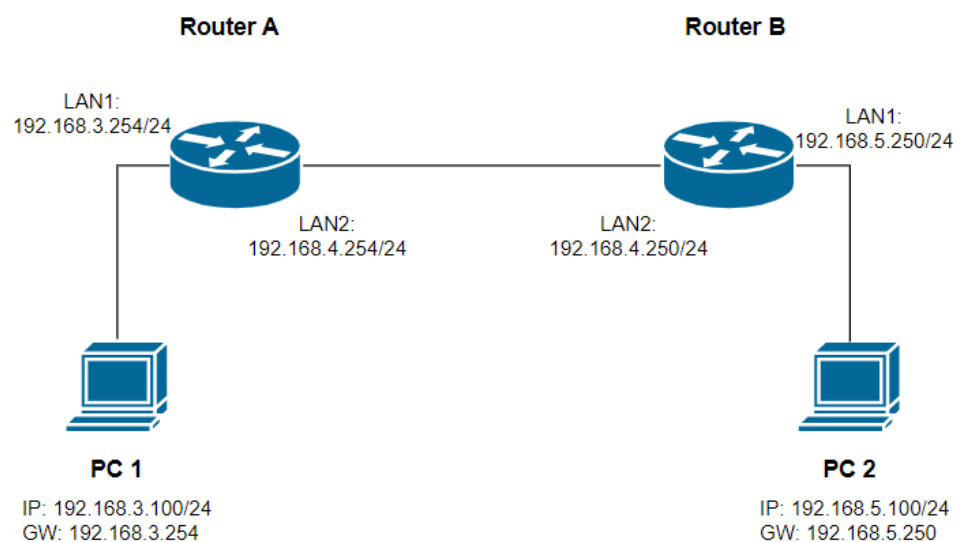
```
(config-rip)# no redistribute {connected |
static |
ospf}
```

#### **Save and Exit RIP configuration.**

```
(config-rip)# exit
```

<b>Option Description</b>	network	Specifies the interface to enable RIP function.
	if-name	Interface name, if-name is case-sensitive.
	redistribute	Redistribute entries learned from specified interfaces
	connected	Entries learned from directly connected interfaces will be re-distributed.
	static	Entries set in a static route will be re-distributed
	ospf	Entries learned from the OSPF will be re-distributed
	version	Specifies which version of RIP will be followed
	1	RIPv1
	2	RIPv2
exit	Commit new settings and exit sub-level configuration mode.	
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	Network interfaces related to this routing feature must be created in advance.	
<b>Examples</b>	RIP function:  Prerequisites: <ul style="list-style-type: none"><li>• TN router A:<ul style="list-style-type: none"><li>- LAN1: 192.168.3.254/24, VLAN ID=3</li><li>- LAN2: 192.168.4.254/24, VLAN ID=4</li></ul></li><li>• TN router B:<ul style="list-style-type: none"><li>- LAN1: 192.168.5.250/24, VLAN ID=5</li><li>- LAN2: 192.168.4.250/24, VLAN ID=4</li></ul></li><li>• PC (1):<ul style="list-style-type: none"><li>- IP: 192.168.3.100/24</li><li>- Gateway: 192.168.3.254</li></ul></li><li>• PC (2):<ul style="list-style-type: none"><li>- IP: 192.168.5.100/24</li><li>- Gateway: 192.168.5.250</li></ul></li></ul>	

Network topology:



Scenario:

- When the maximum hop count is less than 15 in a network topology and some routers are allowed to be removed or added on some occasions, static route (RIP) could be the option for dynamic routing.
- This example takes advantage of RIP to generate a routing table on each router automatically.
- PC1 can communicate with PC2 via its gateway: 192.168.3.254.
- PC2 can communicate with PC1 via its gateway: 192.168.5.250.

Commands:

[On Router A]

```
router# configure
router(config)# router rip
router(config-rip)# version 2
router(config-rip)# network LAN1
router(config-rip)# network LAN2
router(config-rip)# exit
```

[On Router B]

```
router# configure
router(config)# router rip
router(config-rip)# version 2
router(config-rip)# network LAN1
router(config-rip)# network LAN2
router(config-rip)# exit
```

**Error Messages**

```
% Invalid format
% Invalid Network Interface Name.
% Invalid Version. It must be 1 or 2.
^Parse error
```

**Related Commands**

```
show ip rip
show ip route
```

## router ospf

To configure dynamic routing with OSPF virtual-link or area aggregation settings, use the **router ospf** global configuration command and related sub-level configuration command sets. To remove the settings, use the **no** form of this command.

### Synopsis

#### Enable / Disable OSPF

```
(config)# router ospf  
(config)# no router ospf
```

#### Change Router ID and enter sub-level configuration mode

```
(config)# router ospf <router-id>
```

#### Enable /Disable redistribution of OSPF

```
(config-ospf)# redistribute {connected |  
                                  static |  
                                  rip}  
  
(config-ospf)# no redistribute {connected |  
                                  static |  
                                  rip}
```

#### Add / Remove Area ID with Normal Area Type

```
(config-ospf)# area <area-id>  
(config-ospf)# no area <area-id>
```

#### Set Area ID with Stub/NSSA Area Type

```
(config-ospf)# area <area-id> [{stub metric <number> |  
                                  nssa metric <number>}]
```

#### Add / Remove Virtual-link or Area aggregation

```
(config-ospf)# area <area-id> [{virtual-link <router-id> |  
                                  range <dst-network> <netmask>}]  
  
(config-ospf)# no area <area-id> [{virtual-link <router-id> |  
                                  range <dst-network> <netmask>}]
```

#### Save and Exit OSPF configuration

```
(config-ospf)# exit
```

Option		Description
router-id		Router's IP address
exit		Commit new settings and exit sub-level configuration mode.
redistribute		Specifies what entries will be re-distributed
connected		Entries learned from the directly connected interfaces will be re-distributed.
static		Entries set in a static route will be re-distributed.
rip		Entries learned from the RIP will be re-distributed.
area		Specifies the area ID
area-id		An area ID
range		Specifies OSPF area aggregation
dst-network		Destination network
netmask		Netmask of the destination network.
stub metric		Specifies metric of stub area.
number		Metric/Cost of OSPF. Ranges from 1 to 65535
nssa metric		Specifies metric of nssa area.
virtual-link		Specifies neighbor router ID

	n-router-id	A neighbor router ID
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	Network interfaces related to this routing feature must be created in advance.	
<b>Examples</b>	<p>OSPF function:</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>• TN router A: <ul style="list-style-type: none"> <li>- LAN1: 192.168.3.251/24, VLAN ID=3</li> <li>- LAN2: 192.168.4.251/24, VLAN ID=4</li> </ul> </li> <li>• TN router B: <ul style="list-style-type: none"> <li>- LAN2: 192.168.4.252/24, VLAN ID=4</li> <li>- LAN3: 192.168.5.252/24, VLAN ID=5</li> </ul> </li> <li>• TN router C: <ul style="list-style-type: none"> <li>- LAN3: 192.168.5.250/24, VLAN ID=5</li> <li>- LAN4: 192.168.6.250/24, VLAN ID=6</li> </ul> </li> <li>• PC (1): <ul style="list-style-type: none"> <li>- IP: 192.168.3.100/24</li> <li>- Gateway: 192.168.3.251</li> </ul> </li> <li>• PC (2): <ul style="list-style-type: none"> <li>- IP: 192.168.6.100/24</li> <li>- Gateway: 192.168.6.250</li> </ul> </li> </ul> <p>Network topology:</p> <p>Scenario:</p> <ol style="list-style-type: none"> <li>When the maximum hop count is greater than 15 in a network topology and some routers are allowed to be removed or added on some occasions, OSPF could be the option for dynamic routing.</li> <li>This example takes advantage of OSPF to generate a routing table on each router automatically.</li> <li>PC1 can communicate with PC2 via its gateway: 192.168.3.251.</li> <li>PC2 can communicate with PC1 via its gateway: 192.168.6.250.</li> </ol> <p>Commands:</p> <pre>[On Router A] router# configure router(config)# router ospf 192.168.4.251 router(config-ospf)# redistribute connected router(config-ospf)# area 192.168.0.0 router(config-ospf)# exit router(config)# interface vlan 4 router(config-vif)# ip ospf area 192.168.0.0 router(config-vif)# exit</pre>	



	<pre>[On Router B] router# configure router(config)# router ospf 192.168.5.252 router(config-ospf)# area 192.168.0.0 router(config-ospf)# exit router(config)# interface vlan 4 router(config-vif)# ip ospf area 192.168.0.0 router(config-vif)# exit router(config)# interface vlan 5 router(config-vif)# ip ospf area 192.168.0.0 router(config-vif)# exit  [On Router C] router# configure router(config)# router ospf 192.168.6.250 router(config-ospf)# redistribute connected router(config-ospf)# area 192.168.0.0 router(config-ospf)# exit router(config)# interface vlan 5 router(config-vif)# ip ospf area 192.168.0.0 router(config-vif)# exit</pre>
<b>Error Messages</b>	<pre>% Metric must be 1 - 65535 % is not existed in OSPF Area list. % Entry is not found % is not existed in OSPF Virtual Link list. ^Parse error ^Incomplete command</pre>
<b>Related Commands</b>	<pre>show ip ospf show ip route ip ospf</pre>

## show ip route

To check the routing table information on the router, use the **show ip route** command.

### Synopsis

```
# show ip route [{static |  
                kernel}]
```

<b>Option</b>	static	Specifies to display the static routing entries
<b>Description</b>	kernel	Specifies to display the kernel routing table
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router # show ip route Idx  Type      Destination      Next Hop          Interface  Metric ----  - 1     ospf       192.168.3.0/24   192.168.4.251    LAN2       20 2     connected  192.168.4.0/24   192.168.4.252    LAN2       1 3     connected  192.168.5.0/24   192.168.5.252    LAN3       1 4     ospf       192.168.6.0/24   192.168.5.250    LAN3       20 5     connected  192.168.127.0/24 192.168.127.252  LAN        1  router# show ip route static State  Name    Dst Address  Netmask      Next Hop      Metric -----  - Enable  sr1     0.0.0.0      0.0.0.0      19.1.1.1      9 Enable  sr2     22.22.0.0    255.255.0.0  22.22.0.254  10  router# show ip route kernel 192.168.3.0/24 via 192.168.4.251 dev LAN2 proto zebra metric 20 192.168.4.0/24 dev LAN2 proto kernel scope link src 192.168.4.252 192.168.5.0/24 dev LAN3 proto kernel scope link src 192.168.5.252 192.168.6.0/24 via 192.168.5.250 dev LAN3 proto zebra metric 20 192.168.127.0/24 dev LAN proto kernel scope link src 192.168.127.252</pre>	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	ip route	

## show ip rip

To check the RIP settings on the router, use the **show ip rip** command.

### **Synopsis**

# **show ip rip**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show ip rip RIP Protocol          : Disable RIP Version           : v2 Distribution   Connetced          : Disable   Stasis             : Disable   OSPF               : Disable  RIP Enable Table Interface Name  IP                VID      Enable ----- WAN             0.0.0.0           10       Disable LAN20           192.168.127.254  1        Disable LAN6            192.168.6.254    6        Disable</pre>
<b>Error Messages</b>	^Parse error
<b>Related Commands</b>	router rip

## show ip ospf

To check the OSPF settings on the router, use the **show ip ospf** command.

### Synopsis

```
# show ip ospf [{database |
                 instance |
                 neighbor}]
```

<b>Option Description</b>	database	Specifies to display OSPF database
	instance	Specifies to display OSPF routing interface
	neighbor	Specifies to display OSPF neighbor information
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router # show ip ospf  OSPF Global Configuration ----- OSPF                Enabled Router ID           192.168.1.1 Current Router ID  192.168.1.1 Redistribute  OSPF Area Configuration Idx  Area ID          Area Type      Metric ----- 1    192.168.1.1      Normal        - 2    192.168.1.2      Stub          999 3    192.168.3.254   Normal        -  OSPF Virtual Link Configuration Idx  Transit Area ID    Neighbor Router ID ----- 1    192.168.1.1        192.168.1.11  OSPF Aggregation Configuration Idx  Area ID            Network Address  Network Mask ----- 1    192.168.1.1        192.168.3.0    255.255.255.0  router# show ip ospf database  Idx  AreaID            Link State ID  Adv. Router    Route    LS Type ----- 1    192.168.1.2 [Stub]  192.168.1.1  192.168.1.1    Router</pre>	
<b>Error Messages</b>	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	router ospf	

## Multicast Route

### ip multicast-routing static

To enable static multicast route service, use the **ip multicast-routing static** global configuration command. To disable static multicast route service, use the **no** form of this command.

#### Synopsis

(config)# **ip multicast-routing static**

(config)# **no ip multicast-routing**

<b>Option Description</b>	N/A
<b>Defaults</b>	Disabled.
<b>Command Modes</b>	Global configuration
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>In order to let all static multicast route entries take effect, Static Multicast Route mode needs to be enabled.</li><li>Network interfaces related to this routing feature must be created in advance.</li></ul>
<b>Examples</b>	* An illustrative example can be found in the command " <b>ip mroute group</b> ".
<b>Error Messages</b>	^Parse error
<b>Related Commands</b>	ip mroute group show ip mroute

### ip mroute group

To create a static multicast route entry, use the **ip mroute group** global configuration command. To delete the static multicast route entry, use the **no** form of this command.

#### Synopsis

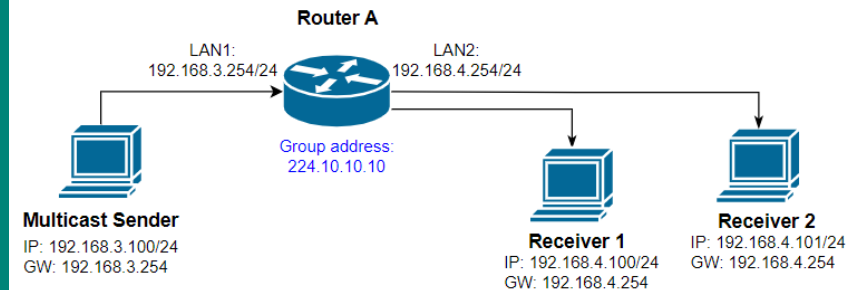
(config)# **ip mroute group** <grp-addr> **src** <src-addr> {**in** <in-if> **out** <out-ifs> | **enable** | **disable**}

(config)# **no ip mroute group** <grp-addr> <src-addr>

<b>Option Description</b>	grp-addr	The IP address of the multicast group address
	src	Specifies the source address
	src-addr	The IP address of the multicast source address or <b>any</b> for any IP address.
	in	Specifies inbound interface
	in-if	The inbound interface name of the multicast stream
	out	Specifies outbound interface
	out-ifs	The outbound interface names of the multicast stream. Comma separated for more than one outbound interface.
	enable	Enables this static multicast route entry
	disable	Disables this static multicast route entry
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>		<ul style="list-style-type: none"><li>In order to let all static multicast route entries take effect, Static Multicast Route mode needs to be enabled.</li><li>Network interfaces related to this routing feature must be created in advance.</li></ul>
<b>Examples</b>	Static multicast route function:  Prerequisites: <ul style="list-style-type: none"><li>TN router A:<ul style="list-style-type: none"><li>- LAN1: 192.168.3.254/24, VLAN ID=3</li><li>- LAN2: 192.168.4.254/24, VLAN ID=4</li></ul></li></ul>	

- TN router B:
  - LAN1: 192.168.5.250/24, VLAN ID=5
  - LAN2: 192.168.4.250/24, VLAN ID=4
- PC (1):
  - IP: 192.168.3.100/24
  - Gateway: 192.168.3.254
- PC (2):
  - IP: 192.168.5.100/24
  - Gateway: 192.168.5.250

Network topology:



Scenario:

- When the maximum hop count is less than 15 in a network topology and some routers are allowed to be removed or added on some occasions, static route (RIP) could be the option for dynamic routing.
- This example takes advantage of RIP to generate a routing table on each router automatically.
- PC1 can communicate with PC2 via its gateway: 192.168.3.254.
- PC2 can communicate with PC1 via its gateway: 192.168.5.250.

Commands:

```
[On Router A]
router# configure
router(config)# router rip
router(config-rip)# version 2
router(config-rip)# network LAN1
router(config-rip)# network LAN2
router(config-rip)# exit
```

<b>Error Messages</b>	% is not existed
	^Parse error
	^Incomplete command
<b>Related Commands</b>	N/A

## show ip mroute

To check the Multicast forwarding table on the router, use the **show ip mroute** command.

### **Synopsis**

```
# show ip mroute {kernel |  
                static}
```

<b>Option</b>	kernel	Specifies to display multicast forwarding table
<b>Description</b>	static	Specifies to display static multicast route configuration settings
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# show ip mroute static State      Group           Source           Inbound  Outbound ----- router# show ip mroute static State      Group           Source           Inbound  Outbound ----- Enable     224.10.10.10    192.168.3.100   LAN1     LAN2,  router# show ip mroute kernel Idx Group           Source           Inbound  Packets  Bytes  Outbound --- 1  224.10.10.10    192.168.3.100 LAN1     0        0      LAN2 2  239.255.255.250 192.168.127.1 LAN      744     209684</pre>	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ip multicast-routing static ip mroute group	

# Broadcast Forward

## ip broadcast-forward

To specify or modify UDP broadcast forwarding settings, use the **ip broadcast-forward** global configuration command sets. To remove the setting, use **no** form of this command.

### Synopsis

#### Enable / Disable UDP broadcast forwarding

```
(config)# ip broadcast-forward
(config)# no ip broadcast-forward
```

#### Create / Delete UDP broadcast forwarding settings

```
(config)# ip broadcast-forward in <in-if> out <out-if> udp <port-list>
(config)# no ip broadcast-forward in <in-if> out <out-if> udp <port-list>
```

<b>Option</b>	in	Specifies inbound interface
<b>Description</b>	in-if	The inbound interface name of the broadcast stream
	out	Specifies outbound interface
	out-if	The outbound interface names of the broadcast stream.
	udp	Specifies UDP destination ports
	port-list	Port List, comma separated for more than one port. e.g. 80,90
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>Inbound and outbound network interfaces must be configured in advance.</li> <li>Multiple UDP ports can be configured in a comma separated port list.</li> </ul>	
<b>Examples</b>	<p>UDP broadcast forwarding function:</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>TN router A: <ul style="list-style-type: none"> <li>LAN1: 192.168.3.254/24, VLAN ID=3</li> <li>LAN2: 192.168.4.254/24, VLAN ID=4</li> </ul> </li> <li>UDP sender: <ul style="list-style-type: none"> <li>IP: 192.168.3.100/24</li> <li>Gateway: 192.168.3.254</li> </ul> </li> <li>UDP receiver: <ul style="list-style-type: none"> <li>IP: 192.168.4.100/24</li> <li>Gateway: 192.168.4.254</li> </ul> </li> </ul> <p>Network topology:</p> <pre> graph LR     subgraph Router_A [Router A]         LAN1[LAN1: 192.168.3.254/24]         LAN2[LAN2: 192.168.4.254/24]     end     subgraph UDP_sender [UDP sender]         S_IP[IP: 192.168.3.100/24]         S_GW[GW: 192.168.3.254]     end     subgraph UDP_receiver [UDP receiver]         R_IP[IP: 192.168.4.100/24]         R_GW[GW: 192.168.4.254]     end     LAN1 --- UDP_sender     LAN2 --- UDP_receiver     </pre> <p>Scenario:</p> <ol style="list-style-type: none"> <li>The UDP sender broadcasts packets to the destination port 6677.</li> <li>The UDP receiver in a different subnet can receive the broadcast packets.</li> </ol>	



	<b>Commands:</b> router# configure router(config)# ip broadcast-forward in LAN1 out LAN2 udp 6677 router(config)# ip broadcast-forward
<b>Error Messages</b>	% Invalid Inbound Interface Name.
	% Invalid Outbound Interface Name.
	% This rule is not existed in Broadcast Forwarding Rule list.
	^Parse error
	^Incomplete command
<b>Related Commands</b>	show ip broadcast-forward

## show ip broadcast-forward

To check the broadcast forward settings on the router, use the **show ip broadcast-forward** command.

### Synopsis

# **show ip broadcast-forward**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show ip broadcast-forward Global Setting      : Enable  In. Interface      Out. Interface  UDP Port ----- LAN1                LAN2                6677,</pre>
<b>Error Messages</b>	^Parse error
	^Incomplete command
<b>Related Commands</b>	ip broadcast-forward

# VRRP

## router vrrp

To enable VRRP function on the router, use the **router vrrp** global configuration command. To disable VRRP function, use the **no** form of this command.

### Synopsis

(config)# **router vrrp**

(config)# **no router vrrp**

<b>Option Description</b>	N/A
<b>Defaults</b>	Disabled
<b>Command Modes</b>	Global configuration
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	* An illustrative example can be found in the command " <b>vrrp</b> ".
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	vrrp vrrp version show vrrp

## vrrp version

To specify VRRP version on the router, use the **vrrp version** global configuration command. To return to default setting, use the **no** form of this command.

### Synopsis

(config)# **vrrp version {2 | 3}**

(config)# **no vrrp version**

<b>Option Description</b>	2	Version 2
	3	Version 3
<b>Defaults</b>	Version 3	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	* An illustrative example can be found in the command " <b>vrrp</b> ".	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	vrrp router vrrp show vrrp	

## vrrp

To specify or modify the VRRP functions, use the **vrrp** global configuration command. To return to the default, use the **no** form of this command.

### Synopsis

#### Create / Remove VRRP entry

```
(config)# vrrp <vrrp-index>  
(config)# no vrrp <vrrp-index>
```

#### Set VRRP interface entry configuration

```
(config-vrrp)# {vrrp |  
  accept |  
  vrid <vid> |  
  virtual-ip <v-ip> |  
  priority <prio> |  
  preempt [delay <preemp-delay>] |  
  interface <ifs> |  
  adver-interval {v2 | v3} <adv-interval>}
```

#### Set VRRP tracking configuration

```
(config-vrrp)# {track-interface <track-ifs> |  
  tracking ping <ping-ip> interval <ping-interval> timeout <timeout-sec>  
  success <success-count> failure <failure-count>}
```

#### Reset / Disable VRRP configuration

```
(config-vrrp)# no {vrrp |  
  priority |  
  preempt |  
  accept |  
  adver-interval |  
  track-interface |  
  tracking ping}
```

#### Save and Exit VRRP configuration

```
(config-vrrp)# exit
```

Option		
<b>Description</b>	vrrp-index	VRRP interface entry index
	exit	Commit new settings and exit sub-level configuration mode.
	vrrp	Enables VRRP entry
	accept	Enables VRRP accept mode function
	vrid	Specifies VRRP virtual router ID
	vid	VRRP virtual router ID
	virtual-ip	Specifies VRRP router's virtual IP
	v-ip	Virtual IP address
	priority	Specifies router's priority in a VRRP group
	prio	Ranges from 1 to 254.
	preempt	Enables preemption feature.
	delay	Specifies a preempt delay time
	preempt-delay	Ranges from 10 to 300 seconds
	interface	Specifies where you want to enable VRRP, LAN or WAN interface.
	ifs	Interface name
	adver-interval	Specifies advertisement interval
	v2	Specifies advertisement interval for VRRP version 2
	v3	Specifies advertisement interval for VRRP version 3
	adv-interval	V2: ranges from 1 to 30 seconds V3: ranges from 10 to 30000 milliseconds

	track-interface	Specifies VRRP tracking feature
	track-ifs	Interface name for VRRP tracking
	tracking ping	Specifies object ping tracking feature
	ping-ip	IP address
	interval	Specifies a time interval to ping destination to verify connection
	ping-interval	Ranges from 1 to 100 seconds
	timeout	Specifies a timeout value for the ping response
	timeout-sec	Ranges from 1 to 100 seconds
	success	Specifies how many times the ping responds in order to know the connection is working
	success-count	Ranges from 1 to 100
	failure	Specifies how many times the ping responds in order to know the connection is not working
	failure-count	Ranges from 1 to 100
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>In order to maintain the network availability between two different networks, enabling ping tracking is highly recommended. An illustrative example can be found below.</li> <li>Maximum number of VRRP interfaces is 16.</li> <li>Network interfaces related to this routing feature must be created in advance.</li> </ul>	
<b>Examples</b>	<p>VRRP with ping tracking:</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>TN router A: <ul style="list-style-type: none"> <li>LAN10: 10.10.10.100/24, VLAN ID=10</li> <li>LAN20: 192.168.126.100/24, VLAN ID=20</li> </ul> </li> <li>TN router B: <ul style="list-style-type: none"> <li>LAN10: 10.10.10.200/24, VLAN ID=10</li> <li>LAN20: 192.168.126.200/24, VLAN ID=20</li> </ul> </li> <li>PC 1: <ul style="list-style-type: none"> <li>IP: 10.10.10.150/24</li> <li>Gateway: 10.10.10.254</li> </ul> </li> <li>PC 2: <ul style="list-style-type: none"> <li>IP: 192.168.126.150/24</li> <li>Gateway: 192.168.126.254</li> </ul> </li> </ul> <p>Network topology:</p> <p>Scenario:</p> <ol style="list-style-type: none"> <li>Router A enables VRRP v3 and acts as the VRRP master with a higher priority (200).</li> <li>Router B enables VRRP v3 and acts as the VRRP backup with a lower priority (100).</li> <li>Virtual IP for VLAN10 is 10.10.10.254; virtual IP for VLAN 20 is 192.168.126.254</li> </ol>	

- d) In order to perceive the connection status between PC 1 and Router A from LAN20, ping tracking IP 10.10.10.150 shall be configured for LAN20.
- e) In order to perceive the connection status between PC 2 and Router A from LAN10, ping tracking IP 192.168.126.150 shall be configured for LAN10.
- f) Normally, PC 1 can send / receive packets to / from PC 2 via Router A.
- g) As long as Router A cannot reach tracking IPs either 10.10.10.150 or 192.168.126.150 in this example, Router B becomes primary and PC 1 and PC 2 can communicate with each other via Router B.

Commands:

[On Router A]

```
router# configure
router(config)# router vrrp
router(config)# vrrp version 3
router(config)# vrrp 1
router(config-vrrp)# vrid 1
router(config-vrrp)# virtual-ip 10.10.10.254
router(config-vrrp)# priority 200
router(config-vrrp)# preempt delay 10
router(config-vrrp)# preempt
router(config-vrrp)# accept
router(config-vrrp)# interface LAN10
router(config-vrrp)# tracking ping 192.168.126.150 interval 1 timeout
3 success 3 failure 3
router(config-vrrp)# vrrp
router(config-vrrp)# exit
router(config)#
router(config)# vrrp 2
router(config-vrrp)# vrid 1
router(config-vrrp)# virtual-ip 192.168.126.254
router(config-vrrp)# priority 200
router(config-vrrp)# preempt delay 10
router(config-vrrp)# preempt
router(config-vrrp)# accept
router(config-vrrp)# interface LAN20
router(config-vrrp)# tracking ping 10.10.10.150 interval 1 timeout 3
success 3 failure 3
router(config-vrrp)# vrrp
router(config-vrrp)# exit
```

[On Router B]

```
router# configure
router(config)# router vrrp
router(config)# vrrp version 3
router(config)# vrrp 1
router(config-vrrp)# vrid 1
router(config-vrrp)# virtual-ip 10.10.10.254
router(config-vrrp)# priority 100
router(config-vrrp)# preempt delay 10
router(config-vrrp)# preempt
router(config-vrrp)# accept
router(config-vrrp)# interface LAN10
router(config-vrrp)# vrrp
router(config-vrrp)# exit
router(config)#
router(config)# vrrp 2
router(config-vrrp)# vrid 1
```

	<pre>router(config-vrrp)# virtual-ip 192.168.126.254 router(config-vrrp)# priority 100 router(config-vrrp)# preempt delay 10 router(config-vrrp)# preempt router(config-vrrp)# accept router(config-vrrp)# interface LAN20 router(config-vrrp)# vrrp router(config-vrrp)# exit</pre>
<b>Error Messages</b>	<pre>% Virtual Router ID must be 1 - 255. % Priority must be 1 - 254. % Preemption must be 10 - 300. % Adv_interval must be 1 - 30 (s). % Adv_interval must be 10 - 30000 (ms) and divisible by 10. % Invalid Track Interface Name. % Interval must be 1 - 100 sec. % Timeout must be 1 - 100 sec. % success_count must be 1 - 100. % failure_count must be 1 - 100. % Invalid Input Interface Name ^Parse error ^Incomplete command</pre>
<b>Related Commands</b>	<pre>router vrrp vrrp version show vrrp</pre>

## show vrrp

To check the VRRP settings on the router, use the **show vrrp** command.

### Synopsis

# **show vrrp** [detail]

<b>Option Description</b>	detail	Specifies to display VRRP detailed settings
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# show vrrp                                 A indicates enable accept mode                                   P indicates enable preempt mode                                     Interface   VRID  Prio  A  P  State   Master addr      VRIP LAN10      1    200  A  P  MASTER  10.10.10.100 10.10.10.254 LAN20      1    200  A  P  MASTER  192.168.126.100 192.168.126.254 router# show vrrp detail VRRP State: Enable VRRP Version: 3 Interface LAN10     State: Enable   IP Address: 10.10.10.100   VRRP Status: MASTER     Virtual IP: 10.10.10.254   Virtual Router ID: 1   Priority: 200     Advertisement Interval (millisec): 100     Accept Mode: Enable     Preemption Mode: Enable</pre>	

	<pre> Preempt Delay (sec): 10 Native Interface Tracking: -- Object Ping Tracking:     Target IP: 192.168.126.150     Interval (sec): 1     Timeout (sec): 3     Success Count: 3     Failure Count: 3  Interface LAN20     State: Enable   IP Address: 192.168.126.100   VRRP Status: MASTER     Virtual IP: 192.168.126.254   Virtual Router ID: 1   Priority: 200     Advertisement Interval (millisec): 100     Accept Mode: Enable     Preemption Mode: Enable     Preempt Delay (sec): 10     Native Interface Tracking: --     Object Ping Tracking:         Target IP: 10.10.10.150         Interval (sec): 1         Timeout (sec): 3         Success Count: 3         Failure Count: 3 </pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	router vrrp vrrp vrrp version

## no vrrp event

To disable VRRP events, use the **no vrrp event** command.

### **Synopsis**

(config)# **no vrrp event**

(config)# **vrrp event {di | link <port>}**

<b>Option</b>	di	Delete DI on/off
<b>Description</b>	link	Detect Port Link on/off
	port	Device port
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable VRRP Event DI router# configure router(config)# vrrp event di router(config)#exit Enable VRRP Event Link router# configure router(config)# vrrp event link 1 router(config)#exit	
<b>Error Messages</b>	Port id must be %d - %d. ^Parse error ^Incomplete command	
<b>Related Commands</b>	show vrrp detail	

## vrrp event priority

To configure the VRRP event priority, use **vrrp event priority** command.

### **Synopsis**

(config)# **vrrp event priority {on<priority> |**

(config)# **vrrp event priority {off<priority> |**

<b>Option</b>	on	Event on
<b>Description</b>	off	Event off
	priority	Event state priority
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set VRRP Event Priority router# configure router(config)# vrrp event priority on 128 router(config)#exit	
<b>Error Messages</b>	Port id must be %d - %d. ^Parse error ^Incomplete command	
<b>Related Commands</b>	show vrrp detail	



## WAN Redundancy

### wan\_redundancy mode

To enable configure WAN redundancy mode, use the **wan\_redundancy mode** command.

#### **Synopsis**

(config)# **wan\_redundancy mode {wan\_backup}**

<b>Option Description</b>	wan_backup	WAN backup mode
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Only wan_backup mode is supported.	
<b>Examples</b>	router# configure router(config)# wan_redundancy mode wan_backup router(config)# exit	
<b>Error Messages</b>	% WAN Redundancy and VRRP cannot be enabled simultaneously.	
<b>Related Commands</b>	show wan_redundancy no wan_redundancy	

### no wan\_redundancy

To disable WAN redundancy, use the **no wan\_redundancy** command.

#### **Synopsis**

(config)# **no wan\_redundancy**

<b>Option Description</b>	N/A	
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# configure router(config)# no wan_redundancy router(config)# exit	
<b>Error Messages</b>	N/A	
<b>Related Commands</b>	show wan_redundancy wan_redundancy mode	

## show wan\_redundancy

To display the status of WAN redundancy and WAN Backup, use the **show WAN\_redundancy** command.

### Synopsis

# **show wan\_redundancy**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show wan_redundancy ----- WAN-Redundancy mode : Disable WAN-Redundancy switchmode : failback WAN-Redundancy priority :   Priority1 : WAN1 (Enabled)   Priority2 : WAN2 (Disabled) Remote host IP address :   Priority1 : 0.0.0.0   Priority2 : 0.0.0.0 Ping check :   Ping check enabled: NO   Ping interval : 5   Ping failure retry times : 3   Ping success retry times : 3   Ping return time out : 5 -----</pre>
<b>Error Messages</b>	N/A
<b>Related Commands</b>	wan_redundancy mode no wan_redundancy

## wan\_backup switchmode

To configure switch mode of WAN Backup, use the **wan\_backup switchmode** command.

### Synopsis

(config-wan-backup)# **switchmode** { failback| failover}

<b>Option</b>	failback	Failback mode
<b>Description</b>	failover	Failover mode
<b>Defaults</b>	failback	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# switchmode failover router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	N/A	
<b>Related Commands</b>	show wan_redundancy	

## wan\_backup ping\_check

To enable ping check of WAN Backup, use **ping\_check** command.

### Synopsis

(config-wan-backup)# **ping\_check**

<b>Option</b>	N/A	
<b>Description</b>		
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	Before enabling ping check, the remote IP address of the enabled interface should be configured. In OnCell models, this option is not configurable and enabled by default.	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# interface WAN2 remotehostip 8.8.8.8 router(config-wan-backup)# interface WAN2 enable router(config-wan-backup)# ping_check router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	% This option is not configurable. % Remote host IP address should be configured on the enabled interface first.	
<b>Related Commands</b>	wan_backup no ping_check wan_backup interface remotehostip wan_backup interface enable show wan_redundancy	

## wan\_backup no ping\_check

To disable ping check of WAN Backup, use the **no ping\_check** command.

### Synopsis

(config-wan-backup)# **no ping\_check**

<b>Option Description</b>	N/A
<b>Defaults</b>	Disabled
<b>Command Modes</b>	Sub-level configuration
<b>Usage Guidelines</b>	In cellular models, this option is not configurable.
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# no ping_check router(config-wan-backup)# exit router(config)# exit
<b>Error Messages</b>	% This option is not configurable.
<b>Related Commands</b>	wan_backup ping_check show wan_redundancy

## wan\_backup ping\_interval

To configure ping interval ping of ping check, use the **ping\_interval** command.

### Synopsis

(config-wan-backup)# **ping\_interval <interval\_timeout>**

<b>Option Description</b>	interval_timeout	Ranges from 1 to 3600 seconds.
<b>Defaults</b>	5	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	Use the configured ping interval to execute a ping check.	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# ping_interval 5 router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	% Invalid ping interval_time. (1-3600 sec)	
<b>Related Commands</b>	wan_backup ping_check show wan_redundancy	

## wan\_backup ping\_timeout

To configure ping interval of ping check, use the **ping\_timeout** command.

### **Synopsis**

(config-wan-backup)# **ping\_timeout <timeout>**

<b>Option Description</b>	timeout	Ranges from 1 to 10 seconds.
<b>Defaults</b>	5	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	When the ping check times out without ping response, it is regarded as failed.	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# ping_timeout 5 router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	% Invalid ping time_out. (1-10 sec)	
<b>Related Commands</b>	wan_backup ping_check show wan_redundancy	

## wan\_backup ping\_success\_retry

To configure the number of successes required for ping checks to be considered successful, use **ping\_success\_retry** command.

### **Synopsis**

(config-wan-backup)# **ping\_success\_retry <success>**

<b>Option Description</b>	success	Ranges from 1 to 10.
<b>Defaults</b>	3	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	When interface ping successes reach the specified value, the ping check result of this interface is regarded as success.	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# ping_success_retry 3 router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	% Invalid ping success retry times. (1-10 times)	
<b>Related Commands</b>	wan_backup ping_check show wan_redundancy	

## wan\_backup ping\_fail\_retry

To configure the number of failures required for ping check to be viewed as a failure, use the **ping\_fail\_retry** command.

### **Synopsis**

(config-wan-backup)# **ping\_fail\_retry <failure>**

<b>Option Description</b>	failure	Ranges from 1 to 10.
<b>Defaults</b>	3	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	When interface ping failures reach the specified value, the ping check is regarded as a failure.	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# ping_fail_retry 3 router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	% Invalid ping failure retry times. (1-10 times)	
<b>Related Commands</b>	wan_backup ping_check show wan_redundancy	

## wan\_backup interface priority

To configure priority of specific WAN interface in WAN Backup, use the **interface priority** command.

### **Synopsis**

(config-wan-backup)# **interface <name> priority <priority>**

<b>Option Description</b>	name	The WAN interface name.
	priority	The priority value of the specific interface. Ranges from 1 to the number of total WAN interfaces.
<b>Defaults</b>	In general, the default priority of the first WAN interface is 1, the second is 2, and so on.	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	For some models, the priority value of some interface may be fixed and not configurable.	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# interface WAN2 priority 2 router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN). % Invalid priority range. (1 -> nums of wan interface) % Priority is not configurable	
<b>Related Commands</b>	show wan_redundancy wan_backup no interface remotehostip wan_backup ping_check	

## wan\_backup interface remotehostip

To configure the remote IP address for ping check, use the **interface remotehostip** command.

### Synopsis

(config-wan-backup)# **interface <name> remotehostip <ipaddr>**

<b>Option</b>	name	The WAN interface name.
<b>Description</b>	ipaddr	The remote IP address for ping check of the specific interface. Non-unicast IP address and 0.0.0.0 is no acceptable.
<b>Defaults</b>	0.0.0.0	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# interface WAN2 remotehostip 8.8.8.8 router(config-wan-backup)# interface WAN2 enable router(config-wan-backup)# ping_check router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN). % Invalid IP Address.	
<b>Related Commands</b>	show wan_redundancy wan_backup no interface remotehostip wan_backup ping_check	

## wan\_backup no interface remotehostip

To clear the configured remote IP address for ping check, use the **no interface remotehostip** command

### Synopsis

(config-wan-backup)# **no interface <name> remotehostip**

<b>Option</b>	name	The WAN interface name.
<b>Description</b>		
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	Before clearing the remote IP address, ping checks should be disabled.	
<b>Examples</b>	router# configure router(config)# wan_backup router(config-wan-backup)# interface WAN2 remotehostip 8.8.8.8 router(config-wan-backup)# interface WAN2 enable router(config-wan-backup)# ping_check router(config-wan-backup)# exit router(config)# exit	
<b>Error Messages</b>	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN). % Invalid IP Address. % when Ping Check is enabled, remote host IP could not be cleared.	
<b>Related Commands</b>	show wan_redundancy wan_backup no interface remotehostip wan_backup ping_check	

## wan\_backup interface enable

To enable specific WAN interface in WAN Backup, use the **interface enable** command.

### Synopsis

(config-wan-backup)# **interface <name> enable**

<b>Option Description</b>	name	The WAN interface name.
<b>Defaults</b>	Disabled. But for some models, some interfaces may be non-configurable and enabled by default.	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	If the ping check is enabled and remotehostip of the specified interface is not configured, this command will be rejected. If DMZ is enabled on the specified interface, this command will be rejected.	
<b>Examples</b>	<pre>router# configure router(config)# wan_backup router(config-wan-backup)# interface WAN2 remotehostip 8.8.8.8 router(config-wan-backup)# interface WAN2 enable router(config-wan-backup)# ping_check router(config-wan-backup)# exit router(config)# exit</pre>	
<b>Error Messages</b>	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN).	
	% Invalid IP Address.	
	% For <name> interface, only one of WAN Redundancy and DMZ functionality can be enabled.	
<b>Related Commands</b>	show wan_redundancy wan_backup interface remotehostip wan_backup no interface enable interface wan no dmz	

## wan\_backup no interface enable

To disable the specified WAN interface in WAN Backup, use the **no interface enable** command.

### Synopsis

(config-wan-backup)# **no interface <name> enable**

<b>Option Description</b>	name	The WAN interface name.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# configure router(config)# wan_backup router(config-wan-backup)# interface WAN2 remotehostip 8.8.8.8 router(config-wan-backup)# no interface WAN2 enable router(config-wan-backup)# ping_check router(config-wan-backup)# exit router(config)# exit</pre>	
	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN).	



<b>Error Messages</b>	% This option is not configurable.
<b>Related Commands</b>	show wan_redundancy wan_backup no interface enable

# 3. NAT, VPN, and Firewall Functions

---

This chapter describes the commands for the NAT, VPN, and firewall function.

## Command Modes

Refer to the following table for the command modes.

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your router by using a normal user account and password.	#	Enter <b>exit</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"><li>• Change terminal settings.</li><li>• Perform basic tests.</li><li>• Display system information.</li></ul>
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter <b>exit</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"><li>• Change terminal settings.</li><li>• Perform basic tests.</li><li>• Display system information.</li><li>• Enter configuration mode.</li></ul>
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	(config)#	To exit to privileged EXEC mode, enter <b>exit</b> .	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example <b>l3l7-policy &lt;firewall-index&gt;</b> command and press enter	(config-l3l7-policy)#	To exit to global configuration mode, enter <b>exit</b> .	A sub-level to configure for example firewall related arguments.

# Command Sets

## Network Address Translation

### Create NAT Rules

#### ip nat

To create an NAT rule, use the **ip nat** global configuration command and related sub-level configuration command sets. To use the default setting, use **no** form of this sub-level configuration command.

#### Synopsis

##### Create / Disable NAT index

```
(config)# ip nat [<nat-index>]
(config)# no ip nat <nat-index> enable
```

##### Set / Clear the NAT mode.

```
(config-nat)# mode {1-1 |
                    n-1 |
                    pat |
                    advance}
(config-nat)# no mode
```

##### Set / Clear Auto Create Source NAT (For mode 1-1 only).

```
(config-nat)# source-nat
(config-nat)# no source-nat
```

##### Set original interface configuration

```
(config-nat)# original in-iface <in-iframe> src-ip <s-ip-addr> src-port <s-port> dst-ip <d-ip-addr> dst-port <d-port>
```

##### Set translated interface configuration

```
(config-nat)# translated out-iface <out-iframe> src-ip <s-ip-addr> src-port <s-port> dst-ip <d-ip-addr> dst-port <d-port>
```

##### Set / Clear protocol. (For mode PAT, Advance only)

```
(config-nat)# protocol <pro-list>
(config-nat)# no protocol
```

##### Set /Clear NAT description

```
(config-nat)# desc <description>
(config-nat)# no desc
```

##### Set / Clear VRRP redundancy. (For mode 1-1 only)

```
(config-nat)# redundancy <vrrp-id>
(config-nat)# no redundancy
```

##### Set NAT rule enabled /disabled in sub-level configuration

```
(config-nat)# enable
(config-nat)# no enable
```

**Set / Clear NAT Loopback.** (For mode 1-1, PAT only).

```
(config-nat)# nat-loopback
(config-nat)# no nat-loopback
```

**Set / Clear Double NAT** (For mode 1-1, PAT only).

```
(config-nat)# double-nat
(config-nat)# no double-nat
```

**Show NAT configuration**

```
(config-nat)# show
```

**Abort NAT configuration**

```
(config-nat)# abort
```

**Save and Exit NAT configuration.**

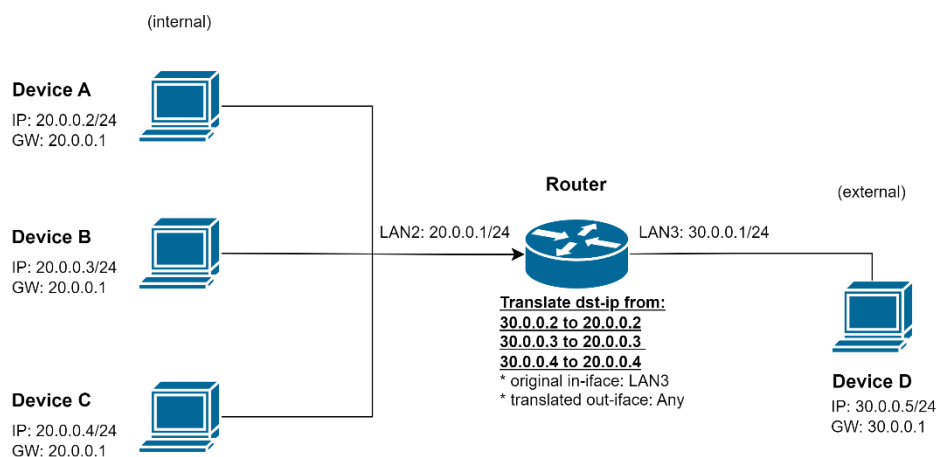
```
(config-nat)# exit
```

Option	Description
nat-index	Index of existing NAT rule. The new NAT rule will be created at this position and original index after this value will be incremented by 1. If <nat-index> is not given, a new NAT rule will be created and appended to the end of the list.
mode	Specifies the NAT mode selection
1-1	1-to-1 NAT
n-1	N-to-1 NAT
pat	Port forward NAT
advance	Advanced NAT
source-nat	Specifies to create Source NAT rule at the same time
original	Specifies the address/port for incoming packet
in-iface	Specifies the interface name for incoming packets
in-ifname	Interface name for incoming packets
src-ip	Specifies source IP address
s-ip-addr	Source IP address or a range of IP addresses. e.g., any, 192.168.127.1, 192.168.127.1-192.168.127.200, 192.168.127.0/27
src-port	Specifies source port
s-port	Source port number. E.g., any, 80, 90-100
dst-ip	Specifies destination IP address
d-ip-addr	Destination IP address or a range of IP addresses. E.g., any, 192.168.127.1, 192.168.127.1-192.168.127.200, 192.168.127.0/27
dst-port	Specifies destination port
d-port	Destination port number. E.g., any, 80, 90-100
translated	Specifies the translated address/port of outgoing packet
out-iface	Specifies the interface name for outgoing packets
enable	Specifies to enable this NAT rule
protocol	Specifies TCP/UDP protocols. Only applicable for PAT and Advance mode.
pro-list	Specifies one of the protocols or their combinations: {tcp   udp   icmp   tcp,udp   tcp,icmp   udp,icmp   tcp,udp,icmp}
redundancy	Specifies VRRP index. Only applicable for 1-1 mode.
vrrp-id	VRRP index.
desc	Specifies the description of this NAT rule
description	Description of this NAT rule. Maximum length is 128. Any whitespace is not allowed.
nat-loopback	Specifies to enable / disable NAT loopback function. This command is used for mode 1-1 and PAT only.
double-nat	Specifies to enable / disable Double-NAT function. This command is used for mode 1-1 and PAT only.

	show	Display overall settings in this entry before exit.
	abort	Exits sub-level configuration mode without saving any changes.
	exit	Commit new settings and exit sub-level configuration mode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>No modification function is provided. In case modification on a specific index is required, remove it first and then add a new rule.</li> <li>Types a valid index to enter sub-level configuration mode.</li> <li>Maximum number of rules is 512.</li> <li>Exits the sub-level configuration mode to let settings take effect.</li> <li>Prior to confirming new NAT settings, utilize the "settingcheck" command to prevent the router from implementing incorrect configurations.</li> </ul>	
<b>Examples</b>	<p><b>1-to-1 NAT with Auto-create Source NAT disabled:</b></p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>TN router: <ul style="list-style-type: none"> <li>LAN2: 20.0.0.1/24, VLAN ID=2, interface used for internal network</li> <li>LAN3: 30.0.0.1/24, VLAN ID=3, interface used for external network</li> </ul> </li> <li>Device(A) on the internal network: <ul style="list-style-type: none"> <li>IP: 30.0.0.5/24</li> <li>Gateway: 30.0.0.1</li> </ul> </li> <li>Device(B) on the external network: <ul style="list-style-type: none"> <li>IP: 20.0.0.2/24</li> <li>Gateway: 20.0.0.1</li> </ul> </li> </ul> <p>Network topology:</p> <pre> graph LR     subgraph Internal         DeviceB[Device B]     end     subgraph External         DeviceA[Device A]     end     Router[Router]     DeviceB --- LAN2[LAN2: 20.0.0.1/24] --- Router     Router --- LAN3[LAN3: 30.0.0.1/24] --- DeviceA </pre> <p>Scenario:</p> <p>On the router, the destination IP address 30.0.0.2 of the packet originating from Device (A) will be transformed to 20.0.0.2 before being transmitted to Device (B).</p> <p>Commands:</p> <pre> router# configure router(config)# ip nat router(config-nat)# mode 1-1 router(config-nat)# original in-iface LAN3 src-ip any src-port any dst-ip 30.0.0.2 dst-port any router(config-nat)# translated out-iface any src-ip any src-port any dst-ip 20.0.0.2 dst-port any router(config-nat)# desc 1to1_woSNAT router(config-nat)# no source-nat router(config-nat)# exit </pre> <p><b>1-to-1 NAT with Auto-create Source NAT enabled:</b></p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>TN router: <ul style="list-style-type: none"> <li>LAN2: 20.0.0.1/24, VLAN ID=2, interface used for internal network</li> <li>LAN3: 30.0.0.1/24, VLAN ID=3, interface used for external network</li> </ul> </li> </ul>	



### Network topology:



### Scenario:

By using the IP range setting of the CLI command, it can achieve the same effect as having three separate individual 1-to-1 NAT rules.

### Commands:

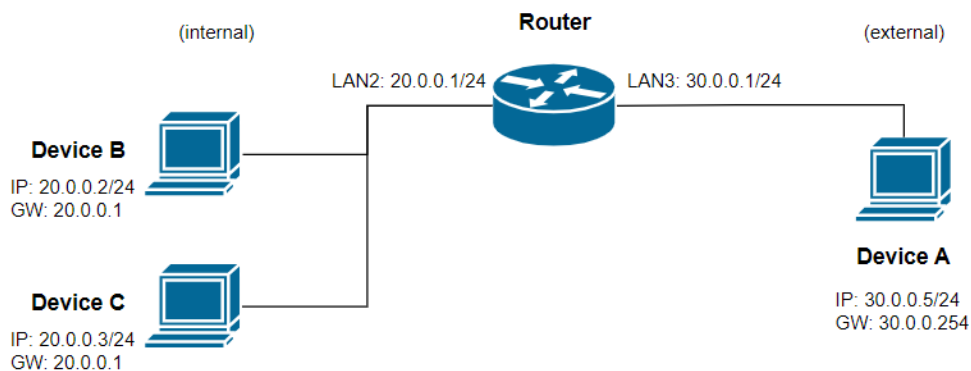
```
router# configure
router(config)# ip nat
router(config-nat)# mode 1-1
router(config-nat)# original in-iface LAN3 src-ip any src-port any
dst-ip 30.0.0.2-30.0.0.4 dst-port any
router(config-nat)# translated out-iface any src-ip any src-port any
dst-ip 20.0.0.2-20.0.0.4 dst-port any
router(config-nat)# desc 1to1_range
router(config-nat)# source-nat
router(config-nat)# exit
```

### N-to-1 NAT:

#### Prerequisites:

- TN router:
  - LAN3: 30.0.0.1/24, VLAN ID=3, interface used for external network
  - LAN2: 20.0.0.1/24, VLAN ID=2, interface used for internal network
- Device(A) on the external network:
  - IP: 30.0.0.5/24
- Device(B) on the internal network:
  - IP: 20.0.0.2/24
  - Gateway: 20.0.0.1
- Device(C) on the internal network:
  - IP: 20.0.0.3/24
  - Gateway: 20.0.0.1

Network topology:



Scenario:

On the router, the source IP address 20.0.0.2 or 20.0.0.3 of the packet originating from Device (B) or Device (C) will be transformed to 30.0.0.1 (masquerading) before being transmitted to Device (A).

Commands:

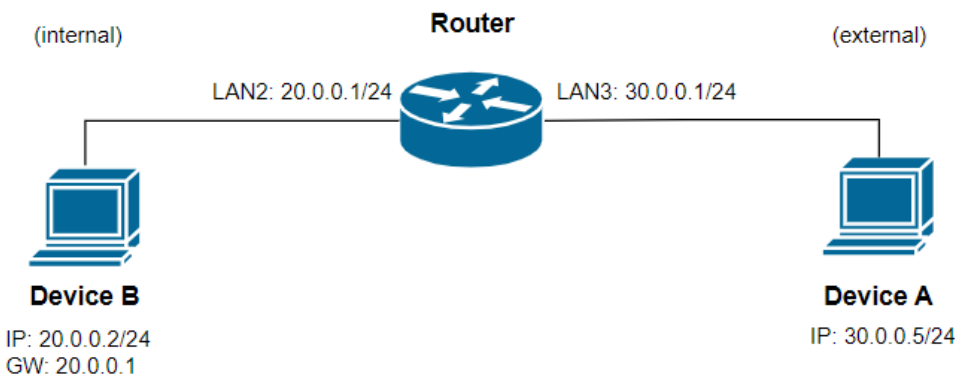
```
router# configure
router(config)# ip nat
router(config-nat)# mode n-1
router(config-nat)# original in-iface any src-ip 20.0.0.2-20.0.0.4
src-port any dst-ip any dst-port any
router(config-nat)# translated out-iface LAN3 src-ip any src-port any
dst-ip any dst-port any
router(config-nat)# desc n-1_example
router(config-nat)# exit
```

Port forward:

Prerequisites:

- TN router:
  - LAN3: 30.0.0.1/24, VLAN ID=3, interface used for external network
  - LAN2: 20.0.0.1/24, VLAN ID=2, interface used for internal network
- Device(A) on the external network:
  - IP: 30.0.0.5/24
  - Gateway: 30.0.0.1
- Device(B) on the internal network:
  - IP: 20.0.0.2/24
  - Gateway: 20.0.0.1
  - SSH port: 22

Network topology:





Scenario:

Device(A) can access ssh service on Device(B) via TN router LAN3 and port 2222.

Commands:

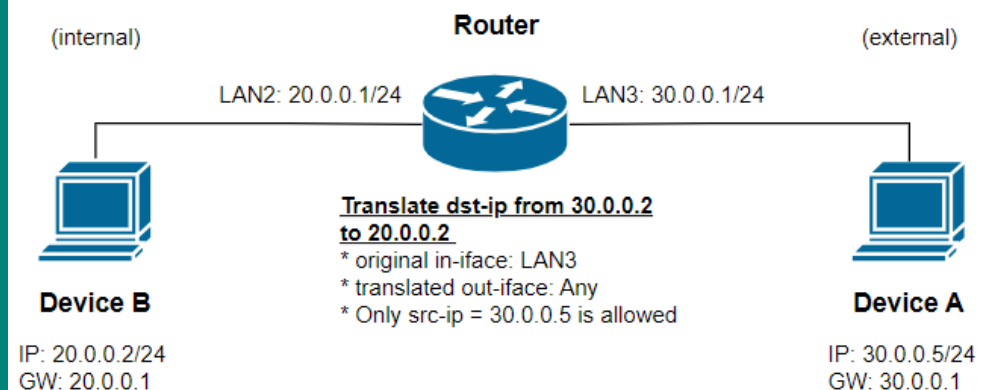
```
router# configure
router(config)# ip nat
router(config-nat)# mode pat
router(config-nat)# original in-iface LAN3 src-ip any src-port any
dst-ip any dst-port 2222
router(config-nat)# translated out-iface any src-ip any src-port any
dst-ip 20.0.0.2 dst-port 22
router(config-nat)# protocol tcp
router(config-nat)# desc pat_example
router(config-nat)# exit
```

**Using Advance Mode to create 1-to-1 NAT and only IP address 30.0.0.5 is allowed to access the SSH server on Device (B) via virtual IP address 30.0.0.2:**

Prerequisites:

- TN router:
  - LAN2: 20.0.0.1/24, VLAN ID=2, interface used for internal network
  - LAN3: 30.0.0.1/24, VLAN ID=3, interface used for external network
- Device(A) on the internal network:
  - IP: 30.0.0.5/24
  - Gateway: 30.0.0.1
- Device(B) on the external network:
  - IP: 20.0.0.2/24
  - Gateway: 20.0.0.1
  - SSH server

Network topology:



Scenario:

- a) On the router, the destination IP address 30.0.0.2 of the packet originating from Device (A) will be transformed to 20.0.0.2 before being transmitted to Device (B) when the source IP is 30.0.0.5.
- b) Only Device (A) can access ssh service on Device (B).
- c) Other devices from external network cannot access ssh service on Device (B).

Commands:

```
router# configure
router(config)# ip nat
router(config-nat)# mode advance
router(config-nat)# original in-iface LAN3 src-ip 30.0.0.5 src-port
any dst-ip 30.0.0.2 dst-port any
```

	<pre>router(config-nat)# translated out-iface any src-ip any src-port any dst-ip 20.0.0.2 dst-port any router(config-nat)# desc advance_example router(config-nat)# protocol tcp router(config-nat)# exit</pre> <p>Apart from the aforementioned command, it is also necessary to manually create a secondary IP address (30.0.0.2) on LAN3:</p> <pre>router(config)# interface vlan 3 router(config-vif)# ip address 30.0.0.2 255.255.255.0 secondary router(config-vif)# exit</pre>
<b>Error Messages</b>	<p>- Ranged Translated Destination IP (), Original Destination IP () mismatch is forbidden</p> <p>% Invalid in-iface Interface Name.</p> <p>% Invalid format</p> <p>% Invalid Protocol. It must be tcp, udp or select multiple protocol with ",".</p> <p>% is over length. It must be 1 - 128.</p> <p>% is not a valid mode.</p> <p>^Parse error</p> <p>^Incomplete command</p>
<b>Related Commands</b>	<pre>no ip nat show ip nat settingcheck</pre>

## Delete NAT Rules

### no ip nat

To remove the NAT rules, use the **no ip nat** global configuration command.

#### **Synopsis**

(config)# **no ip nat** <nat-index>

<b>Option Description</b>	nat-index	Index of existing NAT rule
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<p>Delete an existing NAT rule:</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>TN router: <ul style="list-style-type: none"> <li>- There exists 4 NAT rules before deletion.</li> </ul> </li> </ul> <p>Scenario:</p> <p>The 3rd NAT rule is outdated and needs to be removed.</p> <p>Commands:</p> <pre>router# configure router(config)# no ip nat 3 router(config)# exit</pre>	
<b>Error Messages</b>	<p>% Invalid Index. It must be 1 - .</p> <p>^Parse error</p> <p>^Incomplete command</p>	
<b>Related Commands</b>	<pre>ip nat show ip nat</pre>	

## show ip nat

To check the NAT settings on the router, use the **show ip nat** command.

### Synopsis

# **show ip nat**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre> router# show ip nat ----- Index          : 1 Enable         : Disable Protocol       : -- Mode           : 1-1bi VRRP Binding   : -- Original     Incoming Interface : LAN     Source IP          : --     Source Port        : --     Destination IP     : 192.168.127.10     Destination Port   : -- Translated     Outgoing Interface : ALL     Source IP          : --     Source Port        : --     Destination IP     : 192.168.6.10     Destination Port   : -- ----- Original     Incoming Interface : ALL     Source IP          : 192.168.6.10     Source Port        : --     Destination IP     : --     Destination Port   : -- Translated     Outgoing Interface : LAN     Source IP          : 192.168.127.10     Source Port        : --     Destination IP     : --     Destination Port   : -- ----- </pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	ip nat no ip nat

# Object Management

## object address

To create an IP address object, use the **object address** global configuration command and corresponding sub-level configuration mode commands. To remove the object, use **no** form of this command.

### Synopsis

#### Create a new object of IP address and subnet type and enter the sub-level mode

```
(config)# object address  
(config-obj-addr)#
```

#### Set / Clear object name

```
(config-obj-addr)# name <name-string>  
(config-obj-addr)# no name
```

#### Remove object of IP address and subnet type

```
(config)# no object <name-string>
```

#### Set / Clear object IP address configuration (could be a single IP, or a range of IPs)

```
(config-obj-addr)# ip-addr <ip-string>  
(config-obj-addr)# no ip-addr
```

#### Quit object IP address configuration without saving

```
(config-obj-addr)# abort
```

#### Save and Exit object IP address configuration.

```
(config-obj-addr)# exit
```

<b>Option Description</b>	name	Specifies the object's name
	name-string	A set of characters without a whitespace. Maximum length is 32.
	ip-addr	Specifies the IP address. It could be a single IP or a range of IPs.
	ip-string	E.g. 192.168.127.123, 192.168.127.10-192.168.127.20, 192.168.127.0/24
	abort	Exits sub-level configuration mode without saving any changes.
	exit	Commit new settings and exit sub-level configuration mode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• No modification function is provided. In case modification is required, remove it first and then add a new object.</li><li>• Exits the sub-level configuration mode to let settings take effect.</li><li>• "uuid" option in this command is reserved for Moxa use only.</li></ul>	
<b>Examples</b>	Create an object of IP address type for Layer 3-7 policy: router# configure router(config)# object address router(config-obj-addr)# name ED1 router(config-obj-addr)# ip-addr 192.168.127.1 router(config-obj-addr)# exit	
<b>Error Messages</b>	% Object named xxx is already existed.	
	% No object named xxx found.	
	% IP Address cannot be empty.	
	% xxx is over length. It must be 1 - 32.	
	% Invalid ipaddr.	
	^Parse error ^Incomplete command	

## object service

To create a user-defined service object, use the **object service** global configuration command and corresponding sub-level configuration mode commands. To remove the object, use **no** form of this command.

### Synopsis

#### Create a new object of user-defined service type and enter the sub-level mode

```
(config)# object service {tcp | udp | tcpudp | icmp | ipproto}
(config-obj-serv)#
```

#### Set / Clear object name

```
(config-obj-serv)# name <name-string>
(config-obj-serv)# no name
```

#### Remove object of user-defined service type

```
(config)# no object <name-string>
```

#### Set / Clear object IP protocol configuration (in terms of IP protocol number; only effective while ipproto is selected)

```
(config-obj-serv)# ipproto <proto-number>
(config-obj-serv)# no ipproto
```

#### Set / Clear object port configuration (any, single, range)

```
(config-obj-serv)# port <port-string>
(config-obj-serv)# no port
```

#### Set / Clear object ICMP configuration (only effective while icmp is selected)

```
(config-obj-serv)# icmp-type <type-string>
(config-obj-serv)# icmp-code <code-string>
(config-obj-serv)# no icmp
```

#### Quit object user-defined service configuration without saving

```
(config-obj-serv)# abort
```

#### Save and Exit object user-defined service configuration.

```
(config-obj-serv)# exit
```

<b>Option</b>	tcp	Specifies TCP protocol
<b>Description</b>	udp	Specifies UDP protocol
	tcpudp	Specifies TCP & UDP protocols
	icmp	Specifies ICMP protocol
	ipproto	Specifies a custom IP protocol
	name	Specifies the object's name
	name-string	A set of characters without a whitespace. Maximum length is 32.
	proto-number	IP protocol number. Ranges from 0 to 255.
	icmp-type	Specifies the type of ICMP message
	type-string	E.g. any, 8
	icmp-code	Specifies the code of ICMP message
	code-string	E.g. any, 0
	port	Specifies the port number(s)
	port-string	E.g. any, 100, 60001-60999
	abort	Exits sub-level configuration mode without saving any changes.

	exit	Commit new settings and exit sub-level configuration mode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>No modification function is provided. In case modification is required, remove it first and then add a new object.</li> <li>Exits the sub-level configuration mode to let settings take effect.</li> </ul>	
<b>Examples</b>	Create an object of user-defined service type for Layer 3-7 policy: <pre>router# configure router(config)# object service tcpudp router(config-obj-serv)# name User-defined-Service1 router(config-obj-serv)# port 8888 router(config-obj-serv)# exit</pre>	
<b>Error Messages</b>	<pre>% Object named xxx is already existed. % No object named xxx found. % Unknown Service Type xxx % Port Format Error. % xxx is over length. It must be 1 - 32. % Cannot set IP Protocol if Object Service Type is not ipproto. % Cannot set ICMP Type if Object Service Type is not icmp. % Cannot set ICMP Code if Object Service Type is not icmp. ^Parse error ^Incomplete command</pre>	
<b>Related Commands</b>	show object	

## object network-service

To create a network service object, use the **object network-service** global configuration command and corresponding sub-level configuration mode commands. To remove the object, use **no** form of this command.

### Synopsis

#### Create a new object of network service and enter the sub-level mode

```
(config)# object network-service
(config-obj-net-serv)#
```

#### Set / Clear object name

```
(config-obj-net-serv)# name <name-string>
(config-obj-net-serv)# no name
```

#### Remove object of network service type

```
(config)# no object <name-string>
```

#### Select / Clear pre-defined object configuration

```
(config-obj-net-serv)# select {list | <obj-name>}
(config-obj-net-serv)# no select <obj-name>
```

#### Show selected pre-defined object

```
(config-obj-net-serv)# show
```

#### Quit object network service configuration without saving

```
(config-obj-net-serv)# abort
```

#### Save and Exit object network service configuration.

```
(config-obj-net-serv)# exit
```

<b>Option Description</b>	name	Specifies the object's name																																																																																																		
	name-string	A set of characters without a whitespace. Maximum length is 32.																																																																																																		
	select	Specifies to select a pre-defined network service object																																																																																																		
	list	Specifies to list available objects																																																																																																		
	obj-name	List of available network service objects:																																																																																																		
		<table border="1"> <thead> <tr> <th>Name</th> <th>Detail</th> </tr> </thead> <tbody> <tr> <td colspan="2">-----</td> </tr> <tr> <td colspan="2">Remote-Access</td> </tr> <tr> <td>├ WINS</td> <td>TCP 1512; UDP 1512</td> </tr> <tr> <td>├ TELNET</td> <td>TCP 23</td> </tr> <tr> <td>└ SSH</td> <td>TCP 22</td> </tr> <tr> <td colspan="2">Remote-Desktop</td> </tr> <tr> <td>├ PC-Anywhere</td> <td>TCP 5631; UDP 5632</td> </tr> <tr> <td>├ Chrome-Remote-Desktop</td> <td>UDP 5222</td> </tr> <tr> <td>├ AnyDesk</td> <td>TCP 6568, 7070; UDP 50001-50003</td> </tr> <tr> <td>├ Teamviewer</td> <td>TCP 5938</td> </tr> <tr> <td>├ RDP</td> <td>TCP 3389</td> </tr> <tr> <td>├ VNC</td> <td>TCP 5900</td> </tr> <tr> <td>└ X-WINDOW</td> <td>TCP 6000-6063</td> </tr> <tr> <td colspan="2">Email</td> </tr> <tr> <td>├ IMAP</td> <td>TCP 143</td> </tr> <tr> <td>├ IMAPS</td> <td>TCP 993</td> </tr> <tr> <td>├ POP3</td> <td>TCP 110</td> </tr> <tr> <td>├ POP3S</td> <td>TCP 995</td> </tr> <tr> <td>├ SMTP</td> <td>TCP 25</td> </tr> <tr> <td>└ SMTPS</td> <td>TCP 465</td> </tr> <tr> <td colspan="2">File-Transfer</td> </tr> <tr> <td>├ FTP</td> <td>TCP 21</td> </tr> <tr> <td>├ FTPS</td> <td>TCP 990</td> </tr> <tr> <td>├ SFTP</td> <td>TCP 115; UDP 115</td> </tr> <tr> <td>├ TFTP</td> <td>UDP 69</td> </tr> <tr> <td>├ NFS</td> <td>TCP 111, 2049; UDP 111, 2049</td> </tr> <tr> <td>├ SAMBA</td> <td>TCP 139</td> </tr> <tr> <td>├ AFS3</td> <td>TCP 7000-7009; UDP 7000-7009</td> </tr> <tr> <td>└ SMB</td> <td>TCP 445</td> </tr> <tr> <td colspan="2">Web-Access</td> </tr> <tr> <td>├ HTTP</td> <td>TCP 80</td> </tr> <tr> <td>└ HTTPS</td> <td>TCP 443</td> </tr> <tr> <td colspan="2">Network-Service</td> </tr> <tr> <td>├ BGP</td> <td>TCP 179</td> </tr> <tr> <td>├ DHCP</td> <td>UDP 67</td> </tr> <tr> <td>├ DHCP6</td> <td>UDP 546</td> </tr> <tr> <td>├ DNS</td> <td>TCP 53; UDP 53</td> </tr> <tr> <td>├ NTP</td> <td>TCP 123; UDP 123</td> </tr> <tr> <td>├ ICMP-PING</td> <td>ICMP Type Any Code Any</td> </tr> <tr> <td>├ OSPF</td> <td>IP Protocol 89</td> </tr> <tr> <td>├ RIP</td> <td>TCP 520</td> </tr> <tr> <td>├ SNMP</td> <td>TCP 161-162; UDP 161-162</td> </tr> <tr> <td>└ SYSLOG</td> <td>UDP 514</td> </tr> <tr> <td colspan="2">Authentication</td> </tr> <tr> <td>├ LDAP</td> <td>TCP 389; UDP 389</td> </tr> <tr> <td>├ LDAPS</td> <td>TCP 636; UDP 636</td> </tr> <tr> <td>├ RADIUS</td> <td>UDP 1812-1813</td> </tr> <tr> <td>└ TACACS+</td> <td>TCP 49; UDP 49</td> </tr> </tbody> </table>	Name	Detail	-----		Remote-Access		├ WINS	TCP 1512; UDP 1512	├ TELNET	TCP 23	└ SSH	TCP 22	Remote-Desktop		├ PC-Anywhere	TCP 5631; UDP 5632	├ Chrome-Remote-Desktop	UDP 5222	├ AnyDesk	TCP 6568, 7070; UDP 50001-50003	├ Teamviewer	TCP 5938	├ RDP	TCP 3389	├ VNC	TCP 5900	└ X-WINDOW	TCP 6000-6063	Email		├ IMAP	TCP 143	├ IMAPS	TCP 993	├ POP3	TCP 110	├ POP3S	TCP 995	├ SMTP	TCP 25	└ SMTPS	TCP 465	File-Transfer		├ FTP	TCP 21	├ FTPS	TCP 990	├ SFTP	TCP 115; UDP 115	├ TFTP	UDP 69	├ NFS	TCP 111, 2049; UDP 111, 2049	├ SAMBA	TCP 139	├ AFS3	TCP 7000-7009; UDP 7000-7009	└ SMB	TCP 445	Web-Access		├ HTTP	TCP 80	└ HTTPS	TCP 443	Network-Service		├ BGP	TCP 179	├ DHCP	UDP 67	├ DHCP6	UDP 546	├ DNS	TCP 53; UDP 53	├ NTP	TCP 123; UDP 123	├ ICMP-PING	ICMP Type Any Code Any	├ OSPF	IP Protocol 89	├ RIP	TCP 520	├ SNMP	TCP 161-162; UDP 161-162	└ SYSLOG	UDP 514	Authentication		├ LDAP	TCP 389; UDP 389	├ LDAPS	TCP 636; UDP 636	├ RADIUS	UDP 1812-1813	└ TACACS+	TCP 49; UDP 49
	Name	Detail																																																																																																		
	-----																																																																																																			
	Remote-Access																																																																																																			
	├ WINS	TCP 1512; UDP 1512																																																																																																		
	├ TELNET	TCP 23																																																																																																		
	└ SSH	TCP 22																																																																																																		
	Remote-Desktop																																																																																																			
├ PC-Anywhere	TCP 5631; UDP 5632																																																																																																			
├ Chrome-Remote-Desktop	UDP 5222																																																																																																			
├ AnyDesk	TCP 6568, 7070; UDP 50001-50003																																																																																																			
├ Teamviewer	TCP 5938																																																																																																			
├ RDP	TCP 3389																																																																																																			
├ VNC	TCP 5900																																																																																																			
└ X-WINDOW	TCP 6000-6063																																																																																																			
Email																																																																																																				
├ IMAP	TCP 143																																																																																																			
├ IMAPS	TCP 993																																																																																																			
├ POP3	TCP 110																																																																																																			
├ POP3S	TCP 995																																																																																																			
├ SMTP	TCP 25																																																																																																			
└ SMTPS	TCP 465																																																																																																			
File-Transfer																																																																																																				
├ FTP	TCP 21																																																																																																			
├ FTPS	TCP 990																																																																																																			
├ SFTP	TCP 115; UDP 115																																																																																																			
├ TFTP	UDP 69																																																																																																			
├ NFS	TCP 111, 2049; UDP 111, 2049																																																																																																			
├ SAMBA	TCP 139																																																																																																			
├ AFS3	TCP 7000-7009; UDP 7000-7009																																																																																																			
└ SMB	TCP 445																																																																																																			
Web-Access																																																																																																				
├ HTTP	TCP 80																																																																																																			
└ HTTPS	TCP 443																																																																																																			
Network-Service																																																																																																				
├ BGP	TCP 179																																																																																																			
├ DHCP	UDP 67																																																																																																			
├ DHCP6	UDP 546																																																																																																			
├ DNS	TCP 53; UDP 53																																																																																																			
├ NTP	TCP 123; UDP 123																																																																																																			
├ ICMP-PING	ICMP Type Any Code Any																																																																																																			
├ OSPF	IP Protocol 89																																																																																																			
├ RIP	TCP 520																																																																																																			
├ SNMP	TCP 161-162; UDP 161-162																																																																																																			
└ SYSLOG	UDP 514																																																																																																			
Authentication																																																																																																				
├ LDAP	TCP 389; UDP 389																																																																																																			
├ LDAPS	TCP 636; UDP 636																																																																																																			
├ RADIUS	UDP 1812-1813																																																																																																			
└ TACACS+	TCP 49; UDP 49																																																																																																			

		VOIP-and-Streaming └ SIP TCP 5060; UDP 5060 └ RTSP TCP 554, 7070, 8554; UDP 554 SQL-Server └ MS-SQL TCP 1433-1434 └ MYSQL TCP 3306  You can select Remote-Access to represent selecting WINS, TELNET and SSH individually.
	show	Display overall settings in this entry before exit.
	abort	Exits sub-level configuration mode without saving any changes.
	exit	Commit new settings and exit sub-level configuration mode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>No modification function is provided. In case modification is required, remove it first and then add a new object.</li> <li>Exits the sub-level configuration mode to let settings take effect.</li> </ul>	
<b>Examples</b>	Create an object of Network-Service type for Layer 3-7 policy: <pre> router# configure router(config)# object network-service router(config-obj-net-serv)# name NetworkSrv1 router(config-obj-net-serv)# select File-Transfer router(config-obj-net-serv)# exit </pre>	
<b>Error Messages</b>	% Object named xxx is already existed. % No network service object named xxx was found. % xxx is over length. It must be 1 - 32. % Please at least select one object. ^Parse error ^Incomplete command	
<b>Related Commands</b>	show object	

## object industrial-application-service

To create an industrial application service object, use the **object industrial-application-service** global configuration command and corresponding sub-level configuration mode commands. To remove the object, use **no** form of this command.

### Synopsis

#### Create a new object of industrial application service type and enter the sub-level mode

```
(config)# object industrial-application-service
(config-obj-indust-app)#
```

#### Set / Clear object name

```
(config-obj-indust-app)# name <name-string>
(config-obj-indust-app)# no name
```

#### Remove object of industrial application service type

```
(config-obj-indust-app)# no object <name-string>
```

#### Select / Clear pre-defined object configuration

```
(config-obj-indust-app)# select {list | <obj-name>}
(config-obj-indust-app)# no select <obj-name>
```



**Show selected pre-defined object**`(config-obj-indust-app)# show`**Quit object industrial application service configuration without saving**`(config-obj-indust-app)# abort`**Save and Exit object industrial application service configuration.**`(config-obj-indust-app)# exit`

<b>Option Description</b>	name	Specifies the object's name																						
	name-string	A set of characters without a whitespace. Maximum length is 32.																						
	select	Specifies to select an industrial application service object																						
	list	Specifies to list available objects																						
	obj-name	List of available industrial application service objects:																						
		<table border="1"> <thead> <tr> <th>Name</th> <th>Detail</th> </tr> </thead> <tbody> <tr> <td>Modbus</td> <td>TCP 502; UDP 502</td> </tr> <tr> <td>DNP3</td> <td>TCP 20000</td> </tr> <tr> <td>IEC-60870-5-104</td> <td>TCP 2404</td> </tr> <tr> <td>IEC-61850-MMS</td> <td>TCP 102</td> </tr> <tr> <td>OPC-DA</td> <td>TCP 135</td> </tr> <tr> <td>OPC-UA</td> <td>TCP 4840; UDP 4840</td> </tr> <tr> <td>CIP-EtherNet/IP</td> <td>TCP 44818; UDP 2222</td> </tr> <tr> <td>Siemens-Step7</td> <td>TCP 102</td> </tr> <tr> <td>Moxa-RealCOM</td> <td>TCP 950-981</td> </tr> <tr> <td>Moxa-MXview-Request</td> <td>TCP 161, 162, 443, 4000; UDP 4000, 40404</td> </tr> </tbody> </table>	Name	Detail	Modbus	TCP 502; UDP 502	DNP3	TCP 20000	IEC-60870-5-104	TCP 2404	IEC-61850-MMS	TCP 102	OPC-DA	TCP 135	OPC-UA	TCP 4840; UDP 4840	CIP-EtherNet/IP	TCP 44818; UDP 2222	Siemens-Step7	TCP 102	Moxa-RealCOM	TCP 950-981	Moxa-MXview-Request	TCP 161, 162, 443, 4000; UDP 4000, 40404
	Name	Detail																						
	Modbus	TCP 502; UDP 502																						
	DNP3	TCP 20000																						
	IEC-60870-5-104	TCP 2404																						
IEC-61850-MMS	TCP 102																							
OPC-DA	TCP 135																							
OPC-UA	TCP 4840; UDP 4840																							
CIP-EtherNet/IP	TCP 44818; UDP 2222																							
Siemens-Step7	TCP 102																							
Moxa-RealCOM	TCP 950-981																							
Moxa-MXview-Request	TCP 161, 162, 443, 4000; UDP 4000, 40404																							
show	Display overall settings in this entry before exit.																							
abort	Exits sub-level configuration mode without saving any changes.																							
exit	Commit new settings and exit sub-level configuration mode.																							
<b>Defaults</b>	N/A																							
<b>Command Modes</b>	Global configuration, sub-level configuration																							
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>No modification function is provided. In case modification is required, remove it first and then add a new object.</li> <li>Exits the sub-level configuration mode to let settings take effect.</li> </ul>																							
<b>Examples</b>	<pre> Create an object of Industrial-Application-Service type for Layer 3-7 policy: router# configure router(config)# object industrial-application-service router(config-obj-indust-app)# name Industrial-app-service1 router(config-obj-indust-app)# select Modbus router(config-obj-indust-app)# exit </pre>																							
<b>Error Messages</b>	% Object named xxx is already existed.																							
	% No object named xxx found.																							
	% No network service object named xxx was found.																							
	% xxx is over length. It must be 1 - 32.																							
	% Please at least select one object.																							
	^Parse error																							
	^Incomplete command																							
<b>Related Commands</b>	show object																							

## show object

To check the object settings on the router, use the **show object** command.

### **Synopsis**

# **show object**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show object Name                               Detail ----- obj1                                Network-Service ED1                                 192.168.10.1 User-defined-Service1             TCP 8888; UDP 8888 NetworkSrv1                       File-Transfer Industrial-app-service1           Modbus</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	object address object service object network-service object industrial-application-service

# Firewall

## Layer 2 Policy

### I2-policy

To create a firewall layer 2 policy rule, use the **I2-policy** global configuration command and corresponding sub-level configuration mode commands. To remove the firewall layer 2 policy, use **no** form of this command.

#### **Synopsis**

##### **Create / Remove Layer 2 policy index**

```
(config)# I2-policy <l2-index>  
(config)# no I2-policy <l2-index>
```

##### **Enable / Disable Layer 2 policy.**

```
(config)# I2-policy <l2-index> {enable | disable}
```

##### **Set Layer 2 policy action in sub-level configuration mode**

```
(config-l2filter)# action {accept | drop }
```

##### **Set Layer 2 policy EtherType protocol in sub-level configuration mode**

```
(config-l2filter)# protocol {all | manual} | list | <pro-opts>}
```

##### **Set Layer 2 policy EtherType string in sub-level configuration mode**

```
(config-l2filter)# ether-type <type-string>
```

##### **Set Layer 2 policy source MAC address in sub-level configuration mode**

```
(config-l2filter)# src-mac <mac>
```

##### **Set Layer 2 policy destination MAC address in sub-level configuration mode**

```
(config-l2filter)# dst-mac <mac>
```

##### **Set Layer 2 policy logging enabled / disabled in sub-level configuration mode**

```
(config-l2filter)# logging  
(config-l2filter)# no logging
```

##### **Set Layer 2 policy log severity in sub-level configuration mode**

```
(config-l2filter)# logging severity <severity-level>
```

**Set / Clear Layer 2 policy log destination in sub-level configuration mode** (for multiple logging destinations, use different arguments separately)

```
(config-l2filter)# logging {syslog | flash | trap}  
(config-l2filter)# no logging {syslog | flash | trap}
```

##### **Set Layer 2 policy "from" and "to" interfaces in sub-level configuration mode**

```
(config-l2filter)# interface <if-from> <if-to>
```

##### **Save and Exit Layer 2 policy configuration.**

```
(config-l2filter)# exit
```

<b>Option Description</b>	no	Remove or set to default
	I2-policy	Configure Layer 2 Policy
	I2-index	One of the following: 1. Index of existing <b>Layer 2 policy</b> : New <b>Layer 2 policy</b> will be created at this position and original index after this value will be incremented by 1. 2. A new index: New index value should be the last existing index value plus 1.
	exit	Commit new settings and exit sub-level configuration mode.
	action	Specifies the action when the packet matches the firewall policy
	accept	Accepts the packet
	drop	Drops the packet
	protocol	Specifies ether-type, all or manual
	all	Specifies all listed layer 2 protocols
	manual	Specifies one of listed layer 2 protocols
	list	Specifies to list available protocol options
	pro-opts	Uses one of below protocol options: {ipv4   x25   arp   frame-relay-arp   g8bpq-ax-25-ethernet-packet   dec-assigned-proto   dec-dna-dump-load   dec-dna-remote-console   dec-dna-routing   dec-lat   dec-diagnostics   dec-customer-use   dec-systems-comms-arch   trans-ether-bridging   raw-frame-relay   appletalk-aarp   appletalk   802-1q-virtual-lan-tagged-frame   novell-ipx   netbeui   ip-version-6   ppp   multiprotocol-over-atm   pppoe-discovery-messages   pppoe-session-messages   frame-based-atm-transport-over-ethernet   loopback}
	ether-type	Specifies ether-type
	type-string	Include one of below strings: { 0x0800   0x0805   0x0806   0x0808   0x08FF   0x6000   0x6001   0x6002   0x6003   0x6004   0x6005   0x6006   0x6007   0x6558   0x6559   0x80F3   0x809B   0x8100   0x8137   0x8191   0x86DD   0x880B   0x884C   0x8863   0x8864   0x8884   0x9000}
	src-mac	Specifies to check source MAC address in the packet
	mac	MAC address
	dst-mac	Specifies to check destination MAC address in the packet
	logging	Specifies logging settings for the policy
	severity	Specifies severity of logging
	severity-level	Specifies an integer for: {Emergency(0)   Alert(1)   Critical(2)   Error(3)   Warning(4)   Notice(5)   Information(6)   Debug(7)}
	flash	Specifies writing event logs into flash.
	syslog	Specifies sending event logs to syslog server
	trap	Specifies sending event logs via SNMP trap
	interface	Specifies From and To interfaces
	if-from	ALL or Port ID (consists of module/port-number). e.g. 1/5
	if-to	ALL or Port ID (consists of module/port-number). e.g. 1/5
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>No modification function is provided. In case modification on a specific index is required, remove it first and then add a new policy.</li> <li>Command # <b>protocol manual</b> is required when configuring a specific ether-type.</li> <li>Types a valid index to enter sub-level configuration mode.</li> <li>Exits the sub-level configuration mode to let settings take effect.</li> <li>Network interfaces related to this firewall feature must be created in advance.</li> <li>Layer 2 policy priority is higher than the Layer 3 policy.</li> <li>Trap only works when logging is enabled, SNMP is enabled and SNMP trap is well configured.</li> </ul>	
<b>Examples</b>	Drop ARP packets from a port-based bridge interface member port PORT7 to PORT8:	

	<pre> router# configure router(config)# l2-policy 1 router(config-l2filter)# action drop router(config-l2filter)# interface 1/7 1/8 router(config-l2filter)# protocol manual router(config-l2filter)# ether-type 0x0806 router(config-l2filter)# src-mac 00:00:00:00:00:00 router(config-l2filter)# dst-mac 00:00:00:00:00:00 router(config-l2filter)# exit </pre>
<b>Error Messages</b>	% Invalid Input Interface Name
	% Invalid Output Interface Name.
	% Invalid Index. It must be 1 - N.
	% Layer2 Filter list is empty.
	% Invalid Protocol.
	% Ethertype have values between 0x0600 and 0xFFFF.
	% Invalid Severity Level. (0-7)
	% Port does not exist
	% Invalid format
<b>Related Commands</b>	show l2-policy
	show logging event-log l2-policy severity <range>

## show l2-policy

To check the Layer 2 firewall policy settings on the router, use the **show l2-policy** command.

### Synopsis

# **show l2-policy**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre> router# show l2-policy Index          :1 State          :Enable Action         :ACCEPT Interface      :from ALL to ALL Protocol       :ALL Source MAC     :00:00:00:00:00:00 Destination MAC :00:00:00:00:00:00 ACTION        :ACCEPT Log            : Disable Severity       : &lt;4&gt; Warning Local Storage  : Disable Syslog Server  : Disable Trap Server    : Disable </pre>
<b>Error Messages</b>	^Parse error
	^Incomplete command
<b>Related Commands</b>	l2-policy show logging event-log l2-policy show logging event-log l2-policy severity <range>

## Layer 3 - 7 Policy

### I317-policy

To create a Layer 3-7 firewall policy, use the **I317-policy** global configuration command and corresponding sub-level configuration mode commands. To remove the firewall policy, use **no** form of this command.

#### Synopsis

**Create / Remove Layer 3-7 policy index** (without <firewall-index>, a new index will be created in sequence)

```
(config)# I317-policy [<firewall-index>]  
(config)# no I317-policy <firewall-index>
```

**Enable / Disable Layer 3-7 policy globally or set default action.**

```
(config)# I317-policy {enable |  
                  disable |  
                  default-action {allow | deny}}
```

**Set Layer 3-7 policy enabled / disabled in sub-level configuration mode**

```
(config-I317-policy)# enable  
(config-I317-policy)# no enable
```

**Set / Clear Layer 3-7 policy name in sub-level configuration mode**

```
(config-I317-policy)# name <name-string>  
(config-I317-policy)# no name
```

**Set / Clear Layer 3-7 policy description in sub-level configuration mode**

```
(config-I317-policy)# description <desc>  
(config-I317-policy)# no description
```

**Set Layer 3-7 policy logging enabled / disabled in sub-level configuration mode**

```
(config-I317-policy)# logging  
(config-I317-policy)# no logging
```

**Set / Clear Layer 3-7 policy logging in sub-level configuration mode** (for multiple logging destinations, use different arguments separately)

```
(config-I317-policy)# logging {severity <severity-level> |  
                                  flash |  
                                  syslog |  
                                  trap}  
(config-I317-policy)# no logging {flash |  
                                  syslog |  
                                  trap}
```

**Set / Clear Layer 3-7 policy interface in sub-level configuration mode**

```
(config-I317-policy)# interface <if-from> <if-to>  
(config-I317-policy)# no interface
```

**Set Layer 3-7 policy mode in sub-level configuration mode**

```
(config-I317-policy)# mode {ip |  
                              mac |  
                              ip-mac}
```

**Set / Clear Layer 3-7 policy source MAC address in sub-level configuration mode**

```
(config-l3l7-policy)# src-mac <mac-addr>
(config-l3l7-policy)# no src-mac
```

**Set / Clear Layer 3-7 policy source IP address in sub-level configuration mode**

```
(config-l3l7-policy)# src-ip {list | <object-name>}
(config-l3l7-policy)# no src-ip
```

**Set / Clear Layer 3-7 policy source port in sub-level configuration mode**

```
(config-l3l7-policy)# src-port {list | <object-name>}
(config-l3l7-policy)# no src-port
```

**Set / Clear Layer 3-7 policy destination IP address in sub-level configuration mode**

```
(config-l3l7-policy)# dst-ip {list | <object-name>}
(config-l3l7-policy)# no dst-ip
```

**Set / Clear Layer 3-7 policy destination port in sub-level configuration mode**

```
(config-l3l7-policy)# dst-port {list | <object-name>}
(config-l3l7-policy)# no dst-port
```

**Set Layer 3-7 policy action in sub-level configuration mode**

```
(config-l3l7-policy)# action {allow |
                               deny }
```

**Show Layer 3-7 policy configuration before exit / abort**

```
(config-l3l7-policy)# show
```

**Quit Layer 3-7 policy configuration without saving**

```
(config-l3l7-policy)# abort
```

**Save and Exit Layer 3-7 policy configuration.**

```
(config-l3l7-policy)# exit
```

Option Description	firewall-index	Could be one of below cases: 1. Index of existing firewall policy: New firewall policy will be created at this position and original index after this value will be incremented by 1. 2. A new index: New index value should be the last existing index value plus 1.
	enable	Specifies to enable the Firewall policy
	default-action	Specifies the default action when the packet matches the firewall policy. (allow or deny)
	name	Specifies the Firewall policy's name
	name-string	A set of characters without a whitespace. Maximum length is 32.
	description	Specifies the description of the Firewall rule
	desc	A set of characters without a whitespace. Maximum length is 128.
	logging	Specifies logging settings for the policy
	severity	Specifies severity of logging
	severity-level	Specifies an integer for: {Emergency(0)   Alert(1)   Critical(2)   Error(3)   Warning(4)   Notice(5)   Information(6)   Debug(7)}
	flash	Specifies writing event logs into flash.
	syslog	Specifies sending event logs to syslog server
	trap	Specifies sending event logs via SNMP trap

	interface	Specifies From and To interfaces
	if-from	any or interface name
	if-to	any or interface name
	mode	Specifies filter mode
	ip	IP address filter
	mac	Source MAC filter
	ip-mac	IP and source MAC filter
	src-mac	Specifies to check source MAC address in the packet
	mac-addr	MAC address
	src-ip	Specifies to check source IP addresses in the packet
	list	Lists available objects
	object-name	Pre-defined object
	dst-ip	Specifies to check destination IP addresses in the packet
	src-port	Specifies to check source port in the packet
	dst-port	Specifies to check destination port in the packet
	action	Specifies the action when the packet matches the firewall policy
	allow	Accepts the packet
	deny	Drops the packet
	show	Display overall settings in this entry before exit.
	abort	Exits sub-level configuration mode without saving any changes.
	exit	Commit new settings and exit sub-level configuration mode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• No modification function is provided. In case modification on a specific index is required, remove it first and then add a new policy.</li> <li>• Types a valid index to enter sub-level configuration mode.</li> <li>• Exits the sub-level configuration mode to let settings take effect.</li> <li>• Network interfaces related to this firewall feature must be created in advance.</li> <li>• Layer 2 policy priority is higher than the Layer 3 policy.</li> <li>• Create network(service) object(s) in advance so that those object(s) can be used on this firewall policy.</li> <li>• Configure SNMP Trap in advance when sending event logs via SNMP trap.</li> <li>• Configure Syslog server in advance when sending event logs to syslog server.</li> <li>• "uuid" option in this command is reserved for Moxa use only.</li> </ul>	
<b>Examples</b>	<p>Drop all packets from interface LAN10 to LAN20:</p> <pre>router# configure router(config)# 1317-policy 1 router(config-1317-policy)# name dropLAN10 router(config-1317-policy)# no logging router(config-1317-policy)# logging severity 4 router(config-1317-policy)# logging flash router(config-1317-policy)# no logging syslog router(config-1317-policy)# no logging trap router(config-1317-policy)# interface LAN10 LAN20 router(config-1317-policy)# action deny router(config-1317-policy)# mode ip router(config-1317-policy)# enable router(config-1317-policy)# exit</pre> <p>Delete L3-7 policy index 1:</p> <pre>router# configure router(config)# no 1317-policy 1 router(config)# exit</pre> <p>Allow all packets from the end device (using pre-defined object "ED1" in this example) to LAN20:</p> <pre>router# configure router(config)# 1317-policy 2 router(config-1317-policy)# name Allow-ED1 router(config-1317-policy)# no logging router(config-1317-policy)# logging severity 4</pre>	



	<pre> router(config-l3l7-policy)# logging flash router(config-l3l7-policy)# no logging syslog router(config-l3l7-policy)# no logging trap router(config-l3l7-policy)# interface LAN LAN20 router(config-l3l7-policy)# action allow router(config-l3l7-policy)# mode ip router(config-l3l7-policy)# src-ip ED1 router(config-l3l7-policy)# dst-ip Server1 router(config-l3l7-policy)# enable router(config-l3l7-policy)# exit </pre>
<b>Error Messages</b>	% Policy Name is required.
	% xxx is over length. It must be 1 - 32.
	% Invalid Incoming Interface Name.
	% Invalid Outgoing Interface Name.
	% Invalid Policy Index.
	% Invalid Severity Level. (0-7)
	% Object Not Found.
	^Parse error
	^Incomplete command
<b>Related Commands</b>	<pre> show l3l7-policy show logging event-log l3l7-policy snmp-server host snmp-server trap-mode logging &lt;ip-addr&gt; settingcheck </pre>

## show l3l7-policy

To check the Layer 3-7 firewall policy settings on the router, use the **show l3l7-policy** command.

### Synopsis

# **show l3l7-policy**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre> router# show l3l7-policy Global Policy Settings ----- Status                               : Enable Default Action                       : Deny All  Policy Event Global Setting ----- Log                                   : Enable  Policy Setting ----- Index                                 : 1 Status                               : Enable Name                                  : dropLAN10 Description                           : Incoming Interface                   : LAN10 Outgoing Interface                   : LAN20 </pre>

	Filter Mode	: IP/Port Filtering
	Source IP Address	: any
	Source Port	: any
	Destination IP Address	: any
	Destination Port or Protocol	: any
	Action	: Deny
	Log	: Disable
	Severity	: <4> Warning
	Local Storage	: Enable
	Syslog Server	: Disable
	SNMP Trap Server	: Disable
	-----	
	Index	: 2
	Status	: Enable
	Name	: Allow-ED1
	Description	:
	Incoming Interface	: LAN
	Outgoing Interface	: LAN20
	Filter Mode	: IP/Port Filtering
	Source IP Address	: ED1
	Source Port	: any
	Destination IP Address	: Server1
	Destination Port or Protocol	: any
	Action	: Allow
	Log	: Disable
	Severity	: <4> Warning
	Local Storage	: Enable
	Syslog Server	: Disable
	SNMP Trap Server	: Disable
	-----	
<b>Error</b>	^Parse error	
<b>Messages</b>	^Incomplete command	
<b>Related</b>	l3l7-policy	
<b>Commands</b>	show logging event-log l3l7-policy	

## Malformed Packets

### firewall malformed

To enable logging firewall events including dropped malformed packets, use the **firewall malformed** global configuration command. To disable this feature, use **no** form of this command.

Synopsis

```
(config)# firewall malformed [logging {severity <severity-level> |  
                                flash |  
                                syslog |  
                                trap}]
```

```
(config)# no firewall malformed [logging {flash |  
                                syslog |  
                                trap}]
```

<b>Option Description</b>	logging	Enables logging function for malformed packets.
	severity	Specifies severity of logging for malformed packet function
	severity-level	Specifies an integer for: {Emergency(0)   Alert(1)   Critical(2)   Error(3)   Warning(4)   Notice(5)   Information(6)   Debug(7)}
	flash	Specifies writing event logs into flash.
	syslog	Specifies sending event logs to syslog server
	trap	Specifies sending event logs via SNMP trap
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• Network interfaces related to this firewall feature must be created in advance.</li><li>• Configure SNMP Trap in advance when sending event logs via SNMP trap.</li><li>• Configure Syslog server in advance when sending event logs to syslog server.</li></ul>	
<b>Examples</b>	Drop malformed packets and set severity of log to Information(6): router# configure router(config)# firewall malformed router(config)# firewall malformed logging severity 6 router(config)# exit	
<b>Error Messages</b>	% Severity level is out of range! ^Parse error ^Incomplete command	
<b>Related Commands</b>	show firewall show logging event-log firewall snmp-server host snmp-server trap-mode logging <ip-addr>	

## show firewall

To check Malformed Packets settings on the router, use the **show firewall** command.

### Synopsis

# **show firewall**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	This command only displays Malformed Packets settings. If you need to check firewall policy settings, please use the command "show l3l7-policy" instead.
<b>Examples</b>	router # show firewall Global Setting Log Enable:Enable ----- Malformed Packets Severity :<0> Emergency Flash :Enable Syslog :Enable Trap :Enable -----
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	firewall malformed show logging event-log malformed

## Session Control

### session-control

To create a session control policy, use the **session-control** global configuration command and corresponding sub-level configuration mode commands. To remove the session control policy, use **no** form of this command.

### Synopsis

**Create / Remove session-control policy index** (without <index>, a new index will be created in sequence)

```
(config)# session-control [<index>]  
(config)# no session-control <index>
```

**Set session-control policy enabled / disabled in sub-level configuration mode**

```
(config-session-control)# enable  
(config-session-control)# no enable
```

**Set / Clear session-control policy name in sub-level configuration mode**

```
(config-session-control)# name <name-string>  
(config-session-control)# no name
```

**Set / Clear session-control policy logging in sub-level configuration mode** (for multiple logging destinations, use different arguments separately)

```
(config-session-control)# logging {severity <severity-level> |  
                                  flash |  
                                  syslog |  
                                  trap}
```

```
(config-session-control)# no logging {flash |
                               syslog |
                               trap}
```

**Set / Clear session-control policy destination IP address in sub-level configuration mode**

```
(config-session-control)# dst-ip {list | <object-name>}
(config-session-control)# no dst-ip
```

**Set / Clear session-control policy destination port in sub-level configuration mode**

```
(config-session-control)# dst-port {list | <object-name>}
(config-session-control)# no dst-port
```

**Set session-control policy action in sub-level configuration mode**

```
(config-session-control)# action {monitor |
                                   drop }
```

**Set / Clear total allowed number of TCP connections in sub-level configuration mode**

```
(config-session-control)# total-tcp-conn <number>
(config-session-control)# no total-tcp-conn
```

**Set / Clear total allowed number of concurrent TCP requests in sub-level configuration mode**

```
(config-session-control)# concurrent-tcp-conn <limit>
(config-session-control)# no concurrent-tcp-conn
```

**Show session-control policy configuration before exit / abort**

```
(config-session-control)# show
```

**Quit session-control policy configuration without saving**

```
(config-session-control)# abort
```

**Save and Exit session-control policy in sub-level configuration mode.**

```
(config-session-control)# exit
```

Option Description	index	Could be one of below cases: 1. Index of existing session-control policy: New policy will be created at this position and original index after this value will be incremented by 1. 2. A new index: New index value should be the last existing index value plus 1.
	enable	Specifies to enable the session control policy
	name	Specifies the session control policy's name
	name-string	A set of characters without a whitespace. Maximum length is 32.
	logging	Specifies logging settings for the policy
	severity	Specifies severity of logging
	severity-level	Specifies an integer for: {Emergency(0)   Alert(1)   Critical(2)   Error(3)   Warning(4)   Notice(5)   Information(6)   Debug(7)}
	flash	Specifies writing event logs into flash.
	syslog	Specifies sending event logs to syslog server
	trap	Specifies sending event logs via SNMP trap
	dst-ip	Specifies to check destination IP addresses in the packet
	dst-port	Specifies to check destination port in the packet
	list	Specifies to list available objects
	object-name	Pre-defined object
	action	Specifies the action when the packet matches the session control policy
	monitor	Monitors the packet
	drop	Drops the packet

	total-tcp-conn	Specifies the total allowed number of TCP connections
	number	Max. number of TCP connections
	concurrent-tcp-conn	Specifies the total allowed number of concurrent TCP requests.
	limit	Connections per second
	show	Display overall settings in this entry before exit.
	abort	Exits sub-level configuration mode without saving any changes.
	exit	Commit new settings and exit sub-level configuration mode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>No modification function is provided. In case modification on a specific index is required, remove it first and then add a new policy.</li> <li>Types a valid index to enter sub-level configuration mode.</li> <li>Exits the sub-level configuration mode to let settings take effect.</li> <li>Create network(service) object(s) in advance so that those object(s) can be used on this session control policy.</li> <li>Configure SNMP Trap in advance when sending event logs via SNMP trap.</li> <li>Configure Syslog server in advance when sending event logs to syslog server.</li> <li>"uuid" option in this command is reserved for Moxa use only.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Drop all packets when total TCP connections to Server1 exceeds 10:  <pre>router# configure router(config)# session-control 1 router(config-session-control)# name sc-rule1 router(config-session-control)# enable router(config-session-control)# logging severity 4 router(config-session-control)# logging flash router(config-session-control)# no logging syslog router(config-session-control)# no logging trap router(config-session-control)# action drop router(config-session-control)# dst-ip Server1 router(config-session-control)# total-tcp-conn 10 router(config-session-control)# exit</pre> </li> <li>Delete session control index 1:  <pre>router# configure router(config)# no session-control 1 router(config)# exit</pre> </li> </ul>	
<b>Error Messages</b>	<pre>% Policy Name is required. % Destination IP is required. % Either Total TCP Connections or Concurrent TCP Requests Limitation needs to be set. % xxx is over length. It must be 1 - 32. % Invalid Policy Index. % Invalid Severity Level. (0-7) % Invalid parameter! % Object Not Found. ^Parse error ^Incomplete command</pre>	
<b>Related Commands</b>	<pre>show session-control snmp-server host snmp-server trap-mode logging &lt;ip-addr&gt;</pre>	

## show session-control

To check the session-control policy settings on the router, use the **show session-control** command.

### Synopsis

# **show session-control**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show session-control  Session Control Policy Setting ----- Index                : 1 Status               : Enable Name                 : sc-rule1 Destiantion IP       : Server1 Destiantion Port     : Any Total TCP Connections Limitation : 10 (Connections) Concurrent TCP Requests Limitation : - Action               : Drop Severity             : &lt;4&gt; Warning Local Storage        : Enable Syslog Server        : Disable SNMP Trap Server     : Disable</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	session-control

## Denial of Service (DoS) Defense

### dos

To enable DoS port-scan protection or flood protection, use the **dos** global configuration command. To disable DoS port-scan protection or flood protection, use **no** form of this command.

#### Synopsis

```
(config)# dos {null-scan | xmas-scan | nmap-xmas-scan | syn-fin-scan | fin-scan |
nmap-id-scan | syn-rst-scan | tcp-sessions-without-syn |
icmp-flood <limit> |
syn-flood <limit> |
arp-flood <limit>}
```

```
(config)# no dos {null-scan | xmas-scan | nmap-xmas-scan | syn-fin-scan | fin-scan |
nmap-id-scan | syn-rst-scan | tcp-sessions-without-syn |
icmp-flood | syn-flood | arp-flood}
```

<b>Option Description</b>	null-scan	Specifies port-scan protection method: Null-Scan
	xmas-scan	Specifies port-scan protection method: Xmas-Scan
	nmap-xmas-scan	Specifies port-scan protection method: NMAP-Xmas-Scan
	syn-fin-scan	Specifies port-scan protection method: SYN/FIN Scan
	fin-scan	Specifies port-scan protection method: FIN Scan
	nmap-id-scan	Specifies port-scan protection method: NMAP-ID Scan
	syn-rst-scan	Specifies port-scan protection method: SYN/RST Scan
	tcp-sessions-without-syn	Specifies session SYN protection
	icmp-flood	Specifies flood-protection method: ICMP-Flood
	syn-flood	Specifies flood-protection method: SYN-Flood
	arp-flood	Specifies flood-protection method: ARP-Flood
	limit	The limit value (pkt/sec) to activate ICMP-Flood/SYN-Flood/ARP-Flood). Integer ranges from 1 to 4000.
<b>Defaults</b>	The default settings have all features enabled, except for 'new-tcp-without-syn-scan', which is disabled by default.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable xmas-scan port scan protection: router# configure router(config)# dos xmas-scan	
<b>Error Messages</b>	% Invalid DoS Attack Name.	
	% Limit bandwidth must be 1 - 4000 pkt/s.	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	logging dos show dos	



## Configure DoS Functions

### Synopsis

```
(config)# dos { null-scan | xmas-scan | nmap-xmas-scan | syn-fin-scan | fin-scan | nmap-id-scan
| syn-rst-scan | tcp-sessions-without-syn | icmp-flood <icmp-limit> | syn-flood <syn-limit> |
arp-flood <arp-limit> | udp-flood <udp-limit> }
```

```
(config)# no dos { null-scan | xmas-scan | nmap-xmas-scan | syn-fin-scan | fin-scan | nmap-id-
scan | syn-rst-scan | tcp-sessions-without-syn | icmp-flood | syn-flood | arp-flood | udp-flood }
```

<b>Option Description</b>	dos	Enable DoS (Deny of Service) Defense / Disable DoS (Deny of Service) Defense
	no	Negate Command or Set to Default
	null-scan	Null Scan
	xmas-scan	Xmas Scan
	nmap-xmas-scan	NMAP-Xmas Scan
	syn-fin-scan	SYN/FIN Scan
	fin-scan	FIN Scan
	nmap-id-scan	NMAP-ID Scan
	syn-rst-scan	SYN/RST Scan
	tcp-sessions-without-syn	TCP Sessions Without SYN
	icmp-flood	ICMP-Flood
	icmp-limit	Limit of ICMP Flood (pkt/s)
	syn-flood	SYN-Flood
	syn-limit	Limit of SYN Flood (pkt/s)
	arp-flood	ARP-Flood
	arp-limit	Limit of ARP Flood (pkt/s)
	udp-flood	UDP-Flood
	udp-limit	Limit of UDP Flood (pkt/s)
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Enable xmas-scan port scan protection: router# configure router(config)# dos xmas-scan	
<b>Error Messages</b>	% Limit bandwidth must be 1 - 2000 pkt/s. (for ARP Flood)	
	% Limit bandwidth must be 1 - 4000 pkt/s. (for SYN Flood and ICMP Flood)	
	% Limit bandwidth must be 1 - 8000 pkt/s. (for UDP Flood)	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show dos	

## Show DoS Configuration

### show dos

To show DoS configuration, use the **show dos** command.

#### Synopsis

#### #show dos

<b>Option</b>	show	Show system information
<b>Description</b>	dos	Display DoS Defense configurations
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre>router# show dos null-scan           : Enable xmas-scan           : Enable nmap-xmas-scan     : Enable syn/fin-scan       : Enable fin-scan           : Enable nmap-id-scan       : Enable syn/rst-scan       : Enable tcp-sessions-without-syn: Disable icmp-flood         : Enable      Limit: 1000 (pkt/s) syn-flood          : Enable      Limit: 4000 (pkt/s) arp-flood          : Enable      Limit: 2000 (pkt/s) udp-flood          : Enable      Limit: 2000 (pkt/s) Severity           : &lt;2&gt; Critical Flash              : Enable Syslog             : Enable Trap               : Enable</pre>	
<b>Error Messages</b>	N/A	
<b>Related Commands</b>	dos { null-scan   xmas-scan   nmap-xmas-scan   syn-fin-scan   fin-scan   nmap-id-scan   syn-rst-scan   tcp-sessions-without-syn   icmp-flood <icmp-limit>   syn-flood <syn-limit>   arp-flood <arp-limit>   udp-flood <udp-limit> } no dos { null-scan   xmas-scan   nmap-xmas-scan   syn-fin-scan   fin-scan   nmap-id-scan   syn-rst-scan   tcp-sessions-without-syn   icmp-flood   syn-flood   arp-flood   udp-flood }	

## DoS Log Configuration

### logging dos

To set up DoS logging, severity, and log destinations, use the following commands.

#### **Synopsis**

(config)# **logging dos**

(config)# **logging dos { severity <severity-level> | flash | syslog | trap }**

(config)# **no logging dos**

(config)# **no logging dos { flash | syslog | trap }**

<b>Option</b>	logging	Set logging
<b>Description</b>	no	Negate Command or Set to Default
	dos	Enable DoS log / Disable Dos log
	severity	Set log severity
	flash	Save log in Local Storage
	syslog	Send log in Syslog Server
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Router(config)# logging dos	
<b>Error Messages</b>	% Severity level is out of range!	
<b>Related Commands</b>	dos { null-scan   xmas-scan   nmap-xmas-scan   syn-fin-scan   fin-scan   nmap-id-scan   syn-rst-scan   tcp-sessions-without-syn   icmp-flood <icmp-limit>   syn-flood <syn-limit>   arp-flood <arp-limit>   udp-flood <udp-limit> } no dos { null-scan   xmas-scan   nmap-xmas-scan   syn-fin-scan   fin-scan   nmap-id-scan   syn-rst-scan   tcp-sessions-without-syn   icmp-flood   syn-flood   arp-flood   udp-flood }	

# Soft Lockdown Mode

## soft lockdown-mode

Soft Lockdown Mode is a feature that monitors crucial system metrics such as CPU utilization and available memory. It can restrict both incoming and outgoing traffic on a specified interface in response to specified irregular resource usage to ensure router stability. To enable Soft Lockdown Mode, use the **soft lockdown-mode** global configuration command. To disable Soft Lockdown Mode or return settings to default, use **no** form of this command.

### Synopsis

```
(config)# soft lockdown-mode {enable |  
    interface <if-name> |  
    cpu-utilization <cpu-threshold> |  
    free-memory <mem-threshold> |  
    monitoring-interval <second> |  
    enter <enter-cycle> |  
    leave <leave-cycle> }
```

```
(config)# no soft lockdown-mode {enable |  
    interface |  
    cpu-utilization |  
    free-memory |  
    monitoring-interval |  
    enter |  
    leave }
```

<b>Option Description</b>	enable	Specifies to enable or disable Soft Lockdown Mode.
	interface	Specifies the interface to which this mode is applied.
	if-name	Interface name. Default value is null.
	cpu-utilization	Specifies a threshold percentage when CPU usage is higher than user configured.
	cpu-threshold	Integer value ranges from 1 to 90. Default value is 70.
	free-memory	Specifies a threshold percentage when free memory is lower than user configured.
	mem-threshold	Integer value ranges from 1 to 50. Default value is 20.
	monitoring-interval	Specifies a cycle time (in seconds) to monitor CPU/memory periodically.
	second	Integer value ranges from 1 to 5. Default value is 1.
	enter	Specifies the failure cycles to enter Soft Lockdown Mode.
	enter-cycle	Integer value ranges from 3 to 10. Default value is 5.
	leave	Specifies the normal cycles to leave Soft Lockdown Mode.
	leave-cycle	Integer value ranges from 3 to 10. Default value is 5.
<b>Defaults</b>	Soft lockdown mode is disabled.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>Make sure the intended interface is created before enabling this feature.</li><li>When the Soft Lockdown Mode is enabled, user can not adjust port setting or Vlan setting, otherwise it will cause the interface member mismatch, disrupting normal operations.</li></ul>	
<b>Examples</b>	Enable Soft Lockdown Mode on interface LAN8 and configure thresholds for CPU usage (80%) and free memory (50%). router# configure router(config)# soft lockdown-mode enable router(config)# soft lockdown-mode interface LAN8 router(config)# soft lockdown-mode cpu-utilization 80 router(config)# soft lockdown-mode free-memory 50 router(config)# exit	
	% Invalid interface Interface Name.	

<b>Error Messages</b>	% Must be 1 - 90.
	% Must be 1 - 50.
	% Must be 1 - 5.
	% Must be 3 - 10.
<b>Related Commands</b>	show soft lockdown-mode

## show soft lockdown-mode

To check the Soft Lockdown Mode settings on the router, use the **show soft lockdown-mode** command.

### Synopsis

# **show soft lockdown-mode**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show soft lockdown-mode Soft lockdown mode   Status                               : Not in soft lockdown mode.   Enable                               : Enable   Interface                             : LAN8   CPU utilization threshold(%)         : 80   Free memory Space threshold(%)       : 50   Status monitoring interval(sec)      : 1   Failure cycles to enter soft lockdown mode : 5   Normal cycles to leave soft lockdown mode : 5 router#</pre>
<b>Error Messages</b>	^Parse error
	^Incomplete command
<b>Related Commands</b>	soft lockdown-mode

# Virtual Private Network (VPN)

## IPsec Configuration

### ipsec

To specify or modify IPsec function on the router, use the **ipsec** global configuration command and related sub-level configuration command sets. To disable or remove IPsec connection, use **no** form of this command.

#### **Synopsis**

```
(config)# ipsec {all-connect | nat-t}
(config)# ipsec <ipsec-name>
(config-ipsec)# {exit |
    l2tp |
    remote-gateway <remote-ip> |
    interface <wanif-name> |
    startup-mode {start | wait} |
    local-network <loc-ip> <loc-netmask> |
    local-multi-network <loc-subnet> |
    remote-network <rem-ip> <rem-netmask> |
    remote-multi-network <rem-subnet> |
    identity {address [<addr-loc-ip> <addr-rem-ip>] |
        fqdn <loc-id> <rem-id> |
        key-id <loc-key-id> <rem-key-id> |
        auto} |
    dpd-action {hold |
        clear |
        disable |
        restart} |
    dpd-delay <delay-seconds> |
    dpd-timeout <timeout-seconds>}

(config-ipsec)# no l2tp

(config-ipsec)# phase1
(config-ipsec-phase1)# {ike-mode {main |
    aggressive} |
    ike-version {ikev1 |
        ikev2} |
    auth-mode {psk <psk-key> |
        x509 <loc-cert> <rem-cert> |
        x509ca <loc-cert>} |
    encryption <enc-algo> |
    hash <hash-algo> |
    dh-group <dh-grps> |
    life-time <lt-min> |
    exit}

(config-ipsec)# phase2
(config-ipsec-phase2)# {pfs [<dh-grps>] |
    encryption <enc-algo> |
    hash <hash-algo> |
    life-time <lt-min> |
    exit}

(config-ipsec-phase2)# no pfs

(config)# ipsec <ipsec-name> {enable |
    disable}
```

```
(config)# no ipsec {all-connect |
                    nat-t |
                    <ipsec-name>}
```

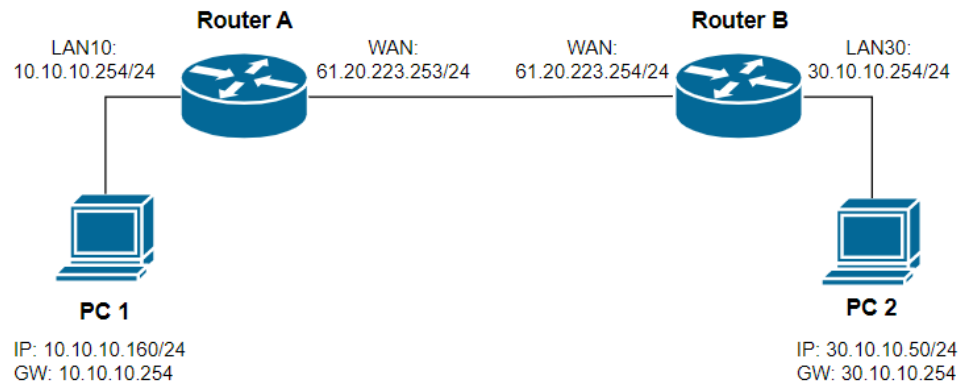
Option Description	all-connect	Enables All IPsec Connection
	nat-t	Enables IPsec NAT-T
	ipsec-name	IPsec connection name. A set of characters without a whitespace. Maximum length is 32.
	exit	Commit new settings and exit sub-level configuration mode.
	l2tp	Enables/disables L2TP tunnel
	remote-gateway	Specifies a remote VPN gateway
	remote-ip	IP address of the remote VPN gateway
	interface	Specifies WAN interface
	wanif-name	WAN, wanif-name is case-sensitive.
	startup-mode	Specifies connection startup mode
	start	This VPN tunnel will actively initiate the connection with the remote VPN gateway.
	wait	This VPN tunnel will wait remote VPN gateway to initiate the connection.
	local-network	Specifies local VPN network
	loc-ip	IP address of the local VPN network
	loc-netmask	Netmask of the local VPN network
	local-multi-network	Specifies local VPN network subnets.
	loc-subnet	Local network subnets. E.g.192.168.127.0/24,....
	remote-network	Specifies remote VPN network
	rem-ip	IP address of the remote VPN network
	rem-netmask	Netmask of the remote VPN network
	remote-multi-network	Specifies remote VPN network subnets
	rem-subnet	Local network subnets. E.g.192.168.127.0/24,....
	identity	Specifies one of four ID types
	address	Specifies "address" as ID type
	addr-loc-ip	Local IP address
	addr-rem-ip	Remote IP address
	fqdn	Specifies "Fully Qualified Domain Name" as ID type
	loc-id	Uses FQDN as local ID
	rem-id	Uses FQDN as remote ID
	key-id	Specifies "Key ID" as ID type
	loc-key-id	Local key-id created by user
	rem-key-id	Remote key-id created by user
	auto	Specifies "auto" as ID type for building connections for use with Cisco's systems.
	dpd-action	Specifies an action when a Dead Peer is detected
	hold	Holds this VPN tunnel
	clear	Clears this VPN tunnel
	disable	Disables Dead Peer Detection
	restart	Restarts this VPN tunnel
	dpd-delay	Specifies a period of dead peer detection messages
	delay-seconds	Delay seconds
	dpd-timeout	Specifies a timeout to check if the connection is alive or not
	timeout-seconds	Timeout seconds
	phase1	Specifies phase1 configuration
	phase2	Specifies phase2 configuration
	ike-mode	Specifies ike-mode
	main	In 'Main' IKE Mode, both the Remote and Local VPN gateway will negotiate which Encryption/Hash algorithm and DH groups can be used in this VPN tunnel.

	aggressive	In "Aggressive" Mode, the Remote and Local VPN gateway will not negotiate the algorithm
	ike-version	Specifies ike-version
	ikev1	Uses IKE version 1 protocol
	ikev2	Uses IKE version 2 protocol
	auth-mode	Specifies authentication mode
	psk	Specifies a pre-shared key
	psk-key	Pre-shared key. A set of characters without a whitespace. Maximum length is 64
	x509	Specifies x509 mode for authentication. Two systems use certificates that users imported in advance in "Local Certificate" as an authentication tool to build an IPsec VPN connection.
	loc-cert	Local Certificate Name
	rem-cert	Remote Certificate Name
	x509ca	Specifies x509ca mode for two systems use certificates that users imported in advance in "Local Certificate", and the CA that users imported in advance in "Trusted CA Certificate" as an authentication tool to build an IPsec VPN connection.
	encryption	Specifies key exchange encryption algorithm
	enc-algo	Specifies one of the encryption algorithms: {des   3des   aes128   aes192   aes256   aes256gcm}
	prf	Specifies PRF: {PRFSHA256   PRFSHA384   PRFSHA512}
	hash	Specifies hash algorithm in key exchange
	hash-algo	Specifies one of the hash algorithms: {md5   sha1   sha256   sha512}
	dh-group	Specifies Diffie-Hellman groups (the Key Exchange group between the Remote and VPN Gateways)
	iana-number	Specifies an IANA number for one of the DH groups: {1:DH1 (modp768)   2:DH2 (modp1024)   5: DH5 (modp1536)   14:DH14 (modp2048)   15: DH15 (modp3072)   16: DH16 (modp4096)   17: DH17 (modp6144)   18: DH18 (modp8192)   22: DH22 (modp1024s160)   23:DH23 (modp2048s224)   24: DH24 (modp2048s256)   31:DH31 (curve25519)}
	life-time	Specifies key exchange life time
	lt-min	Ranges from 30 to 43200 minutes
	pfs	Enables/disables Packet Forward Secrecy option
	enable	Enables an IPsec VPN Connection
	disable	Disables an IPsec VPN Connection
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• Specifies a non-existing &lt;ipsec-name&gt; will create a new entry of an IPsec connection.</li> <li>• Types a valid name of the VPN tunnel to enter sub-level configuration mode.</li> <li>• Exits the sub-level configuration mode to let settings take effect.</li> </ul>	
<b>Examples</b>	<p><b>IPsec (Site to Site):</b></p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>• TN router A: <ul style="list-style-type: none"> <li>- WAN: 61.20.223.253/24, VLAN ID=20, WAN interface</li> <li>- LAN10: 10.10.10.254/24, VLAN ID=10, interface used for internal network</li> <li>- L2TP server: disabled</li> </ul> </li> <li>• TN router B: <ul style="list-style-type: none"> <li>- WAN: 61.20.223.254/24, VLAN ID=20, WAN interface</li> <li>- LAN30: 30.10.10.254/24, VLAN ID=30, interface used for internal network</li> <li>- L2TP server: disabled</li> </ul> </li> <li>• PC-1: <ul style="list-style-type: none"> <li>- IP: 10.10.10.160/24</li> <li>- Gateway: 10.10.10.254</li> </ul> </li> </ul>	



- PC-2 :
  - IP: 30.10.10.50/24
  - Gateway: 30.10.10.254

Network topology:



Scenario:

- Router (A) and Router (B) establish an IPsec VPN site-to-site tunnel.
- PC (1) and PC (2) can communicate with each other via this VPN site-to-site tunnel.

Commands:

On Router A:

```
router(config)# ipsec all-connect
router(config)# ipsec S2S-A
router(config-ipsec)# remote-gateway 61.20.223.254
router(config-ipsec)# interface WAN
router(config-ipsec)# startup-mode start
router(config-ipsec)# local-multi-network 10.10.10.0/24
router(config-ipsec)# remote-multi-network 30.10.10.0/24
router(config-ipsec)# identity address
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
router(config-ipsec-phase1)# ike-version ikev2
router(config-ipsec-phase1)# auth-mode psk 12345678
router(config-ipsec-phase1)# encryption aes256
router(config-ipsec-phase1)# hash sha256
router(config-ipsec-phase1)# dh-group 2048
router(config-ipsec-phase1)# life-time 43200
router(config-ipsec-phase1)# exit
router(config-ipsec)# phase2
router(config-ipsec-phase2)# pfs 2048
router(config-ipsec-phase2)# encryption aes256
router(config-ipsec-phase2)# hash sha256
router(config-ipsec-phase2)# life-time 43200
router(config-ipsec-phase2)# exit
router(config-ipsec)# dpd-action restart
router(config-ipsec)# dpd-delay 30
router(config-ipsec)# dpd-timeout 120
router(config-ipsec)# exit
router(config)#
```

On Router B:

```
router(config)# ipsec all-connect
router(config)# ipsec S2S-B
router(config-ipsec)# remote-gateway 61.20.223.253
```

```

router(config-ipsec)# interface WAN
router(config-ipsec)# startup-mode start
router(config-ipsec)# local-multi-network 30.10.10.0/24
router(config-ipsec)# remote-multi-network 10.10.10.0/24
router(config-ipsec)# identity address
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
router(config-ipsec-phase1)# ike-version ikev2
router(config-ipsec-phase1)# auth-mode psk 12345678
router(config-ipsec-phase1)# encryption aes256
router(config-ipsec-phase1)# hash sha256
router(config-ipsec-phase1)# dh-group 2048
router(config-ipsec-phase1)# life-time 43200
router(config-ipsec-phase1)# exit
router(config-ipsec)# phase2
router(config-ipsec-phase2)# pfs 2048
router(config-ipsec-phase2)# encryption aes256
router(config-ipsec-phase2)# hash sha256
router(config-ipsec-phase2)# life-time 43200
router(config-ipsec-phase2)# exit
router(config-ipsec)# dpd-action restart
router(config-ipsec)# dpd-delay 30
router(config-ipsec)# dpd-timeout 120
router(config-ipsec)# exit
router(config)#

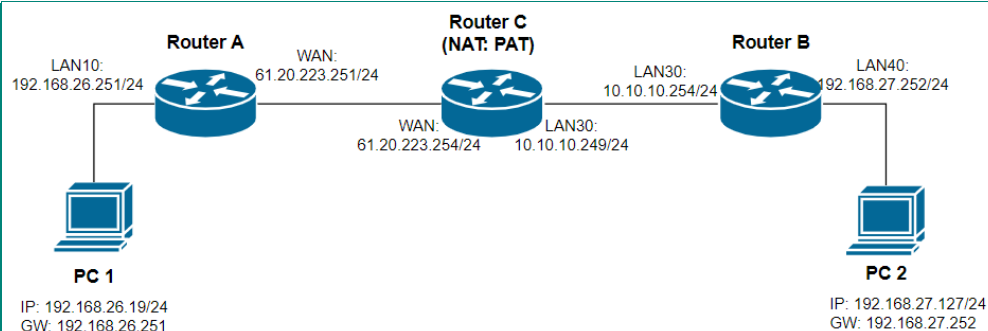
```

#### **IPsec (Site to Site: with NAT [PAT in the middle]):**

##### Prerequisites:

- TN router A:
  - WAN: 61.20.223.251/24, VLAN ID=20, WAN interface
  - LAN10: 192.168.26.251/24, VLAN ID=10, interface used for internal network
  - Gateway: 61.20.223.254
  - L2TP server: disabled
- TN router B:
  - LAN30: 10.10.10.254/24, VLAN ID=20, WAN interface
  - LAN40: 192.168.27.252/24, VLAN ID=40, interface used for internal network
  - Gateway: 10.10.10.249
  - L2TP server: disabled
- Router C:
  - WAN: 61.20.223.254/24, VLAN ID=20, WAN interface
  - LAN30: 10.10.10.249/24, VLAN ID=30, interface used for internal network
  - NAT: enable PAT
    - Translate WAN IP:500 to local 10.10.10.254:500
    - Translate WAN IP:4500 to local 10.10.10.254:4500
- PC-1:
  - IP: 192.168.26.19/24
  - Gateway: 192.168.26.251
- PC-2 :
  - IP: 192.168.27.127/24
  - Gateway: 192.168.27.252

Network topology:



#### Scenario:

- Router (A) is the router on the external network which has a public IP address.
- Router (B) is the router on the internal network which does not have a public IP address.
- Router (C) enables NAT [PAT mode] to pass through IPsec packets.
- Router (A) and Router (B) establish an IPsec VPN site-to-site tunnel.
- PC (1) and PC (2) can communicate with each other via this VPN site-to-site tunnel.

#### Commands:

##### On Router A:

```

router(config)# ipsec all-connect
router(config)# ipsec nat-t
router(config)# ipsec S2S-A
router(config-ipsec)# remote-gateway 61.20.223.254
router(config-ipsec)# interface WAN
router(config-ipsec)# startup-mode start
router(config-ipsec)# local-multi-network 192.168.26.0/24
router(config-ipsec)# remote-multi-network 192.168.27.0/24
router(config-ipsec)# identity address 192.168.26.251 192.168.27.252
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
router(config-ipsec-phase1)# ike-version ikev1
router(config-ipsec-phase1)# auth-mode psk 12345678
router(config-ipsec-phase1)# encryption aes256
router(config-ipsec-phase1)# hash sha256
router(config-ipsec-phase1)# dh-group 2048
router(config-ipsec-phase1)# life-time 43200
router(config-ipsec-phase1)# exit
router(config-ipsec)# phase2
router(config-ipsec-phase2)# encryption aes256
router(config-ipsec-phase2)# hash sha256
router(config-ipsec-phase2)# life-time 43200
router(config-ipsec-phase2)# exit
router(config-ipsec)# dpd-action restart
router(config-ipsec)# dpd-delay 30
router(config-ipsec)# dpd-timeout 120
router(config-ipsec)# exit
router(config)#

```

##### On Router B:

```

router(config)# ipsec all-connect
router(config)# ipsec nat-t
router(config)# ipsec S2S-B
router(config-ipsec)# remote-gateway 61.20.223.251
router(config-ipsec)# interface WAN
router(config-ipsec)# startup-mode start

```

```

router(config-ipsec)# local-multi-network 192.168.27.0/24
router(config-ipsec)# remote-multi-network 192.168.26.0/24
router(config-ipsec)# identity address 192.168.27.252 192.168.26.251
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
router(config-ipsec-phase1)# ike-version ikev1
router(config-ipsec-phase1)# auth-mode psk 12345678
router(config-ipsec-phase1)# encryption aes256
router(config-ipsec-phase1)# hash sha256
router(config-ipsec-phase1)# dh-group 2048
router(config-ipsec-phase1)# life-time 43200
router(config-ipsec-phase1)# exit
router(config-ipsec)# phase2
router(config-ipsec-phase2)# encryption aes256
router(config-ipsec-phase2)# hash sha256
router(config-ipsec-phase2)# life-time 43200
router(config-ipsec-phase2)# exit
router(config-ipsec)# dpd-action restart
router(config-ipsec)# dpd-delay 30
router(config-ipsec)# dpd-timeout 120
router(config-ipsec)# exit
router(config)#

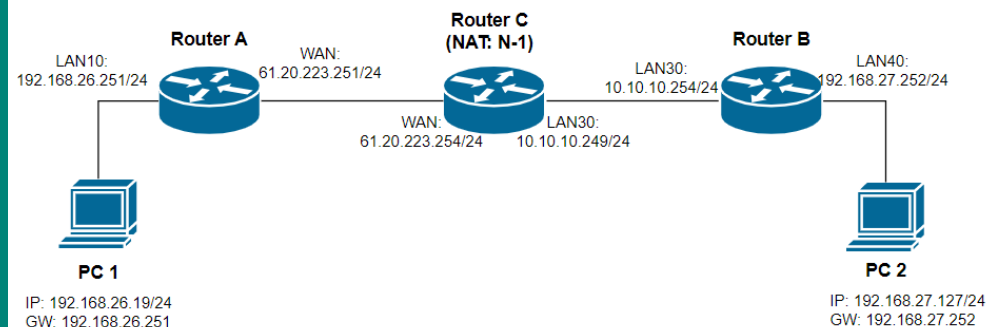
```

### IPsec (Site to Site: with NAT [N-to-1 in the middle]):

#### Prerequisites:

- TN router A:
  - WAN: 61.20.223.251/24, VLAN ID=20, WAN interface
  - LAN10: 192.168.26.251/24, VLAN ID=10, interface used for internal network
  - Gateway: 61.20.223.254
  - L2TP server: disabled
- TN router B:
  - LAN30: 10.10.10.254/24, VLAN ID=20, WAN interface
  - LAN40: 192.168.27.252/24, VLAN ID=40, interface used for internal network
  - Gateway: 10.10.10.249
  - L2TP server: disabled
- Router C:
  - WAN: 61.20.223.254/24, VLAN ID=20, WAN interface
  - LAN30: 10.10.10.249/24, VLAN ID=30, interface used for internal network
  - NAT: enable N-to-1
    - Translate local IP: 10.10.10.254 to WAN IP: 61.20.223.254
- PC-1:
  - IP: 192.168.26.19/24
  - Gateway: 192.168.26.251
- PC-2 :
  - IP: 192.168.27.127/24
  - Gateway: 192.168.27.252

#### Network topology:



Scenario:

- a) Router (A) is the router on the external network which has a public IP address.
- b) Router (B) is the router on the internal network which does not have a public IP address.
- c) Router (C) enables NAT [N-to-1 mode] to pass through IPsec packets.
- d) Router (A) and Router (B) establish an IPsec VPN site-to-site tunnel.
- e) PC (1) and PC (2) can communicate with each other via this VPN site-to-site tunnel.

Commands:

On Router A:

```
router(config)# ipsec all-connect
router(config)# ipsec nat-t
router(config)# ipsec S2S-A
router(config-ipsec)# remote-gateway 61.20.223.254
router(config-ipsec)# interface WAN
router(config-ipsec)# startup-mode start
router(config-ipsec)# local-multi-network 192.168.26.0/24
router(config-ipsec)# remote-multi-network 192.168.27.0/24
router(config-ipsec)# identity address 192.168.26.251 192.168.27.252
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
router(config-ipsec-phase1)# ike-version ikev1
router(config-ipsec-phase1)# auth-mode psk 12345678
router(config-ipsec-phase1)# encryption aes256
router(config-ipsec-phase1)# hash sha256
router(config-ipsec-phase1)# dh-group 2048
router(config-ipsec-phase1)# life-time 43200
router(config-ipsec-phase1)# exit
router(config-ipsec)# phase2
router(config-ipsec-phase2)# encryption aes256
router(config-ipsec-phase2)# hash sha256
router(config-ipsec-phase2)# life-time 43200
router(config-ipsec-phase2)# exit
router(config-ipsec)# dpd-action restart
router(config-ipsec)# dpd-delay 30
router(config-ipsec)# dpd-timeout 120
router(config-ipsec)# exit
router(config)#
```

On Router B:

```
router(config)# ipsec all-connect
router(config)# ipsec nat-t
router(config)# ipsec S2S-B
router(config-ipsec)# remote-gateway 61.20.223.251
router(config-ipsec)# interface WAN
router(config-ipsec)# startup-mode start
router(config-ipsec)# local-multi-network 192.168.27.0/24
router(config-ipsec)# remote-multi-network 192.168.26.0/24
router(config-ipsec)# identity address 192.168.27.252 192.168.26.251
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
router(config-ipsec-phase1)# ike-version ikev1
router(config-ipsec-phase1)# auth-mode psk 12345678
router(config-ipsec-phase1)# encryption aes256
router(config-ipsec-phase1)# hash sha256
router(config-ipsec-phase1)# dh-group 2048
router(config-ipsec-phase1)# life-time 43200
```

	<pre> router(config-ipsec-phase1)# exit router(config-ipsec)# phase2 router(config-ipsec-phase2)# encryption aes256 router(config-ipsec-phase2)# hash sha256 router(config-ipsec-phase2)# life-time 43200 router(config-ipsec-phase2)# exit router(config-ipsec)# dpd-action restart router(config-ipsec)# dpd-delay 30 router(config-ipsec)# dpd-timeout 120 router(config-ipsec)# exit router(config)# </pre>
<b>Error Messages</b>	% is over length. It must be 1 - 32.
	% is not existed in IPsec Connection list.
	% Invalid Netmask.
	% Remote ID can not be NULL.
	% is over length. It must be 1 - 64.
	% No such encryption algorithm.
	% No such hash algorithm.
	% Mod P must be 768, 1024, 1536 or 2048.
	% Invalid IKE Life Time Value. It must be 30 - 43200.
% is over length. It must be 1 - 32.	
	^Parse error
	^Incomplete command
<b>Related Commands</b>	<pre> show ipsec show logging event-log vpn </pre>

## show ipsec

To check the IPsec VPN configuration and status on the router, use the **show ipsec** command.

### Synopsis

```
# show ipsec [{status |
               <ipsec-name>}]
```

<b>Option</b>	status	Specifies to display IPsec VPN connection status
<b>Description</b>	ipsec-name	Specifies to display the configuration of this IPsec VPN connection
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<pre> router # show ipsec Global Setting All Connection      : Disable NAT-T              : Disable VPN Log            : Disable Syslog             : Disable Trap               : Disable  Connection List State  Name      Remote Gateway  Local Subnet      Remote Subnet ----- Disable ipst    0.0.0.0         192.168.127.0 /24 </pre>	
<b>Error Messages</b>	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	ipsec	

## show logging event-log vpn

To check the VPN event logs on the router, use the **show logging event-log vpn** command.

### **Synopsis**

# **show logging event-log vpn** [severity <level-range>]

<b>Option</b>	severity	Specifies to display a specific range of severity levels
<b>Description</b>	level-range	Severity level ranges 0 to 7. Specifies a range of level. E.g. 1-1, 5-7, ...
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router # show logging event-log vpn VPN Log: 0 message lines logged, ----- Index Date Time Severity Event -----	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ipsec	

# L2TP Server

## I2tp

To specify or modify L2TP server function on the router, use the **I2tp** global configuration command. To disable L2TP server mode or remove the user, use no form of this command.

### Synopsis

```
(config)# I2tp {interface WAN local-ip <loc-ip> offer-ip <ip1> <ip2> |  
                user <username> password <pwd>}
```

```
(config)# no I2tp {interface WAN |  
                  user <username>}
```

<b>Option</b>	interface	Specifies WAN interface
<b>Description</b>	local-ip	Specifies IP address of the local subnet
	loc-ip	IP address of the local subnet
	offer-ip	Specifies offered IP ranges
	ip1	IP address 1 as a start of the range
	ip2	IP address 2 as an end of the range
	user	Specifies a user name for L2TP connection
	username	User name, 1 to 32 characters
	password	Specifies a user password for L2TP connection
	pwd	User password, 1 to 32 characters
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Configures WAN interface in advance is required to use this command.	
<b>Examples</b>	<p>L2TP over IPsec (Site to Site(Any)):</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> <li>• TN router: <ul style="list-style-type: none"> <li>- WAN: 10.10.10.254/24, VLAN ID=10, WAN interface</li> <li>- LAN20: 192.168.126.100/24, VLAN ID=20, interface used for internal network</li> <li>- Layer 3 filter policy: Accept source IP addresses: from 192.168.100.1 to 192.168.100.254</li> </ul> </li> <li>• PC-1 from WAN: <ul style="list-style-type: none"> <li>- IP: 10.10.10.160/24</li> <li>- Gateway: 10.10.10.254</li> </ul> </li> <li>• PC-2 on the internal network: <ul style="list-style-type: none"> <li>- IP: 192.168.126.50/24</li> <li>- Gateway: 192.168.126.100</li> </ul> </li> </ul> <p>Network topology:</p> <pre> graph LR     PC1[PC 1] --- WAN: 10.10.10.254/24  RouterA[Router A]     RouterA --- LAN20: 192.168.126.100/24  PC2[PC 2]     </pre> <p>Scenario:</p> <p>a) Router (A) enables L2TP server and offered IP ranges are from 192.168.100.1 to 192.168.100.20. The VPN user "vpnusr" and password "moxamoxa" is created.</p>	



- b) Router (A) configures IPsec related settings (such as pre-shared key: 12345678 ) with L2TP tunnel enabled.
- c) PC (1) acts as a L2TP client and gets offered IP 192.168.100.1 from Router (A).
- d) PC (1) can start a communication with PC (2) via the IP 192.168.100.1 but fails via the IP 10.10.10.160 because the layer 3 filter policy only accepts the source IP comes from 192.168.100.0/24.

**Commands:**

```

router(config)# ipsec all-connect
router(config)# ipsec L2TP-test
router(config-ipsec)# l2tp
router(config-ipsec)# interface WAN
router(config-ipsec)# startup-mode wait
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
router(config-ipsec-phase1)# ike-version ikev1
router(config-ipsec-phase1)# auth-mode psk 12345678
router(config-ipsec-phase1)# encryption aes256
router(config-ipsec-phase1)# hash sha256
router(config-ipsec-phase1)# dh-group 2048
router(config-ipsec-phase1)# life-time 43200
router(config-ipsec-phase1)# exit
router(config-ipsec)# phase2
router(config-ipsec-phase2)# encryption aes256
router(config-ipsec-phase2)# hash sha256
router(config-ipsec-phase2)# life-time 43200
router(config-ipsec-phase2)# exit
router(config-ipsec)# dpd-action clear
router(config-ipsec)# dpd-delay 30
router(config-ipsec)# dpd-timeout 120
router(config-ipsec)# exit
router(config)# l2tp interface WAN local-ip 192.168.100.254 offer-ip
192.168.100.1 192.168.100.20
router(config)# l2tp user vpnusr password moxamoxa
router(config)#

```

<b>Error Messages</b>	% is invalid WAN interface name
	% is over length. It must be 1 - 32.
	^Parse error
	^Incomplete command
<b>Related Commands</b>	show l2tp

## show l2tp

To check the L2TP server settings on the router, use the **show l2tp** command.

### **Synopsis**

# **show l2tp**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router # show l2tp WAN Server Setting L2TP Server Mode      : Disable Local IP               : 191.0.0.254 Offered IP Range      : 191.0.0.1 - 191.0.0.100  User Name/Password User Name              : luser1</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	l2tp

# OpenVPN

## ovpn

To enter OpenVPN Client configuration submode and configure OpenVPN settings.

### Synopsis

(config)# **ovpn**

<b>Option Description</b>	vpvn	Enter OpenVPN Client configuration submode.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	The configurations set under the submode should be applied via ovpn_apply command.	
<b>Examples</b>	Enter OpenVPN Client configuration submode (config)# ovpn	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ovpn_apply	

## enable/disable

To enable / disable OpenVPN Client connection, use the enable/disable commands.

### Synopsis

(config-ovpn)# { enable | disable }

<b>Option Description</b>	enable disable	Enable OpenVPN Client. Disable OpenVPN Client.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Not applied before ovpn_apply is executed.	
<b>Examples</b>	Enable OpenVPN Client (config-ovpn)# enable  Disable OpenVPN Client (config-ovpn)# disable	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ovpn_apply	

## description

To configure the description of OpenVPN Client profile use the **description** command.

### **Synopsis**

(config-ovpn)# **description** \$desc

<b>Option</b>	description	Configure the description of OpenVPN Client profile
<b>Description</b>	desc	The description of the profile.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Not applied before ovpn_apply is executed.	
<b>Examples</b>	Set description of OpenVPN Client to "OVPN-profile" (config-ovpn)# description OVPN-profile	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ovpn_apply	

## username

To set username of OpenVPN Client profile for authentication, use the **username** command.

### **Synopsis**

(config-ovpn)# **username** \$un

<b>Option</b>	username	Configure the username for authentication.
<b>Description</b>	un	The username to be set.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Not applied before ovpn_apply is executed.	
<b>Examples</b>	Set username of OpenVPN Client to "OVPN-username" (config-ovpn)# username OVPN-username	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ovpn_apply	

## password

To set the password of OpenVPN Client profile for authentication, use the **password** command.

### **Synopsis**

(config-ovpn)# **password** \$pwd

<b>Option</b>	password	Configure the password for authentication.
<b>Description</b>	pwd	The password to be set.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	Not applied before ovpn_apply is executed.	
<b>Examples</b>	Set password of OpenVPN Client to "OVPN-password" (config-ovpn)# password OVPN-password	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ovpn_apply	

## ovpn\_apply

To apply modified settings of OpenVPN Client, use the **ovpn\_apply** command.

### **Synopsis**

(config-ovpn)# **ovpn\_apply**

<b>Option</b>	ovpn_apply	Apply the modified OpenVPN Client configuration.
<b>Description</b>		
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Modify the description, username and password of the OpenVPN Client and apply the changes. (config-ovpn)# description OVPN-description (config-ovpn)# username OVPN-username (config-ovpn)# password OVPN-password (config-ovpn)# ovpn_apply	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	description \$desc username \$un password \$pwd	

## show ovpn

To show the information of OpenVPN Client, use the **show ovpn** command.

### Synopsis

# **show ovpn**

<b>Option</b>	show	Display system information.
<b>Description</b>	ovpn	Display OpenVPN Client information.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Show the information of OpenVPN client. router# show ovpn ----- OpenVPN : 5170808 OpenVPN Description : test123 OpenVPN Profile Name : client1.ovpn OpenVPN Username : username OpenVPN Password : OpenVPN Status : connected OpenVPN Server : 192.168.50.241:1194 OpenVPN Client : 10.8.0.6 OpenVPN Duration Time : 00:00:39 OpenVPN Last Connected Time: 2024-06-19T12:06:07+08:00 Open VPN Data Received/Sent : 250/0 -----	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	N/A	

## 4. Layer 2 Functions

---

This chapter describes the commands for the Layer 2 functions.

### Command Modes

Refer to the following table for the command modes.

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your router by using a normal user account and password.	#	Enter <b>exit</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"><li>• Change terminal settings.</li><li>• Perform basic tests.</li><li>• Display system information.</li></ul>
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter <b>exit</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"><li>• Change terminal settings.</li><li>• Perform basic tests.</li><li>• Display system information.</li><li>• Enter configuration mode.</li></ul>
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	(config)#	To exit to privileged EXEC mode, enter <b>exit</b> .	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example <b>interface ethernet</b> <mod-port> command and press enter	(config-if)#	To exit to global configuration mode, enter <b>exit</b> .	A sub-level to configure for example Ethernet port related arguments.

# Command Sets

## Port

### Port Settings

#### interface ethernet shutdown

To disable an Ethernet port, use the **interface ethernet** global configuration command and **shutdown** sub-level configuration command. To enable the Ethernet port, use the **no** form of this command.

##### Synopsis

```
(config)# interface ethernet <mod-port>
```

```
(config-if)# {exit |  
              shutdown }
```

```
(config-if)# no shutdown
```

<b>Option</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
<b>Description</b>	exit shutdown	Commit new settings and exit sub-level configuration mode. Disables the Ethernet port.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<ul style="list-style-type: none"><li>Disable PORT9: router# configure router(config)# interface ethernet 1/9 router(config-if)# shutdown router(config-if)# exit</li><li>Enable PORT9: router# configure router(config)# interface ethernet 1/9 router(config-if)# no shutdown router(config-if)# exit</li></ul>	
<b>Error Messages</b>	% Illegal parameter ^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces ethernet show interfaces trunk	



## interface ethernet name

To modify an Ethernet port's name, use the **interface ethernet** global configuration command and **name** sub-level configuration command set. To return to the default name, use the **no** form of this command.

### Synopsis

(config)# **interface ethernet** <mod-port>

(config-if)# **name** <token1> [<token2> [<token3> [<token4> [<token5> ]]]]

(config-if)# **no name**

<b>Option Description</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	name	Specifies the description of the Ethernet port.
	token1	A set of characters without a whitespace.
	token2	A set of characters without a whitespace.
	token3	A set of characters without a whitespace.
	token4	A set of characters without a whitespace.
	token5	A set of characters without a whitespace.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>The port's name is composed of a maximum of 5 tokens, with a whitespace positioned between each token.</li> <li>The format of the token must be a-z, A-Z, 0-9 or . - _ @ ! # \$ % ^ &amp; * ( ) . /</li> <li>Maximum length of port name including whitespaces is 127.</li> </ul>	
<b>Examples</b>	Set PORT9's name to "DCU 2". In this example, token1=DCU token2=2  <pre>router# configure router(config)# interface ethernet 1/9 router(config-if)# name DCU 2 router(config-if)# exit</pre>	
<b>Error Messages</b>	% Length of port name is too long	
	% Not in correct format	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show interfaces	
	ethernet	

## interface ethernet speed-duplex

To specify or modify an Ethernet port's speed-duplex, use the **interface ethernet** global configuration command and **speed-duplex** sub-level configuration command set. To return to the default setting, use the **no** form of this command.

### Synopsis

```
(config)# interface ethernet <mod-port>
(config-if)# speed-duplex {10M-Full |
                           10M-Half |
                           100M-Full |
                           100M-Half |
                           Auto }
```

```
(config-if)# no speed-duplex
```

<b>Option</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
<b>Description</b>	speed-duplex	Specifies speed duplex mode
	10M-Full	Fixed speed duplex mode: 10M-Full
	10M-Half	Fixed speed duplex mode: 10M-Half
	100M-Full	Fixed speed duplex mode: 100M-Full
	100M-Half	Fixed speed duplex mode: 100M-Half
	Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices.
<b>Defaults</b>	Auto.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set PORT9's speed duplex to 100M-Full: router# configure router(config)# interface ethernet 1/9 router(config-if)# speed-duplex 100M-Full router(config-if)# exit	
<b>Error Messages</b>	% Illegal parameter	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show interfaces ethernet	

## interface ethernet flowcontrol

To specify or modify an Ethernet port's flowcontrol, use the **interface ethernet** global configuration command and **flowcontrol** sub-level configuration command set. To return to the default setting, use the **no** form of this command.

### **Synopsis**

(config)# **interface ethernet** <mod-port>

(config-if)# **flowcontrol**

(config-if)# **no flowcontrol**

<b>Option</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
<b>Description</b>	flowcontrol	Enables flow control for this port when the port's Speed is set to Auto.
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	Set speed-duplex to Auto before enabling flow control.	
<b>Examples</b>	Enable PORT10's flow control: router# configure router(config)# interface ethernet 1/10 router(config-if)# speed-duplex Auto router(config-if)# flowcontrol router(config-if)# exit	
<b>Error Messages</b>	% Illegal parameter	
	% Force speed can not be set flow control!!	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show interfaces ethernet	

## interface ethernet media

To specify or modify an Ethernet port's medium type, use the **interface ethernet** global configuration command and **media** sub-level configuration command set. To return to the default setting, use the **no** form of this command.

### Synopsis

```
(config)# interface ethernet <mod-port>
(config-if)# media cable-mode {mdi |
                               mdix |
                               auto}
```

```
(config-if)# no media cable-mode
```

<b>Option Description</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	media	Specifies the type for medium detection.
	mdi	Specifies MDI
	mdix	Specifies MDIX
	auto	Specifies auto-negotiation
	cable-mode	Returns to default setting
<b>Defaults</b>	Auto	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Set PORT9's medium detection type to MDI: router# configure router(config)# interface ethernet 1/9 router(config-if)# media cable-mode mdi router(config-if)# exit	
<b>Error Messages</b>	% Illegal parameter	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show interfaces ethernet	

## interface ethernet poe

To specify a PoE port's settings including power output mode, PD Failure Check and Scheduling, use the **interface ethernet** global configuration command and **poe** sub-level configuration command set. To return to the default setting, use the **no** form of this command.

### Synopsis

```
(config)# interface ethernet <mod-port>
(config-if)# poe {enable |
    auto |
    force budget <watt> |
    high-power |
    legacy-pd-detect |
    power-priority <priority> |
    pdfail [{ip <pd-ip> |
        periods <sec> |
        no-response-timeout <times> |
        no-response-action {no-action |
            reboot-pd |
            power-off-pd}}]} |
    scheduling <rule>}
(config-if)# no poe [{legacy-pd-detect |
    power-priority |
    pdfail [{ip |
        periods |
        no-response-timeout |
        no-response-action}]} |
    scheduling}]
```

<b>Option Description</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	poe	Specifies PoE function
	enable	Specifies to enable PoE for the port
	auto	Specifies to set the PoE output mode to Auto
	force budget	Specifies to set the PoE output mode to Force
	watt	Integer for Watt. This value should be between 1 and 36.
	high-power	Specifies to set the PoE output mode to High-Power
	legacy-pd-detect	Specifies to enable or disable Legacy PD Detection
	power-priority	Specifies the priority of the port to use with the Auto Power Cutting feature.
	priority	Specifies an integer value for priority: {Critical(0)   High(1)   Low(2)}
	pdfail	Specifies to enable or disable the PD Failure Check feature
	ip	Specifies IP address for PD failure detection
	pd-ip	Specifies the PD's IP address
	periods	Specifies how often PD failure checks will run
	sec	Specifies the duration of the failure check. Ranges from 5 to 300.
	no-response-timeout	Specifies the maximum number of IP checking cycles to try before determining a PD is not responding.
	times	Specifies the number of cycles. Ranges from 1 to 10.
	no-response-action	Specifies what action to take when a PD failure is detected
	no-action	Specifies to takes no action
	reboot-pd	Specifies to reboot the PD
power-off-pd	Specifies to power off the PD	
scheduling	Specifies the use of scheduling rules	
rule	The name of the preconfigured scheduling rule	
<b>Defaults</b>	N/A	
<b>Command</b>	Global configuration, sub-level configuration	

<b>Modes</b>	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>To proceed with PD Failure Check or Scheduling mentioned in this instruction, it's necessary to have PoE power output enabled beforehand.</li> <li>To proceed with Scheduling mentioned in this instruction, it's necessary to create a scheduling rule beforehand.</li> </ul>
<b>Examples</b>	<ul style="list-style-type: none"> <li>Specifies Output mode to Force and allocate 30 watts power for PORT4:  <pre>router# configure router(config)# interface ethernet 1/4 router(config-if)# poe enable router(config-if)# poe force budget 30 router(config-if)# exit</pre> </li> <li>Enable PD Failure Check and reboot PD after 5 cycles attempt (20 seconds per cycle) without success for PORT4:  <pre>router# configure router(config)# interface ethernet 1/4 router(config-if)# poe pdfail router(config-if)# poe pdfail ip 192.168.127.100 router(config-if)# poe pdfail periods 20 router(config-if)# poe pdfail no-response-timeout 5 router(config-if)# poe pdfail no-response-action reboot-pd router(config-if)# exit</pre> </li> <li>Apply schedule rule "rule-example" for PORT4:  <pre>router# configure router(config)# interface ethernet 1/4 router(config-if)# poe scheduling rule-example router(config-if)# exit</pre> </li> </ul>
<b>Error Messages</b>	<pre>% Illegal parameter % POE port Watt should be between 1 and 36 % Power priority should be between 0 and 2. % Invalid IP Address. % Periods should be between 5 and 300. % Cycles should be between 1 and 10. % Invalid rule name. ^Parse error ^Incomplete command</pre>
<b>Related Commands</b>	<pre>show interfaces ethernet poe system poe scheduling</pre>

## VLAN port settings: interface ethernet switchport

To specify or modify VLAN port settings of an Ethernet port, use the **interface ethernet** global configuration command and **switchport** sub-level configuration command sets. To return to the default VLAN setting of the Ethernet port, use the **no** form of this command.

### Synopsis

```
(config)# interface ethernet <mod-port>
(config-if)# switchport {access vlan <vlan-id> |
                        trunk {fixed vlan {add | remove} <vlan-ids> |
                                native vlan <vlan-id>} |
                        hybrid {fixed vlan {add | remove} <vlan-ids> {tag | untag} |
                                native vlan <vlan-id>}
```

```
(config-if)# no switchport {access vlan |
                              trunk {fixed vlan |
                                        native vlan} |
                              hybrid {fixed vlan {tag | untag} |
                                        native vlan}}
```

<b>Option</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
<b>Description</b>	switchport	Specifies VLAN types
	access vlan	Specifies VLAN type: Access. Connects single devices without tags.
	vlan-id	Ranges from 1 to 4094.
	trunk	Specifies VLAN type: Trunk. Connects another 802.1Q VLAN aware switch.
	fixed vlan	Specifies other VLAN ID for tagged devices that connect to the port.
	vlan-ids	Ranges from 1 to 4094. Use commas to separate different VLAN IDs.
	add	Specifies to add tagged VLAN.
	remove	Specifies to remove tagged VLAN.
	tag	Specifies tagged VLAN IDs
	untag	Specifies untagged VLAN IDs
	native vlan	Specifies the default VLAN ID for untagged devices that connect to the port
	hybrid	Specifies VLAN type: Hybrid. Connects another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.
<b>Defaults</b>	<ul style="list-style-type: none"> <li>• Default native vlan is 1.</li> <li>• Default access vlan is 1.</li> </ul>	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command</li> <li>• Make sure the VLAN ID is created in advance before using it.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>• Set access VLAN ID (10) to PORT7:  <pre>router# configure router(config)# interface ethernet 1/7 router(config-if)# switchport access vlan 10 router(config-if)# exit</pre> </li> <li>• For Trunk-group 2, change port type from "Access" to "Trunk" and return access VLAN ID to default value 1.  <pre>router# configure router(config)# interface trunk 2 router(config-if)# no switchport trunk native vlan router(config-if)# exit</pre> </li> <li>• For Trunk-group 2, add a tagged VLAN 5 when trunk type is specified.  <pre>router# configure router(config)# interface trunk 2 router(config-if)# switchport trunk fixed vlan add 5 router(config-if)# exit</pre> </li> </ul>	

	<ul style="list-style-type: none"> <li>For Trunk-group 2, remove all tagged VLAN when trunk type is specified.  <pre>router# configure router(config)# interface trunk 2 router(config-if)# no switchport trunk fixed vlan router(config-if)# exit</pre> </li> </ul>
<b>Error Messages</b>	% VLAN id is out of range!
	vlan id does not exist!!
	^Parse error ^Incomplete command
<b>Related Commands</b>	vlan create show interfaces ethernet

## show interfaces ethernet

To check the status of the interfaces, use the **show interfaces ethernet** command.

### Synopsis

# **show interfaces ethernet** [<mod-port> [**config** | **rate-limit** | **counters**]]

<b>Option Description</b>	mod-port	Port ID or list. Ex. 1/1,2,3,2/1-3,5,...																																																																								
	config	Displays port general settings including media type, description, speed, etc for the specified port.																																																																								
	rate-limit	Displays rate-limit settings for the specified port.																																																																								
	counters	Displays packet counters including TX, RX for the specified port.																																																																								
<b>Defaults</b>	N/A																																																																									
<b>Command Modes</b>	Privileged EXEC / User EXEC																																																																									
<b>Usage Guidelines</b>	N/A																																																																									
<b>Examples</b>	<ul style="list-style-type: none"> <li>Display overall port settings and status.  <pre>router# show interfaces ethernet</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>Link</th> <th>Type</th> <th>Description</th> <th>Speed</th> <th>FDX</th> <th>Flow Ctrl</th> <th>MDI/MDIX</th> </tr> </thead> <tbody> <tr> <td>1/1</td> <td>Down</td> <td>1000TX</td> <td></td> <td>--</td> <td>--</td> <td></td> <td>--</td> </tr> <tr> <td>1/2</td> <td>Up</td> <td>1000TX</td> <td>main port</td> <td>100M-Full</td> <td>Off</td> <td></td> <td>MDI</td> </tr> <tr> <td>1/3</td> <td>Disable</td> <td>1000TX</td> <td></td> <td>--</td> <td>--</td> <td></td> <td>--</td> </tr> <tr> <td>1/4</td> <td>Disable</td> <td>1000TX</td> <td></td> <td>--</td> <td>--</td> <td></td> <td>--</td> </tr> <tr> <td>1/5</td> <td>Down</td> <td>1000TX</td> <td>main port 5</td> <td>--</td> <td>--</td> <td></td> <td>--</td> </tr> <tr> <td>1/6</td> <td>Down</td> <td>1000TX</td> <td></td> <td>--</td> <td>--</td> <td></td> <td>--</td> </tr> <tr> <td>1/7</td> <td>Down</td> <td>1000TX</td> <td></td> <td>--</td> <td>--</td> <td></td> <td>--</td> </tr> <tr> <td>1/8</td> <td>Down</td> <td>1000TX</td> <td></td> <td>--</td> <td>--</td> <td></td> <td>--</td> </tr> </tbody> </table> </li> </ul>		Port	Link	Type	Description	Speed	FDX	Flow Ctrl	MDI/MDIX	1/1	Down	1000TX		--	--		--	1/2	Up	1000TX	main port	100M-Full	Off		MDI	1/3	Disable	1000TX		--	--		--	1/4	Disable	1000TX		--	--		--	1/5	Down	1000TX	main port 5	--	--		--	1/6	Down	1000TX		--	--		--	1/7	Down	1000TX		--	--		--	1/8	Down	1000TX		--	--		--
	Port	Link	Type	Description	Speed	FDX	Flow Ctrl	MDI/MDIX																																																																		
	1/1	Down	1000TX		--	--		--																																																																		
	1/2	Up	1000TX	main port	100M-Full	Off		MDI																																																																		
	1/3	Disable	1000TX		--	--		--																																																																		
1/4	Disable	1000TX		--	--		--																																																																			
1/5	Down	1000TX	main port 5	--	--		--																																																																			
1/6	Down	1000TX		--	--		--																																																																			
1/7	Down	1000TX		--	--		--																																																																			
1/8	Down	1000TX		--	--		--																																																																			
<ul style="list-style-type: none"> <li>Display general settings for port 2.  <pre>router# show interfaces ethernet 1/2 config</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>Enable</th> <th>Type</th> <th>Description</th> <th>Speed</th> <th>FDX</th> <th>Flow Ctrl</th> <th>MDI/MDIX</th> </tr> </thead> <tbody> <tr> <td>1/2</td> <td>Yes</td> <td>100TX</td> <td>100TX</td> <td>Auto</td> <td>Disable</td> <td></td> <td>Auto</td> </tr> </tbody> </table> </li> </ul>		Port	Enable	Type	Description	Speed	FDX	Flow Ctrl	MDI/MDIX	1/2	Yes	100TX	100TX	Auto	Disable		Auto																																																									
Port	Enable	Type	Description	Speed	FDX	Flow Ctrl	MDI/MDIX																																																																			
1/2	Yes	100TX	100TX	Auto	Disable		Auto																																																																			
<ul style="list-style-type: none"> <li>Display rate-limit settings for port 2.  <pre>router# # show interfaces ethernet 1/2 rate-limit</pre> <pre>Port 1/2:   Ingress Limit Rate: Not Limited   Egress Limit Rate : Not Limited</pre> </li> </ul>																																																																										
<ul style="list-style-type: none"> <li>Display packet counter information for port 2.  <pre>router# show interfaces ethernet 1/2 counters</pre> <pre>Port 1/2 (last sample time: 604613 secs ago) - TX -   Unicast Packets      : 421628          +421628   Multicast Packets    : 20056           +20056</pre> </li> </ul>																																																																										



	Broadcast Packets	: 107	+107
	Collision Packets	: 0	+0
	- RX -		
	Unicast Packets	: 365440	+365440
	Multicast Packets	: 270530	+270530
	Broadcast Packets	: 36674	+36674
	Pause Packets	: 0	+0
	- Error -		
	TX Late	: 0	+0
	TX Excessive	: 0	+0
	RX CRC error	: 0	+0
	RX Discard	: 0	+0
	RX Undersize	: 0	+0
	RX Fragments	: 0	+0
	RX Oversize	: 0	+0
	RX Jabber	: 0	+0
<b>Error Messages</b>	^Parse error		
	^Incomplete command		
<b>Related Commands</b>	interface ethernet shutdown interface ethernet name interface ethernet speed-duplex interface ethernet flowcontrol interface ethernet media		

## Link Aggregation

In order to create and configure trunked ports, two CLI command sets **interface trunk** and **interface ethernet** are required for this purpose.

### interface ethernet trunk-group

To add or remove Ethernet ports to the trunked port, use the **interface ethernet** global configuration command and **trunk-group** sub-level configuration command set. To remove the Ethernet port from the trunk group, use the **no** form of this command.

#### Synopsis

(config)# **interface ethernet** <mod-port>

(config-if)# **trunk-group** <index>

(config-if)# **no trunk-group**

<b>Option Description</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	trunk-group	Specifies the trunk-group to be added/removed
	index	Trunk group's index; starting from 1. Maximum number of trunk groups differs among different models.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Configure PORT11 and PORT12 to be members of trunk group 1: router# configure router(config)# interface ethernet 1/11 router(config-if)# trunk-group 1 router(config-if)# exit router(config)# interface ethernet 1/12 router(config-if)# trunk-group 1 router(config-if)# exit	
<b>Error Messages</b>	% Trunk ID is only allowed from 1 to 4	
	^Parse error	
	^Incomplete command	

<b>Related Commands</b>	interface trunk show interfaces trunk
-------------------------	------------------------------------------

## interface trunk shutdown

To disable a trunked port, use the **interface trunk** global configuration command and **shutdown** sub-level configuration command. To enable the trunked port, use the **no** form of this command.

### Synopsis

```
(config)# interface trunk <trunk-id>
```

```
(config-if)# {exit |  
              shutdown }
```

```
(config-if)# no shutdown
```

<b>Option Description</b>	trunk-id	Trunk group ID. Maximum number of trunk groups differs among different models.
	exit	Commit new settings and exit sub-level configuration mode.
	shutdown	Disables the trunked port.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command.	
<b>Examples</b>	Enable trunk group 1 and set VLAN ID (1) to this trunk group: router# configure router(config)# interface trunk 1 router(config-if)# no shutdown router(config-if)# switchport access vlan 1 router(config-if)# exit	
<b>Error Messages</b>	% There is no member in Trunk	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	interface ethernet show interfaces trunk	

## interface trunk name

To modify a trunked port's name, use the **interface trunk** global configuration command and **name** sub-level configuration command set. To return to the default name, use the **no** form of this command.

### Synopsis

```
(config)# interface trunk <trunk-id>
```

```
(config-if)# name <token1> [<token2> [<token3> [<token4> [<token5>]]]]
```

```
(config-if)# no name
```

<b>Option Description</b>	trunk-id	Trunk group ID. Maximum number of trunk groups differs among different models.
	name	Specifies the description of the trunked port.
	token1	A set of characters without a whitespace.
	token2	A set of characters without a whitespace.
	token3	A set of characters without a whitespace.
	token4	A set of characters without a whitespace.
token5	A set of characters without a whitespace.	
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• The trunk port name is composed of a maximum of 5 tokens, with a whitespace positioned between each token.</li><li>• The format of the token must be a-z, A-Z, 0-9 or . - _ @ ! # \$ % ^ &amp; * ( ) . /</li><li>• Maximum length of trunk port's name including whitespaces is 127.</li><li>• Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command</li></ul>	
<b>Examples</b>	Set the name of trunk group 1 as "NewTrk". In this example, token1=NewTrk  router# configure router(config)# interface trunk 1 router(config-if)# name NewTrk router(config-if)# exit	
<b>Error Messages</b>	% Length of port name is too long.	
	% Not in correct format	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	interface ethernet show interfaces trunk	

## VLAN port settings: interface trunk switchport

To specify or modify VLAN port settings of a trunked port, use the **interface trunk** global configuration command and **switchport** sub-level configuration command sets. To return to the default VLAN setting of the trunked port, use the **no** form of this command.

### Synopsis

```
(config)# interface trunk <trunk-id>
```

```
(config-if)# switchport {access vlan <vlan-id> |  
                  trunk {fixed vlan {add | remove} <vlan-ids> |  
                          native vlan <vlan-id>}} |  
                  hybrid {fixed vlan {add | remove} <vlan-ids> {tag | untag} |  
                          native vlan <vlan-id>}}
```

```
(config-if)# no switchport {access vlan |  
                  trunk {fixed vlan |  
                          native vlan}} |  
                  hybrid {fixed vlan {tag | untag} |  
                          native vlan}}
```

<b>Option Description</b>	trunk-id	Trunk group ID. Maximum number of trunk groups differs among different models.
	switchport	Specifies VLAN types
	access vlan	Specifies VLAN type: Access. Connects single devices without tags.
	vlan-id	Ranges from 1 to 4094.
	trunk	Specifies VLAN type: Trunk. Connects another 802.1Q VLAN aware switch.
	fixed vlan	Specifies other VLAN ID for tagged devices that connect to the port.
	vlan-ids	Ranges from 1 to 4094. Use commas to separate different VLAN IDs.
	add	Specifies to add tagged VLAN.
	remove	Specifies to remove tagged VLAN.
	tag	Specifies tagged VLAN IDs
	untag	Specifies untagged VLAN IDs
	native vlan	Specifies the default VLAN ID for untagged devices that connect to the port
	hybrid	Specifies VLAN type: Hybrid. Connects another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.
	<b>Defaults</b>	<ul style="list-style-type: none"> <li>• Default native vlan is 1.</li> <li>• Default access vlan is 1.</li> </ul>
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>• Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command.</li> <li>• Make sure the VLAN ID is created in advance before using it.</li> </ul>	
<b>Examples</b>	<ul style="list-style-type: none"> <li>• For Trunk-group 2, change port type from "Access" to "Trunk" and return access VLAN ID to default value 1.  <pre>router# configure router(config)# interface trunk 2 router(config-if)# no switchport trunk native vlan router(config-if)# exit router(config)# exit</pre> </li> <li>• For Trunk-group 2, add a tagged VLAN 5 when trunk type is specified.  <pre>router# configure router(config)# interface trunk 2 router(config-if)# switchport trunk fixed vlan add 5 router(config-if)# exit router(config)# exit</pre> </li> <li>• For Trunk-group 2, remove all tagged VLAN when trunk type is specified.  <pre>router# configure router(config)# interface trunk 2 router(config-if)# no switchport trunk fixed vlan router(config-if)# exit router(config)# exit</pre> </li> </ul>	
<b>Error Messages</b>	% VLAN id is out of range!	
	vlan id does not exist!!	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	interface ethernet show interfaces trunk	

## show interfaces trunk

To check the status of the trunk ports, use the **show interfaces trunk** command.

### Synopsis

# **show interfaces trunk** [<trunk-id> [counters]]

<b>Option</b>	trunk-id	ID or a common separated ID list of the trunk port
<b>Description</b>	counters	Displays packet counters including TX, RX for the specified trunk port
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Display overall trunk port settings.  <pre>router# show interfaces trunk Trk#  Type  Enable Description                               Speed -----  - 1      Static Yes                               1G-Full</pre> </li> <li>Display status for trunk port 1.  <pre>router# show interfaces trunk 1  Trunk-1   Name :   Type : Static   Member  Status   -----  -   1/7      Success   1/8      Fail</pre> </li> <li>Display packet counter information for trunk port 1.  <pre>router# show interfaces trunk 1 counters Trk1 (last sample time: 605221 secs ago) - TX -   Unicast Packets      : 5733      +5733   Multicast Packets    : 1331      +1331   Broadcast Packets    : 102       +102   Collision Packets    : 0          +0 - RX -   Unicast Packets      : 6756      +6756   Multicast Packets    : 81         +81   Broadcast Packets    : 54         +54   Pause Packets        : 0          +0 - Error -   TX Late              : 0          +0   TX Excessive         : 0          +0   RX CRC error         : 0          +0   RX Discard           : 0          +0   RX Undersize         : 0          +0   RX Fragments         : 0          +0   RX Oversize          : 0          +0   RX Jabber            : 0          +0</pre> </li> </ul>	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	interface trunk name interface trunk switchport interface ethernet trunk-group	

## PoE

### poe system

Use the **poe system** global configuration commands on the router for configuring PoE related settings. Use the **no** form of this command to disable PoE settings.

#### Synopsis

```
(config)# poe system {enable |  
                    power-budget budget <value> |  
                    threshold {power <value> |  
                                cutoff}}
```

```
(config)# no poe system [threshold {power | cutoff}]
```

<b>Option</b>	enable	Specifies to enable PoE power output
<b>Description</b>	power-budget budget	Specifies the PoE power budget (if applicable).
	threshold	Specifies the power budget threshold
	power	Specifies the power threshold value
	value	Integer (Watt)
	cutoff	Specifies to enable or disable the Auto Power Cutt-off function
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>To proceed with threshold or cutoff settings, it's necessary to have PoE power output enabled beforehand.</li><li>When Auto Power Cutt-off is disabled, the router will calculate power budget based on the Power Allocation settings of all ports.</li><li>Adjustability of the PoE power budget varies across different models.</li></ul>	
<b>Examples</b>	Enable Auto Power Cutt-off and set the power threshold to 50 watts: router# configure router(config)# poe system enable router(config)# poe system threshold cutoff router(config)# poe system threshold power 50 router(config)# exit	
<b>Error Messages</b>	% Power threshold should be between 30 and 95. % System power budget should be between 95 and 95. ^Parse error ^Incomplete command	
<b>Related Commands</b>	poe scheduling interface ethernet poe show poe	

### poe scheduling

Use the **poe scheduling** global configuration commands on the router for scheduling availability of PoE for each PoE port. Use the **no** form of this command to disable PoE settings.

#### Synopsis

```
(config)# poe scheduling <rule-name> {<year> <month> <day> <start-hour> <start-min> <end-hour>  
<end-min> |
```

```
        activate |  
        repeat <schedule-day>}
```

```
(config)# no poe scheduling {<rule-name> |  
                             activate |  
                             repeat <schedule-day>}
```

<b>Option</b>	rule-name	Specifies a name for the scheduling rule. Max. length is 63.
<b>Description</b>	year	Specifies start date (year)

	month	Specifies start date (month), ranges from 1 to 12.
	day	Specifies start date (day), ranges from 1 to 31.
	start-hour	Specifies start hour, ranges from 0 to 23.
	start-min	Specifies start minute, ranges from 0 to 59.
	end-hour	Specifies end hour, ranges from 0 to 23.
	end-min	Specifies end minute, ranges from 0 to 59.
	activate	Specifies to enable / disable the rule
	repeat	Specifies to repeat execution of the rule on a daily or weekly basis.
	schedule-day	Specifies one of below strings for scheduled day: { daily   weekday   weekend   sunday   monday   tuesday   wednesday   thursday   friday   Saturday } For multiple days, execute this command multiple times.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	To proceed with scheduling settings, it's necessary to have PoE power output enabled beforehand.	
<b>Examples</b>	<ul style="list-style-type: none"> <li>Create a rule-example to schedule 8 a.m. to 6 p.m. on weekdays:  <pre>router# configure router(config)# poe scheduling rule-example 2023 8 10 8 0 18 0 router(config)# poe scheduling rule-example repeat weekday router(config)# poe scheduling rule-example activate router(config)# exit</pre> </li> <li>Delete the rule "rule-example":  <pre>router# configure router(config)# no poe scheduling rule-example router(config)# exit</pre> </li> </ul>	
<b>Error Messages</b>	% The rule name is too long (max. 63).	
	% The year of start date should begin since 1900.	
	% The month of start date should be between 1 and 12.	
	% The day of start date should be between 1 and 31.	
	% The hour of start time should be between 0 and 23.	
	% The minute of start time should be between 0 and 59.	
	% The hour of end time should be between 0 and 23.	
	% The minute of end time should be between 0 and 59.	
	% Invalid rule name.	
	% Invalid repeat day.	
	% Schedule is conflict.	
	^Parse error	
^Incomplete command		
<b>Related Commands</b>	poe system interface ethernet poe show poe	

## show poe

To check the PoE port status on the router, use the **show poe** command.

### Synopsis

# **show poe**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	Output only available on PoE models.

<b>Examples</b>	<pre> router# show poe PoE system status:   PoE power output      : Enable   PoE power budget      : 95 Watts   PoE power threshold   : 95 Watts   PoE threahold cutoff  : Cutoff   Sum of allocated power : 16 Watts   Sum of measured power  : 4 Watts   PSE input voltage (VEE): 54 Volts </pre>
	<pre> +-----+  Power      Consumption Voltage Current PD Failure PD Status    Port Status Output Class   (W)      (V)      (mA)  Check  Description  +-----+    1 Enable Off   N/A      N/A      N/A      N/A  Disable  NIC    2 Enable Off   N/A      N/A      N/A      N/A  Disable  NIC    3 Enable Off   N/A      N/A      N/A      N/A  Disable  NIC    4 Enable On    0        4        55       58  Disable  Powered    5 Enable Off   N/A      N/A      N/A      N/A  Disable  Not Present    6 Enable Off   N/A      N/A      N/A      N/A  Disable  Not Present    7 Enable Off   N/A      N/A      N/A      N/A  Disable  Not Present    8 Enable Off   N/A      N/A      N/A      N/A  Disable  NIC   G3 Enable Off   N/A      N/A      N/A      N/A  Disable  Not Present   G4 Enable Off   N/A      N/A      N/A      N/A  Disable  Not Present   G7 Enable Off   N/A      N/A      N/A      N/A  Disable  Not Present   G8 Enable Off   N/A      N/A      N/A      N/A  Disable  Not Present </pre>
<b>Error Messages</b>	% Not support POE on this switch
	^Parse error
	^Incomplete command
<b>Related Commands</b>	N/A



# Network Redundancy

## Layer 2 Redundant Protocols

### redundancy mode

Use the **redundancy mode** global configuration command on the switch to change the redundancy protocol mode.

#### Synopsis

```
(config)# redundancy mode {rstp |  
                           turbo-ring-v2}
```

<b>Option</b>	rstp	Rapid Spanning Tree
<b>Description</b>	turbo-ring-v2	Turbo ring version 2
<b>Defaults</b>	The default redundancy protocol mode is RSTP.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	* An illustrative example can be found in the command " <b>redundancy spanning-tree</b> " and " <b>redundancy turbo-ring-v2</b> ".	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show redundancy mode	

### show redundancy mode

To check the redundancy mode on the router, use the **show redundancy mode** command.

#### Synopsis

```
# show redundancy mode
```

<b>Option</b>	N/A	
<b>Description</b>		
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# show redundancy mode Current redundancy mode : Turbo Ring V2	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	redundancy mode	

## RSTP

### redundancy spanning-tree

To specify or modify redundant protocols (RSTP) on the router, use the **redundancy spanning-tree** global configuration command and related sub-level configuration command sets. To return RSTP to default settings, use the **no** form of this command.

#### Synopsis

```
(config)# redundancy
```

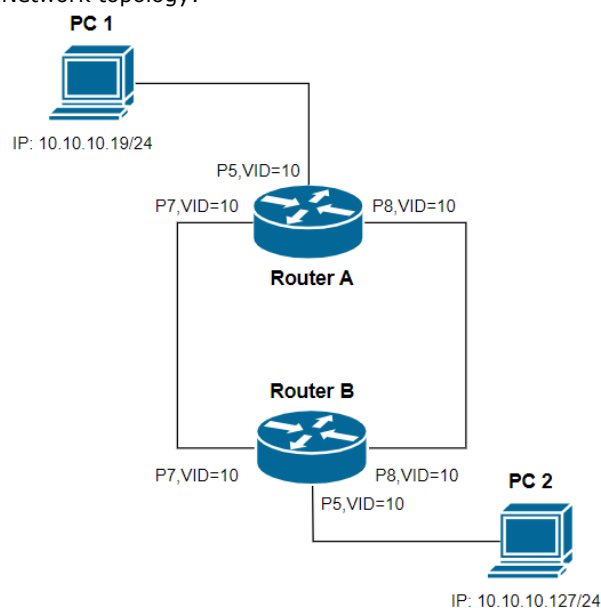
```
(config-rdnt)# {exit |
```

```
    spanning-tree {priority <prio> |  
                    hello-time <hello-second> |  
                    forward-delay <delay-second> |  
                    max-age <age-second>}}
```

```
(config-rdnt)# no spanning-tree {priority |  
                                     hello-time |  
                                     forward-delay |  
                                     max-age}
```

<b>Option</b>	exit	Commit new settings and exit sub-level configuration mode
<b>Description</b>	spanning-tree	Specifies spanning-tree settings
	priority	Specifies this device's bridge priority
	prio	Ranges from 0 to 61440, and must be the multiples of 4096
	hello-time	Specifies Hello time
	hello-second	Ranges from 1 to 2 seconds
	forward-delay	Specifies the amount of time this device waits before checking to see if it should change to a different state.
	delay-second	Ranges from 4 to 30 seconds
	max-age	Specifies spanning tree max age
	age-second	Ranges from 6 to 40 seconds
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• <math>2 * (\text{hello-time} + 1.0 \text{ sec}) \leq \text{max-age} \leq 2 * (\text{forward-delay} - 1.0 \text{ sec})</math></li><li>• Enable spanning-tree feature in the command "<b>interface ethernet</b>" to let RSTP take effect.</li></ul>	
<b>Examples</b>	Specify RSTP on two routers:  Prerequisites: <ul style="list-style-type: none"><li>• TN router A:<ul style="list-style-type: none"><li>- P5: VLAN ID=10</li><li>- RSTP ports: P7 and P8</li></ul></li><li>• TN router B:<ul style="list-style-type: none"><li>- P5: VLAN ID=10</li><li>- RSTP ports: P7 and P8</li></ul></li><li>• PC-1:<ul style="list-style-type: none"><li>- IP: 10.10.10.19/24</li></ul></li><li>• PC-2 :<ul style="list-style-type: none"><li>- IP: 10.10.10.127/24</li></ul></li></ul>	

#### Network topology:



#### Scenario:

- Router (A) and Router (B) enable RSTP to provide redundancy for communication. Router (B) could be other brand which does not support Moxa proprietary Turbo Ring V2 redundancy protocol.
- PC (1) and PC (2) can communicate with each other via Router (A) and Router (B).
- This feature provides a functionality of network redundancy.

#### Commands:

##### On Router A:

```
router(config)# redundancy mode rstp
router(config)# redundancy
router(config-rdnt)# spanning-tree priority 32768
router(config-rdnt)# spanning-tree forward-delay 15
router(config-rdnt)# spanning-tree max-age 20
router(config-rdnt)# spanning-tree hello-time 2
router(config-rdnt)# exit
router(config)# interface ethernet 1/7
router(config-if)# no shutdown
router(config-if)# speed-duplex Auto
router(config-if)# no flowcontrol
router(config-if)# media cable-mode auto
router(config-if)# switchport access vlan 10
router(config-if)# spanning-tree
router(config-if)# exit
router(config)# interface ethernet 1/8
router(config-if)# no shutdown
router(config-if)# speed-duplex Auto
router(config-if)# no flowcontrol
router(config-if)# media cable-mode auto
router(config-if)# switchport access vlan 10
router(config-if)# spanning-tree
router(config-if)# exit
```

#### Error Messages

The BPDU forward delay time must be in the range from 4 to 30 secs  
The formula must be obeyed:  
 $2 \times (\text{Hello Time} + 1 \text{ sec}) \leq \text{Max age} \leq 2 \times (\text{Forward Delay} - 1 \text{ sec})$

	BPDU hello time must be in the range from 1 to 2 secs
	The bridge priority must be in the range from 0 to 61440
	The bridge priority must be the multiples of 4096
	^Parse error
	^Incomplete command
<b>Related Commands</b>	spanning-tree forward-delay spanning-tree max-age show redundancy spanning-tree

## interface ethernet spanning-tree

To specify or modify RSTP function, use the **interface ethernet** global configuration command and **spanning-tree** sub-level configuration command set. To return to default settings, use the **no** form of this command.

### Synopsis

```
(config)# interface ethernet <mod-port>
(config-if)# spanning-tree [{edge-port |
priority <pri-value>|
cost <cost-value>}]

(config-if)# no spanning-tree [{edge-port |
priority |
cost }]
```

<b>Option Description</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	spanning-tree	Enables spanning tree function
	edge-port	Configures as edge port.
	priority	Specifies port priority
	pri-value	Ranges from 0 to 240, and must be multiples of 16
	cost	Specifies port cost
	cost-value	Ranges from 1 to 200000000.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A.	
<b>Examples</b>	* An illustrative example can be found in the command " <b>redundancy spanning-tree</b> ".	
<b>Error Messages</b>	% Illegal parameter	
	% Cost value must be in the range 1 ~ 200000000	
	% Priority value must be multiples of 16 and not exceed 240	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	show redundancy spanning-tree	

## show redundancy spanning-tree

Use the **show redundancy spanning-tree** user EXEC command to display the spanning-tree state information.

### **Synopsis**

# **show redundancy spanning-tree**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show redundant spanning-tree  Spanning tree status : Enabled Role                  : Root Bridge priority       : 32768 Hello time            : 2 sec Forwarding delay      : 30 sec Max age time          : 20 sec  Int#  Enable   Edge Port   Prio   Cost       Status 1/1   Disabled  Auto       128    200000    --- 1/2   Disabled  Auto       128    200000    --- 1/3   Disabled  Auto       128    200000    --- 1/4   Disabled  Auto       128    200000    --- 1/5   Disabled  Auto       128    200000    --- 1/6   Disabled  Auto       128    200000    --- 1/7   Enabled   False      128    200000    Forwarding 1/8   Enabled   False      128    200000    Link Down</pre>
<b>Error messages</b>	<pre>^Parse error ^Incomplete command</pre>
<b>Related Commands</b>	<pre>spanning-tree forward-delay spanning-tree hello-time spanning-tree max-age spanning-tree priority spanning-tree spanning-tree cost spanning-tree edge-port spanning-tree priority</pre>

## Turbo Ring V2

### redundancy turbo-ring-v2

To specify or modify redundant protocol (Turbo Ring V2) on the router, use the **redundancy turbo-ring-v2** global configuration command and related sub-level configuration command sets. To disable Turbo Ring V2, use the **no** form of this command.

#### Synopsis

```
(config)# redundancy
```

```
(config-rdnt)# {exit |
```

```
    turbo-ring-v2 {<ring-id> {master |
```

```
        primary interface <pri-if> secondary interface <sec-if>} |
```

```
        coupling {dual-homing primary interface <pri-if> backup
```

```
interface <sec-if> |
```

```
        backup interface <sec-if> |
```

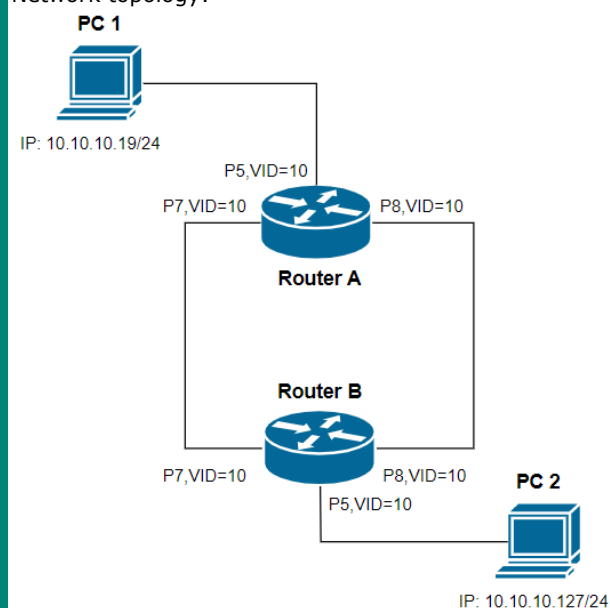
```
        primary interface <pri-if>}}}
```

```
(config-rdnt)# no turbo-ring-v2 {<ring-id> [master] |
```

```
        coupling}}
```

<b>Option</b>	exit	Commit new settings and exit sub-level configuration mode
<b>Description</b>	turbo-ring-v2	Specifies Turbo Ring V2 settings
	ring-id	Ring ID. Only 1 or 2 is allowed to specify Ring 1 or Ring 2.
	master	Specifies the router as the master of the Ring.
	primary interface	Specifies first redundant port
	pri-if	Port ID (consists of module/port-number). E.g. 1/1, 1/5
	secondary interface	Specifies second redundant port
	sec-if	Port ID (consists of module/port-number). E.g. 1/1, 1/5
	coupling	Specifies the router as Coupler
	dual-homing	Specifies Dual-homing mode
	primary interface	Specifies the primary port
	backup interface	Specifies the backup port
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	At least enable one turbo-ring domain or coupling. But cannot enable two turbo-ring domains and coupling at the same time.	
<b>Examples</b>	Specify Turbo Ring v2 on two routers:  Prerequisites: <ul style="list-style-type: none"> <li>• TN router A: <ul style="list-style-type: none"> <li>- P5: VLAN ID=10</li> <li>- P7: VLAN ID=10, 1st redundant port</li> <li>- P8: VLAN ID=10, 2nd redundant port</li> <li>- Ring 1 is enabled.</li> </ul> </li> <li>• TN router B: <ul style="list-style-type: none"> <li>- P5: VLAN ID=10</li> <li>- P7: VLAN ID=10, 1st redundant port</li> <li>- P8: VLAN ID=10, 2nd redundant port</li> <li>- Ring 1 is enabled.</li> </ul> </li> <li>• PC-1: <ul style="list-style-type: none"> <li>- IP: 10.10.10.19/24</li> </ul> </li> <li>• PC-2 : <ul style="list-style-type: none"> <li>- IP: 10.10.10.127/24</li> </ul> </li> </ul>	

#### Network topology:



#### Scenario:

- Router (A) and Router (B) both enable Moxa Turbo Ring v2 to provide redundancy for communication.
- PC (1) and PC (2) can communicate with each other via Router (A) and Router (B).
- This feature provides a network redundancy to achieve a fast recovery time when the primary path is disconnected.

#### Commands:

##### On Router A:

```
router(config)# redundancy mode turbo-ring-v2
router(config)# redundancy
router(config-rdnt)# turbo-ring-v2 1 primary interface 1/7 secondary
interface 1/8
router(config-rdnt)# no turbo-ring-v2 1 master
router(config-rdnt)# no turbo-ring-v2 2 master
router(config-rdnt)# no turbo-ring-v2 2
router(config-rdnt)# no turbo-ring-v2 coupling
router(config-rdnt)# exit
```

##### On Router B:

```
router(config)# redundancy mode turbo-ring-v2
router(config)# redundancy
router(config-rdnt)# turbo-ring-v2 1 primary interface 1/7 secondary
interface 1/8
router(config-rdnt)# no turbo-ring-v2 1 master
router(config-rdnt)# no turbo-ring-v2 2 master
router(config-rdnt)# no turbo-ring-v2 2
router(config-rdnt)# no turbo-ring-v2 coupling
router(config-rdnt)# exit
```

#### Error Messages

Turbo ring v2 only supports maximum 2 ring domains

Ring1: One port couldn't be set as 1st and 2nd redundant port simultaneously!!!

Ring2: One port couldn't be set as Ring1 redundant port simultaneously!!!

Coupling: One port couldn't be set as 1st and 2nd redundant port simultaneously!!!

Primary port couldn't be set as Ring2 redundant port simultaneously!!!

Backup port couldn't be set as Ring2 redundant port simultaneously!!!

Coupling port couldn't be set as Ring2 redundant port simultaneously!!!

	Please select at least one Ring!!!
	Ring1, ring2, coupling couldn't be enabled simultaneously!!!
	Please enable one Ring in "Ring Coupling" mode!!!
	^Parse error
	^Incomplete command
<b>Related Commands</b>	show turbo-ring-v2

## show redundancy turbo-ring-v2

Use the **show spanning-tree turbo-ring-v2** user EXEC command to display Turbo Ring v2 configuration and state information.

### Synopsis

# **show redundancy turbo-ring-v2**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre> router# show redundancy turbo-ring-v2 Turbo Ring V2 settings:     Ring 1: Enabled               Set as master: Disabled               1st port:      7               2nd port:      8     Ring 2: Disabled               Set as master: Disabled               1st port:      5               2nd port:      6     Ring Coupling: Disabled               Primary Port:3               Backup Port:4  Turbo Ring V2 status:     Ring 1:               Status:Healthy               Master/Slave:Slave               1st Ring Port Status:7 Forwarding               2nd Ring Port Status:8 Forwarding     Ring 2:               Status:---               Master/Slave:---               1st Ring Port Status:---               2nd Ring Port Status:---     Coupling:               Mode:---               Coupling Port Status: --- </pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	redundancy turbo-ring-v2



## Turbo Chain

Please note that settings and available options will vary by product model.

### redundancy mode turbo-chain

Set L2 redundancy mode to Turbo Chain.

#### Synopsis

(config)# **redundancy mode turbo-chain**

<b>Option Description</b>	turbo-chain	Turbo chain
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global Configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Firewall/VPN Router 00000# configure Firewall/VPN Router 00000(config)# redundancy mode turbo-chain	
<b>Error messages</b>	^Incomplete command ^Parse error	
<b>Related Commands</b>	show redundancy mode show redundancy turbo-chain	

### turbo-chain

Set Turbo Chain configuration.

#### Synopsis

(config-rdnt)# **turbo-chain role { head | member | tail } primary interface <ethernet-port-id> secondary interface <ethernet-port-id>**

<b>Option Description</b>	<b>role</b>	Role of this switch in Turbo Chain
	<b>head</b>	Turbo Chain head switch
	<b>member</b>	Turbo Chain member switch
	<b>tail</b>	Turbo Chain tail switch
	<b>primary</b>	Turbo Chain primary port
	<b>secondary</b>	Turbo Chain secondary port
	<b>interface</b>	Interface of Turbo Chain
	<b>ethernet-port-id</b>	Ethernet port ID. e.g. 1/1
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Redundancy Configuration Sub-mode	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>Chain ports cannot be the same port.</li><li>Trunk ports cannot be set as chain ports.</li></ul>	
<b>Examples</b>	Firewall/VPN Router 00000# configure Firewall/VPN Router 00000(config)# redundancy Firewall/VPN Router 00000(config-rdnt)# turbo-chain role member primary interface 1/7 secondary interface 1/8	
<b>Error messages</b>	% Interface <ethernet-port-id> not exist % Identical Turbo Chain ports.	
<b>Related Commands</b>	show redundancy turbo-chain	

## show redundancy turbo-chain

Show Turbo Chain configuration and status.

### Synopsis

#### show redundancy turbo-chain

<b>Option</b>	<b>show</b>	Show system information
<b>Description</b>	<b>redundancy</b>	Display redundancy protocol status
	<b>turbo-chain</b>	Display turbo chain status
<b>Defaults</b>	N/A	
<b>Command</b>	Privileged EXEC	
<b>Modes</b>		
<b>Usage</b>	N/A	
<b>Guidelines</b>		
<b>Examples</b>	<pre>Firewall/VPN Router 00000# show redundancy turbo-chain Admin Status : Enabled Role          : Head ----- Port Role      Port Number Port State ----- Head Port      1/8          Forwarding Member Port    1/7          Forwarding  Firewall/VPN Router 00000# sh red turbo-chain Admin Status : Disabled Role          : Member ----- Port Role      Port Number Port State ----- Member Port 1  1/7          --- Member Port 2  1/8          ---</pre>	
<b>Error messages</b>	N/A	
<b>Related Commands</b>	redundancy mode turbo-chain turbo-chain role { head   member   tail } primary interface <ethernet-port-id> secondary interface <ethernet-port-id>	



### **NOTE**

If the device is not capable of sending SMS notification, the SMS action in the "combination" is ignored.

# Virtual LAN

## Create/Remove VLAN ports

### vlan create

To create VLAN IDs on the router, use the **vlan create** global configuration command. To remove the VLAN IDs, use the **no** form of this command.

#### Synopsis

(config)# **vlan create** <string-vlan-ids>

(config)# **no vlan create** <string-vlan-ids>

<b>Option Description</b>	string-vlan-ids	A VLAN ID or a list of VLAN IDs separated by comma.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>• VLAN ID ranges from 1 to 4094.</li><li>• If the VLAN ID is associated with a WAN interface, removing the VLAN ID will also clear the VLAN ID of the WAN, subsequently deleting the VLAN entry from the VLAN list.</li><li>• The removal command won't take effect if you attempt to remove a managed VLAN ID.</li><li>• If you remove a non-managed VLAN ID, it will also remove the associated LAN interface, subsequently deleting the VLAN entry from the VLAN list.</li></ul>	
<b>Examples</b>	<ul style="list-style-type: none"><li>• Specify VLAN ID 55: router# configure router(config)# vlan create 55 router(config)# exit</li><li>• Remove VLAN ID 55 (and associated LAN interface if any): router# configure router(config)# no vlan create 55 router(config)# exit</li></ul>	
<b>Error Messages</b>	% vlan is invalid!! Should be range from 1 to 4094 ^Parse error ^Incomplete command	
<b>Related Commands</b>	show vlan interface vlan	

## show vlan

Use the **show vlan** user EXEC command to display VLAN status information.

### Synopsis

# **show vlan**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre>router# show vlan vlan mode: 802.1Q vlan mgmt vlan: 1  VLAN 1:   Access Ports: 1/1, 1/2, 1/3, 1/4, 1/6, 1/9, 1/10, 1/11,                 1/12, 1/13, 1/14, 1/15, 1/16,   Trunk Ports:   Hybrid Ports:   Bridge Ports: VLAN 10:   Access Ports: 1/5, 1/7, 1/8,   Trunk Ports:   Hybrid Ports:   Bridge Ports: VLAN 55:   Access Ports:   Trunk Ports:   Hybrid Ports:   Bridge Ports:</pre>
<b>Error Messages</b>	^Parse error ^Incomplete command
<b>Related Commands</b>	vlan create show vlan config

## show vlan config

Use the **show vlan config** user EXEC command to display VLAN configuration information.

### Synopsis

# **show vlan config**

<b>Option Description</b>	N/A
<b>Defaults</b>	N/A
<b>Command Modes</b>	Privileged EXEC / User EXEC
<b>Usage Guidelines</b>	N/A
<b>Examples</b>	<pre> router# show vlan config vlan mode: 802.1Q vlan VLAN  Ports(Type) ----- 1      1/1(A), 1/2(A), 1/3(A), 1/4(A), 1/6(A), 1/9(A), 1/10(A),       1/11(A), 1/12(A), 1/13(A), 1/14(A), 1/15(A), 1/16(A), 10     1/5(A), 1/7(A), 1/8(A), ===== Port   Trunk Native vlan Port   Fixed VLAN  (Tagged) Port   Fixed VLAN  (Untagged)  Current VLAN interface vid:       1, 10, 55,           </pre>
<b>Error Messages</b>	^Parse error
<b>Related Commands</b>	interface ethernet switchport vlan create show vlan

# Multicast

## IGMP Snooping

### ip igmp-snooping

Use the **ip igmp-snooping** global configuration command on the switch to globally enable Internet Group Management Protocol (IGMP) snooping on the switch. Use the command with keywords to enable IGMP snooping. Use the **no** form of this command to disable IGMP snooping.

#### Synopsis

```
(config)# ip igmp-snooping {vlan <vlan-id> [mrouter <mod-port>] |  
                           querier vlan <vlan-id> [v3] |  
                           query-interval <seconds>}
```

```
(config)# no ip igmp-snooping [{vlan <vlan-id> |  
                               querier vlan <vlan-id>}]
```

<b>Option Description</b>	vlan	Specifies VLAN parameters and enables IGMP Snooping
	vlan-id	Ranges from 1 to 4094
	mrouter	Specifies the Port ID that will connect to the multicast routers. Note that IGMP snooping vlan <vlan-id> needs to be specified in advance.
	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	querier vlan	Specifies IGMP snooping query enable
	v3	Specifies IGMPv3 mode
	query-interval	Specifies IGMP snooping query interval
	seconds	Ranges from 20 to 600 seconds
<b>Defaults</b>	IGMP snooping is globally disabled.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"><li>IGMP snooping function will be enabled automatically as soon as the first VLAN is configured.</li><li>Use <b>ip igmp-snooping querier vlan &lt;vlan-id&gt; v3</b> can make the switch to send IGMP V3 query, otherwise the default is V2 query.</li><li>Make sure the VLAN ID is created in advance before using it.</li></ul>	
<b>Examples</b>	Enable IGMP snooping on VLAN ID(1) and enable querier function (V3). Then specify static multicast querier port on PORT1 and PORT3 : router# configure router(config)# ip igmp-snooping vlan 1 router(config)# ip igmp-snooping querier vlan 1 v3 router(config)# ip igmp-snooping vlan 1 mrouter 1/1,1/3, router(config)# exit	
<b>Error Messages</b>	% Please check the multicast mac address's type !!!	
	% Vlan IGMP Function is Disabled !!!	
	% Vlan entry not found!!!	
	^Parse error	
<b>Related Commands</b>	^Incomplete command	
	show ip igmp config	

## show ip igmp

Use the **show ip igmp** user EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration and the IGMP table of the switch.

### Synopsis

```
# show ip igmp [{group <grp-addr> [source <src-addr>] |  
config}]
```

<b>Option Description</b>	group	Show IGMP table by specified group address
	grp-addr	Multicast group IP address
	source	Show IGMP table by specified group address and source address
	src-addr	Multicast source IP address
	config	Show IGMP snooping settings
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	router# show ip igmp config IGMP Snooping :Enable Query Interval :125 (sec)  VID   Static(S) Multicast Querier   Enable Querier ----- 1 1, 3, Enable (V3)	
<b>Examples</b>	N/A	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	ip igmp-snooping	

## Static Multicast MAC

### ip igmp static-group

Use the **ip igmp static-group** global configuration command on the switch to add a static multicast MAC address and its member ports. Use the **no** form of this command to remove the static multicast group or its member ports.

#### Synopsis

```
(config)# ip igmp static-group <mac-address> interface <module-port>
```

```
(config)# no ip igmp static-group [mac-address [interface <module-port>]]
```

<b>Option</b>	mac-address	MAC address XX:XX:XX:XX:XX:XX
<b>Description</b>	interface	Specifies binding ports
	module-port	Port (Trunk) ID or list. Ex. 1/1,2,4-5,2/1,Trk1,Trk2-Trk
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router(config)# ip igmp static-group 01:00:5E:01:01:08 interface 1/8 router(config)# no ip igmp static-group	
<b>Error Messages</b>	Add new static multicast MAC address Fail!!! Please check the multicast mac address's type!!! Add new static multicast MAC address Fail!!! Not enough space to add a new static multicast MAC address!!! The member port should not be GMRP-enabled port!!! ^Parse error ^Incomplete command	
<b>Related Commands</b>	show mac-address-table mcast show ip igmp config	



# QoS and Rate Control

## QoS Classification

### qos mode

Use the **qos mode** global configuration command on the switch to configure the current QoS strategy. Use **no** form of this command to return to the default.

#### Synopsis

```
(config)# qos mode {weighted-fair |  
                    strict}
```

```
(config)# no qos mode
```

<b>Option</b>	weighted-fair	Weighted fair queuing
<b>Description</b>	strict	Strict queuing
<b>Defaults</b>	Default QoS strategy is Weighted-fair queuing.	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify QoS mode to "strict" : router# configure router(config)# qos mode strict router(config)# exit	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	show qos	

## qos mapping

Use the **qos mapping** global configuration command on the switch to configure the CoS and DSCP mappings. Use **no** form of this command to return to the default value.

### Synopsis

```
(config)# qos mapping {cos-to-queue <cos-value> <queue> |  
                    dscp-to-queue <dscp-value> <queue>}
```

```
(config)# no qos mapping {dscp-to-queue |  
                        cos-to-queue}
```

<b>Option</b>	cos-to-queue	CoS to traffic queue
<b>Description</b>	cos-value	CoS value (0~7)
	queue	Traffic queue (port priority). Ranges from 0(Low) to 3(High)
	dscp-to-queue	DSCP to traffic queue
	dscp-value	DSCP value (0~63)
<b>Defaults</b>	Cos (queue) : 0 (0), 1(0), 2(1), 3(1), 4(2), 5(2), 6(3), 7(3) DSCP(Cos) : 0-15(0), 16-31(1), 32-47(2), 48-63(3)	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify CoS (1) to queue Normal (1): router# configure router(config)# qos mapping cos-to-queue 1 1 router(config)# exit	
<b>Error Messages</b>	% Invalid parameter. CoS value must be 0~7 and queue number must be 0~3	
	% Invalid parameter. DSCP value must be 0~63 and queue value must be 0~3	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show qos	

## interface trunk qos

To specify or modify QoS settings to a trunked port, use the **interface trunk** global configuration command and **qos** sub-level configuration command sets. To return to the default QoS setting to the trunked port, use the **no** form of this command.

### Synopsis

```
(config)# interface trunk <trunk-id>
(config-if)# qos {inspect {cos |
                    dscp}|
                default-cos <cos-value>}
```

```
(config-if)# no qos {inspect {cos |
                    dscp}|
                default-cos}
```

<b>Option Description</b>	trunk-id	Trunk group ID. Maximum number of trunk groups differs among different models.
	qos	Specifies QoS settings
	inspect	Specifies cos/dscp inspection
	cos	Enables "inspect CoS"
	dscp	Enables "inspect ToS"
	default-cos	Specifies default CoS value
	cos-value	Ranges from 0 to 7
<b>Defaults</b>	CoS is enabled; DSCP is enabled.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	<ul style="list-style-type: none"> <li>Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command</li> <li>The priority of an ingress frame is determined in the following order: <ol style="list-style-type: none"> <li>CoS</li> <li>DSCP</li> <li>Port priority</li> </ol> </li> </ul>	
<b>Examples</b>	Disable CoS on trk1 and change port priority to 7(High): <pre>router# configure router(config)# interface trunk 1 router(config-if)# no qos inspect cos router(config-if)# qos default-cos 7 router(config-if)# exit</pre>	
<b>Error Messages</b>	% CoS value is out of range! The allowed value range is 0 to 7	
	^Parse error ^Incomplete command	
<b>Related Commands</b>	show qos	

## interface ethernet qos

To specify or modify QoS settings to an Ethernet port, use the **interface ethernet** global configuration command and **qos** sub-level configuration command sets. To return to the default QoS setting to the Ethernet port, use the **no** form of this command.

### Synopsis

```
(config)# interface ethernet <mod-port>
(config-if)# qos {inspect {cos |
                    dscp} |
                 default-cos <cos-value>}

(config-if)# no qos {inspect {cos |
                        dscp}|
                   default-cos}
```

<b>Option Description</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	qos	Specifies QoS settings
	inspect	Specifies cos/dscp inspection
	cos	Enables "inspect CoS"
	dscp	Enables "inspect ToS"
	default-cos	Specifies default CoS value
	cos-value	Ranges from 0 to 7
<b>Defaults</b>	CoS is enabled; DSCP is enabled.	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	The priority of an ingress frame is determined in the following order: 1. CoS 2. DSCP 3. Port priority	
<b>Examples</b>	Disable CoS on Ethernet PORT1 and change port priority to 7(High): router# configure router(config)# interface ethernet 1/1 router(config-if)# no qos inspect cos router(config-if)# qos default-cos 7 router(config-if)# exit	
<b>Error Messages</b>	% CoS value is out of range! The allowed value range is 0 to 7 ^Parse error ^Incomplete command	
<b>Related Commands</b>	show qos	

## show qos

Use the **show qos** user EXEC command to display QoS related settings.

### Synopsis

```
# show qos [{cos-to-queue |  
            dscp-to-queue}]
```

<b>Option</b>	qos	Display QoS configuration
<b>Description</b>	cos-to-queue	CoS to traffic queue mappings
	dscp-to-queue	DSCP to traffic queue mappings
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# show qos  Queuing Mechanism : Weighted Fair (1:2:4:8)  Int# CoS Inspection ToS Inspection CoS ----- 1/1 Disabled Enabled 7 1/2 Enabled Enabled 3 1/3 Enabled Enabled 3 1/4 Enabled Enabled 3 1/5 Enabled Enabled 3 1/6 Enabled Enabled 3 Trk1 Disabled Enabled 7	
<b>Error Messages</b>	^Parse error ^Incomplete command	
<b>Related Commands</b>	qos mode qos mapping interface trunk qos interface ethernet qos	

## Rate Limiting

### interface ethernet rate-limit

To specify or modify a rate limiting percentage, use the **interface ethernet** global configuration command and related sub-level configuration command sets. To return to the default settings, use the **no** form of this command.

#### Synopsis

```
(config)# interface ethernet <mod-port>
```

```
(config-if)# rate-limit normal {ingress percentage | egress percentage} <number>
```

```
(config-if)# no rate-limit normal {ingress percentage | egress percentage}
```

<b>Option</b>	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,.
<b>Description</b>	rate-limit normal	Specifies rate-limit for ingress/egress packets
	ingress percentage	Specifies ingress percentage
	egress percentage	Specifies egress percentage
	number	Specifies an integer for: {Not limited(0)   3%(3)   5%(5)   10%(10)   15%(15)   25%(25)   35%(35)   50%(50)   65%(65)   85%(85)}
<b>Defaults</b>	Not limited	
<b>Command Modes</b>	Global configuration, sub-level configuration	
<b>Usage Guidelines</b>	N/A.	
<b>Examples</b>	Specify 50% rate limit of egress on PORT3: router# configure router(config)# interface ethernet 1/3 router(config-if)# rate-limit normal egress percentage 50 router(config-if)# exit	
<b>Error Messages</b>	% Illegal parameter	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	rate-limit ingress	

## rate-limit ingress

Use the **rate-limit ingress** configuration command on the router to configure the ingress policy.

### Synopsis

```
(config)# rate-limit ingress mode {bcast |  
                                     bcast-mcast |  
                                     bcast-mcast-dlf |  
                                     all}
```

```
(config)# rate-limit ingress action {drop-packet |  
                                     port-disable }
```

```
(config)# rate-limit ingress port-disable period <second>
```

<b>Option</b>	mode	Specifies the mode
<b>Description</b>	bcast	Limit broadcast frames
	bcast-mcast	Limit broadcast and multicast frames
	bcast-mcast-dlf	Limit broadcast, multicast and flooded unicast which is also known as DLF (destination lookup failure) frames
	all	All traffic
	action	Specifies the action to take.
	drop-packet	Drop incoming packets that do not comply with the ingress policy.
	port-disable	Disable the port that do not comply with the ingress policy.
	period	Specifies a duration during which the port remains disabled.
	second	Integer value ranges from 1 to 65535.
<b>Defaults</b>	Limit broadcast frames/Drop Packeeet	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	After the specified duration for port disablement ends, the port will be reactivated. Yet, if the port fails to comply with the ingress policy once more, it will be disabled again.	
<b>Examples</b>	Specify rate limit ingress policy to bcast-mcast and disable the port that exceeds the designated bandwidth for 500 seconds: router# configure router(config)# rate-limit ingress mode bcast-mcast router(config)#rate-limit ingress action port-disable router(config)#rate-limit ingress port-disable period 500 router(config)# exit	
<b>Error Messages</b>	% Invalid Period Value. It must be 0 - 65535.	
	^Parse error	
	^Incomplete command	
<b>Related Commands</b>	interface ethernet rate-limit	

## MAC Address Table

### mac-address-table aging-time

To specify or modify the aging time of the MAC address table, use the **mac-address-table aging-time** global configuration command. To return to the default, use the **no** form of this command.

#### **Synopsis**

(config)# **mac-address-table aging-time** <second>

(config)# **no mac-address-table aging-time**

<b>Option Description</b>	second	Ranges from 5 to 300 seconds.
<b>Defaults</b>	300	
<b>Command Modes</b>	Global configuration	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	Specify the aging-time to 200 seconds: router# configure router(config)# mac-address-table aging-time 200 router(config)# exit	
<b>Error Messages</b>	% Age time should between 5~300s! ^Parse error ^Incomplete command	
<b>Related Commands</b>	show mac-address-table	



## show mac-address-table

Use the **show mac-address-table** user EXEC command to display the MAC addresses in the MAC address table.

### Synopsis

```
# show mac-address-table [{static |
                           learned |
                           mcast |
                           aging-time}]
# show mac-address-table interface {ethernet <mod-port> |
                                   trunk <trunk-id>}
```

<b>Option</b>	static	Retrieve static MAC addresses
<b>Description</b>	learned	Retrieve learned MAC addresses
	mcast	Retrieve Multicast address
	aging-time	MAC entry aging time
	interface	Retrieve MAC address by interface
	ethernet	Ethernet Port interface
	mod-port	Port ID. Ex. 1/3, 2/1,...
	trunk	Trunk interface
	trunk-id	Trunk ID.
<b>Defaults</b>	N/A	
<b>Command Modes</b>	Privileged EXEC / User EXEC	
<b>Usage Guidelines</b>	N/A	
<b>Examples</b>	router# show mac-address-table	
	Idx	MAC
	Type	VLAN
	Port	
	-----	-----
	1	01-00-5E-7F-FF-FA
	2	50-7B-9D-E1-82-5A
	mcast (s)	1
	ucast (1)	1
	1/1,1/2,	1/2,
	router# show mac-address-table aging-time	
	MAC address aging time: 300 sec	
<b>Error Messages</b>	^Parse error	
<b>Related Commands</b>	^Incomplete command	
	mac-address-table aging-time	

## 5. Supplementary Information

---

Below table lists known issues or limitation related to CLI of Firmware v3.6

Item	CLI	Descriptions
S-2	(config)# interface ethernet <mod-port> (config-if)# trunk-mode	TN router only supports static trunk mode. Therefore, there is no need to configure trunk-mode in this case.
S-3	(config)# package	This command is currently listed but reserved for future use.
S-4	# package uninstall <pkg-name>	This command is currently listed but reserved for future use.
S-5	(config)# interface bridge (config-brg) goose-pass-through	The command is included in the list as deprecated to prevent migration errors when moving from version 2.0 to 3.0.
S-7	(config-vif) ip address <ip> <netmask> secondary	When the secondary IP is same as interface's IP address, no error message appears.

## 6. Command Compatibility

To ensure a seamless user experience, we are temporarily maintaining certain deprecated Command Line Interface (CLI) commands. These commands will remain usable for one year following the release of the new CLI command version. We advise you to transition to the new commands at your earliest convenience to ensure ongoing efficiency and support. For more details, please refer to the updated CLI command list below.

Index	Deprecated CLI	Fine-tuned CLI	Version Since
1	goose-pass-through no goose-pass-through	keep deprecated CLI	V.3.0
2	firewall <policy Index> no firewall <policy Index>	keep deprecated CLI	V2.0
3	l2-filter <UINT:index> #submode "l2_filter" // Set policy accept packets action accept // Set policy drop packets action drop // Set filter protocol protocol <STRING:protocol> // Set filter ether type ether-type <STRING:type> // Set source mac address src-mac <MACADDR:macaddr> // Set destination mac address dst-mac <MACADDR:macaddr> // Set log logging no logging logging severity <UINT:level> logging syslog no logging syslog logging flash no logging flash // Set interface interface <STRING:if_from> <STRING:if_to> // Exit policy configuration mode exit #endsubmode  l2-filter <UINT:index> enable l2-filter <UINT:index> disable no l2-filter <UINT:index> logging-capacity snmp-trap- warning <b>layer2-filter</b> logging-capacity email-warning <b>layer2-filter</b> logging-capacity over-size-action overwrite-oldest <b>layer2-filter</b> logging-capacity over-size-action stop-recording <b>layer2-filter</b>	l2-policy <UINT:index> #submode "l2_policy" // Set policy accept packets action accept // Set policy drop packets action drop // Set filter protocol protocol <STRING:protocol> // Set filter ether type ether-type <STRING:type> // Set source mac address src-mac <MACADDR:macaddr> // Set destination mac address dst-mac <MACADDR:macaddr> // Set log logging no logging logging severity <UINT:level> logging syslog no logging syslog logging flash no logging flash // Set interface interface <STRING:if_from> <STRING:if_to> // Exit policy configuration mode exit #endsubmode  <b>l2-policy</b> <UINT:index> enable <b>l2-policy</b> <UINT:index> disable no <b>l2-policy</b> <UINT:index> logging-capacity snmp-trap-warning <b>layer2- policy</b> logging-capacity email-warning <b>layer2-policy</b> logging-capacity over-size-action overwrite-oldest <b>layer2-policy</b> logging-capacity over-size-action stop-recording <b>layer2-policy</b> logging-capacity <UINT:threshold> <b>layer2- policy</b>	V3.3

Index	Deprecated CLI	Fine-tuned CLI	Version Since
	logging-capacity <UINT:threshold> <b>layer2-filter</b> no logging-capacity snmp-trap-warning <b>layer2-filter</b> no logging-capacity email-warning <b>layer2-filter</b> no logging-capacity <b>layer2-filter</b>	no logging-capacity snmp-trap-warning <b>layer2-policy</b> no logging-capacity email-warning layer2-policy no logging-capacity <b>layer2-policy</b>	
4	// show l2-filter log show logging event-log l2-filter // show l2-filter log with severity show logging event-log l2-filter severity <STRING:range> show l2-filter clear logging event-log l2-filter	// show l2- <b>policy</b> log show logging event-log l2- <b>policy</b> // show l2-policy log with severity show logging event-log l2- <b>policy</b> severity <STRING:range> show l2- <b>policy</b> clear logging event-log l2- <b>policy</b>	V3.3
5	dos icmp-death <UINT:limit> no dos icmp-death dos new-tcp-without-syn-scan no dos new-tcp-without-syn-scan	dos <b>icmp-flood</b> <UINT:limit> no dos <b>icmp-flood</b> dos <b>tcp-sessions-without-syn</b> no dos <b>tcp-sessions-without-syn</b>	V3.3
6	ip dhcp-relay option82 remote-id-type ip	ip dhcp-relay option82 remote-id-type <b>interface</b> <STRING:interface>	V3.4
7	spanning-tree hello-time <UINT:seconds> no spanning-tree hello-time spanning-tree forward-delay <UINT:seconds> no spanning-tree forward-delay spanning-tree max-age <UINT:seconds> no spanning-tree max-age	spanning-tree time <UINT:hello_time> <UINT:forward_delay> <UINT:max_age>	V3.4