MX-ROS V3 CLI Command Set User Manual

Version 1.14, November 2026

www.moxa.com/products

© 2026 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

© 2026 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

Table of Contents

1. Overview 4
Supported Series and Firmware Versions 4
Document Conventions 4
Command Modes 5
Command Sets 7
System 7
snmp-server community 35
Security 56
Diagnostics 98
copy diagnostic-logging 153
Network Services 154
2. Layer 2 Functions 182
Command Modes 182
Command Sets 183
Port 183
Network Redundancy 202
Virtual LAN 224
Multicast 227
QoS and Rate Control 230
3. Interfaces and Routing Functions 242
Command Modes 242
Command Sets 243
Interfaces 243
Routing 311
4. NAT, VPN and Firewall Functions 351
Command Modes 351
Command Sets 352
Network Address Translation 352
Firewall 374
Virtual Private Network (VPN) 433
IPS 449
5. MXsecurity 463
Command Modes 463
Command Sets 464
MXsecurity 464
6. Cellular Functions 467
Command Modes 467
Command Sets 468
SMS 481
SMS Notification 495
GNSS 496
Power Management 504
MRC 510
Serial 511
7. Supplementary Information 544
8. Command Compatibility 545

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-G1002 Series	v3.30.1
EDR-8010 Series	v3.30
EDR-G9004 Series	v3.30
EDR-G9010 Series	v3.30
ioPAC 6500 Firewall Modules	v3.30
NAT-102 Series	v3.30
NAT-108 Series	v3.30
OnCell G4302-LTE4 Series	v3.30
OnCell G4308-LTE4 Series	v3.30
TN-4900 Series	v3.32



Note

Before upgrading a NAT-100 Series device from v1.x to v3.x, we suggest saving the previous version's configuration first, then redoing the device's configuration after the upgrade to prevent compatibility issues.



Note

Starting from v3.12, 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 v3.12 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 features and feature and settings may vary. The versions listed here may be released after publication of this document.

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 **Text** 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 **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information. • Enter configuration mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	(config)#	To exit to privileged EXEC mode, enter **exit**.	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example **ip dhcp pool <index>** command and press enter	(dhcp-config)#	To exit to global configuration mode, enter **exit**.	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

Example 1: List a command list (note that '?' will not be displayed on the console)

```
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#
```

Example 2: List command parameters (note that '?' will not be displayed on the console)

```
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)#
```

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**]]

Option Description	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.
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	Warning: After resetting to factory defaults, previous settings cannot be recovered. To avoid this situation, you should export the current configuration file before proceeding.	
Examples	• Reload factory default settings and keep existing certificates. `router# reload factory-default` `Proceed with reload to factory default? [Y/n]` • Reload factory default settings and remove existing certificates. `router# reload factory-default no cert` `Proceed with reload to factory default? [Y/n]` • Halt and perform a warm restart `router# reload` `Proceed with reload ? [Y/n]`	
Error Messages	N/A	
Related Commands	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**

Option Description	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.
Defaults	The default text is: "Firewall/VPN Router [6 last digits of serial number]"	
Command Modes	Global configuration	
Usage Guidelines	• The system name is composed of a maximum of 5 tokens, with a whitespace positioned between each token. • Allowed characters: a-z, A-Z, 0-9 or . - _ @ ! # $ % ^ & * ( ). / • Maximum length of system name including whitespaces is 30.	
Examples	• Specify/modify the system name to "MOXA Ethernet Router TN-4908". In this example, token1=MOXA token2=Ethernet token3=Router token4=TN-4908 `router# configure` `router(config)# hostname MOXA Ethernet Router TN-4908` `router(config)# exit` • Resetting router's name to default settings. `router# configure` `router(config)# no hostname` `router(config)# exit`	
Error Messages	Length of router hostname is too long	
	^Parse error	
Related Commands	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**

Option Description	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.
Defaults	Empty string	
Command Modes	Global configuration	
Usage Guidelines	• The contact information is composed of a maximum of 5 tokens, with a whitespace positioned between each token. • Allowed characters: a-z, A-Z, 0-9 or . - _ @ ! # $ % ^ & * ( ). / • Maximum length of contact information including whitespaces is 40.	
Examples	Specify/modify the system Contact Information to "Green Line Bob". In this example, token1=Green token2=Line token3=Bob `router# configure` `router(config)# snmp-server contact Green line Bob` `router(config)# exit` • Resetting contact info to default settings. `router# configure` `router(config)# no snmp-server contact` `router(config)# exit`	
Error Messages	Length of maintainer info is too long	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	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.
Defaults	Empty string	
Command Modes	Global configuration	
Usage Guidelines	• The system description is composed of a maximum of 5 tokens, with a whitespace positioned between each token. • Allowed characters: a-z, A-Z, 0-9 or . - _ @ ! # $ % ^ & * ( ). / • Maximum length of system description including whitespaces is 40.	
Examples	• Specify/modify the system description to "Moxa TN router". In this example, token1=Moxa token2=TN token3=router `router# configure` `router(config)# snmp-server description Moxa TN router` `router(config)# exit` • Resetting system description to default settings. `router# configure` `router(config)# no snmp-server description` `router(config)# exit`	
Error Messages	Length of system description is too long	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	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.
Defaults	The default text is "Device Location".	
Command Modes	Global configuration	
Usage Guidelines	• The location is composed of a maximum of 5 tokens, with a whitespace positioned between each token. • Allowed characters: a-z, A-Z, 0-9 or . - _ @ ! # $ % ^ & * ( ). / • Maximum length of location including whitespaces is 80.	
Examples	Specify/modify the location of the device to "Consist 1". In this example, token1=Consist token2=1 `router# configure` `router(config)# snmp-server location Consist 1` `router(config)# exit` • Resetting device location to default settings. `router# configure` `router(config)# no snmp-server location` `router(config)# exit`	
Error Messages	Length of location is too long	
	% Not in correct format	
	^Parse error	
	^Incomplete command	
Related Commands	show system	

show system

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

Synopsis

show system

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error messages	^Parse error	
	^Incomplete command	
Related Commands	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

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

Option Description	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
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	The system will reboot automatically, regardless of command success.	
Examples	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 transfering...` `Initial checking, please wait.` `Verified OK` `buildinPkg/` `buildinPkg/MXSecurity_TN-4900_V2.0.12_Build_23072113.pkg` `buildinPkg/Security_TN-4900_V7.0.9_Build_23071914.pkg` `Checking transfer:Firmware Upgrade OK! Restart the device.`	
Error Messages	Input error	
	Invalid parameter!	
	^Parse error	
	^Incomplete command	
Related Commands	show version auto-backup enable	

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 {config-file | diagnostic-logging | ha-firmware} <filename> |
{**scp** | **sftp**} <account> <password> <ip> **config-file** <cfg-path-name>}

Option Description	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
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	• After importing configuration file successfully, console terminal will restart automatically. • After exporting configuration file successfully, existing configuration file on USB will be replaced. • Default configuration file name after export is Sys.ini. • CLI treats the configuration file name as case-insensitive. • Hardware interface must be enabled before selecting USB storage device.	
Examples	• Backup current configuration file to a remote TFTP server. `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#` • Restore configuration from a remote SCP server. `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.`	
Error Messages	Input error	
	No USB Device	
	Invalid parameter!	
	% Configuration Upload Fail!	
	% Config file import failed.	
	^Parse error	
	^Incomplete command	

Related Commands	show running-config 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

Option Description	digital-signature	Enables / disables digital signature on the configuration file.
	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.
Defaults	Disabled.	
Command Modes	Privileged EXEC	
Usage Guidelines	• This CLI command shall not be exported nor imported via a configuration file. • 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.	
Examples	• Enable Digital Signature. `router# config-file digital-signature` • Change Encryption Key to **moxa1234**. `router# config-file encryption-password moxa1234`	
Error Messages	Password Length should be less than 30	
	^Parse error	
	^Incomplete command	
Related Commands	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

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

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• A local storage (ABC-02) has to be plugged in advance. • Hardware interface (USB) has to be enabled in advance. The corresponding CLI command is provided below: (config)# auto-backup enable	
Examples	• 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` • 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`	
Error Messages	^Parse error	
	^Incomplete command	

Related Commands	show auto-backup 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**

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	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.	
Examples	N/A	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

show auto-backup

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

Synopsis

show auto-backup

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

show running-config

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

Synopsis

show running-config

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC /User EXEC	
Usage Guidelines	N/A	
Examples	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)	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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>] |
privilege <privilege>}

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

Option Description	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.
Defaults	user: admin pass: moxa privilege: 1 (admin) user: user pass: moxa privilege: 3 (user) user: configadmin pass: moxa privilege 2 (configuration admin)	
Command Modes	Global configuration	
Usage Guidelines	• <pwd-string> by default Min number of characters is 4 and Max number of characters is 64. and no rule for password creation is set. • The current logged user cannot be deleted or have privilege changed. • The default authority for a newly created account is set as User if the privilege level is not specified. • Passwords can only contain the letters a-z, A-Z, numbers 0-9 and special characters _@!#$%^&*().-+={}[]|:;,~ and cannot have any spaces.	
Examples	• Add a new user with configuration admin privilege. `router# configure` `router(config)# username test password test1234 privilege 2` `router(config)# exit` • Delete an existing user `router# configure` `router(config)# no username test` `router(config)# exit` • Modify existing user password. `router# configure` `router(config)# username test password abc1234` `router(config)# exit` • Modify existing user privilege `router# configure` `router(config)# username test privilege 1` `router(config)# exit` • Deactive an existing user `router# configure` `router(config)# username test privilege 4` `router(config)# exit`	
Error Messages	% 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	
	^Parse error	
	^Incomplete command	

Related Commands	show users password policy username <username> 2fa { disable | enable } username <username> 2fa type { totp [secret <code> recovery <code>] | email <email-address> [recovery <code>] } [no] 2fa 2fa totp-timeout <timeout> 2fa totp-tolerance { disable | enable } 2fa algorithm { SHA1 | SHA256 | SHA512 } 2fa { http | https | telnet | ssh } { disable | enable } show 2fa

show users

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

Synopsis

show users

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`router# show users` `Login account information:` `Name Authority Password expire 2FA Type 2FA Status` `------------------------ ---------------- ----- ----` `admin Admin -- TOTP Enabled` `test Admin -- Email Disabled` `tttt user -- TOTP Disabled`	
Error messages	^Parse error	
	^Incomplete command	
Related Commands	username <name> password <pwd-string> [privilege <privilege>] username <username> 2fa { disable | enable } username <username> 2fa type { totp [secret <code> recovery <code>] | email <email-address> [recovery <code>] } [no] 2fa 2fa totp-timeout <timeout> 2fa totp-tolerance { disable | enable } 2fa algorithm { SHA1 | SHA256 | SHA512 } 2fa { http | https | telnet | ssh } { disable | enable } show 2fa	

username 2fa

To enable 2FA mode for a specified user, use the **username 2fa** global configuration command.

Synopsis:

(config)# **username** <username> **2fa** { disable | enable }

Option Description	username	Set of characters without a whitespace. This field is case-sensitive.
	2fa	2-Factor Authentication
	disable	Disables the 2FA mode for this account.
	enable	Enables the 2FA mode for this account.
Defaults	disabled	

Command Modes	Global configuration
Usage Guidelines	The account will request TOTP code via authenticator or email if the mode is enabled. The account needs to do authenticator binding or email binding at next login process after 2FA enabled. Only users with admin permissions can change the 2FA mode. After enable 2FA, the 2FA type shall be configured.
Examples	Add a new user with configuration admin privilege. `router# configure` `router(config)# username test password test1234 privilege 2` 2FA mode. Enable `router(config)# username test 2fa enable` `Disable an admin privilege account` `router(config)# username test 2fa disable`
Error Messages	% The username is not available
	% Only users with admin permissions can change the 2FA mode.
	^Parse error
	^Incomplete command
Related Commands	username <name> {password <pwd-string> [privilege <privilege>] | privilege <privilege> } username <username> 2fa type { totp [secret <code> recovery <code>] | email <email -address> [recovery <code>] } [no] 2fa 2fa totp-timeout <timeout> 2fa totp-tolerance { disable | enable } 2fa algorithm { SHA1 | SHA256 | SHA512 } 2fa { http | https | telnet | ssh } { disable | enable } show 2fa

username 2fa type

To configure the 2FA type used for a specified user,use the **username 2fa type** global configuration command.

Synopsis:

(config)# **username** <username> **2fa type** { totp [secret <code> recovery <code>] | email <email-address> [recovery <code>] }

Option Description	username	Set of characters without a whitespace. This field is case-sensitive.
	2fa	2-Factor Authentication
	type	Specifies the 2FA type
	totp	Time-Based One-Time Password (TOTP) as the 2FA method. This is a time-based code verification mechanism where the code is periodically updated.
	secret	The secret code string used for generating TOTP codes.
	recovery	The recovery code string used for account recovery in case the user loses access to their TOTP device.
	code-string	The code string
	email	Email-based verification as the 2FA method. This involves sending a specific code to the user's email, which will expire after a certain period of time.
	email-address	The email address to which the verification code will be sent when using email-based 2FA.
Defaults	type: totp	
Command Modes	Global configuration	
Usage Guidelines	Identify the User: Determine the username of the account for which you want to enable 2FA.	

	Choose the 2FA Type: Decide whether you want to enable TOTP or email-based verification. Execute the Command: Use the command format to enable the desired 2FA type for the user. Verify the Configuration: Ensure that the 2FA type has been correctly set for the user by checking the system's 2FA settings.
Examples	Add a new user with configuration admin privilege. router# configure router(config)# username test password test1234 privilege 2 Enable 2FA mode. router(config)# username test 2fa enable Setup 2FA type. TOTP Type without secret code and recovery code router(config)# username test 2fa type totp TOTP Type with secret code and recovery code router(config)# username test 2fa type totp secret AABBCCDD recovery CCBBAA Email Type router(config)# username test 2fa type email test@email.com recovery CCBBAA
Error Messages	% The username is not available
	% Over length. It must be 8 - 8 (totp)
	% Over length. It must be 6 - 128 (email)
	% Over length. It must be 8 - 8 (recovery)
	^Parse error
	^Incomplete command
Related Commands	username <name> {password <pwd-string> [privilege <privilege>] | privilege <privilege> } username <username> 2fa { disable | enable } show users [no] 2fa 2fa totp-timeout <timeout> 2fa totp-tolerance { disable | enable } 2fa algorithm { SHA1 | SHA256 | SHA512 } 2fa { http | https | telnet | ssh } { disable | enable } show 2fa

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}

Option Description	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.
Defaults	By default no password rules are set	
Command Modes	Global configuration	
Usage Guidelines	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.	
Examples	• Set password minimum length to 8 `router# configure` `router(config)# password-policy minimum-length 8` `router(config)# exit` • Revoking password minimum length `router# configure` `router(config)# no password-policy minimum-length` `router(config)# exit` • Set password complexity. `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` • Revoking password complexity `router# configure` `router(config)# no password-policy complexity-check` `router(config)# exit`	
Error Messages	% Password minimum length should between 4~16	
	% Password lifetime should be between 0~365	
	^Parse error	
	^Incomplete command	
Related Commands	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}]

Option Description	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.
Defaults	HTTP and HTTPS services are enabled.	
Command Modes	Global configuration	
Usage Guidelines	Maximum number of concurrent login users for HTTP+HTTPS is 10.	
Examples	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`	
Error Messages	% 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	
Related Commands	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**]

Option Description	port	Specifies telnet port number
	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.
Defaults	Telnet service is enabled, default port number is 23	
Command Modes	Global configuration	
Usage Guidelines	• Valid port number ranges are 23, and from 1024 to 65535. Please make sure other services do not use the same port in advance. • Maximum number of concurrent login users for telnet+SSH is 5.	
Examples	Enable telnet support and set port number to 8080. `router# configure` `router(config)# ip telnet port 8080` `router(config)# ip telnet` `router(config)# exit`	
Error Messages	Maximum Login Users For TELNET+SSH % should be in range of 1 to 5.	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	port	Specifies ssh port number
	port-number	Server listening port number. Valid ranges are 22, 1024 to 65535, default is 22
Defaults	SSH service is enabled, default port number is 22.	
Command Modes	Global configuration	
Usage Guidelines	• Valid port number ranges are 22, and from 1024 to 65535. Please make sure other services do not use the same port in advance. • Maximum number of concurrent login users for telnet+SSH is 5.	
Examples	Enable ssh support and set port number to 4040. `router# configure` `router(config)# ip ssh port 4040` `router(config)# ip ssh` `router(config)# exit`	
Error Messages	% SSH port xxx is invaild, the interval is from 1 to 65535.	
	% Assign duplicated port number is not allowed	
	^Parse error	
	^Incomplete command	

Related Commands	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**

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

Option Description	N/A	
Defaults	Enabled	
Command Modes	Global configuration	
Usage Guidelines	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.	
Examples	N/A	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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

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

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

Option Description	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
Defaults	Default version is v1-v2c	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Specify/modify SNMP version to v3 support. `router# configure` `router(config)# snmp-server version v3` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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}

(config)# **snmp-server community** <UINT:index> <STRING:community> <STRING:mode>

Option Description	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 - _ @ ! # $ % & * ( ) . + = { } [ ] | : ; , ~, no spaces are allowed.
	ro	Access mode: read-only
	rw	Access mode: read-write
	no-access	Access mode: no-access
Defaults	Public community is ro Private community is rw	
Command Modes	Global configuration	
Usage Guidelines	• Specifies read-only access. Authorized management stations are only able to retrieve MIB objects. • Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects	
Examples	Specify/modify rouser as read-only community string. `router# configure` `router(config)# snmp-server community 1 rouser ro` `router(config)# exit`	
Error Messages	% 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	
Related Commands	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 | sha256 | sha512** } [**priv** {**des** | **aes**} **<password>]**

Option Description	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
	sha256	Authentication type: SHA256
	sha512	Authentication type: SHA512
	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 - _ @ ! # $ % & * ( ) . + = { } [ ] | : ; , ~, no spaces are allowed.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Length of password must be at least 8 characters.	
Examples	• Specify/modify data encryption (DES) key to moxamoxa for admin user-group. `router# configure` `router(config)# snmp-server user admin auth md5 priv des moxamoxa` `router(config)# exit` • Specify/modify authentication type to sha without altering priv and password arguments. `router# configure` `router(config)# snmp-server user admin auth sha` `router(config)# exit`	
Error Messages	% SNMP user must be (admin | user)!!	
	% SNMP authtype must be (no-auth | md5 | sha | sha256 | sha512)!!	
	% Data Encryption must be at least 8 bytes !!!	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	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.
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	• The length of the hexadecimal string is required to be an even number. • The <hex-string> must use combination of letters from 0-9, a-f, A-F. • The <hex-string> must contain a prefix string **800021f305**. • In order to use this command, SNMP version is required to be configured as either v1-v2c-v3 or v3. • It is required to re-apply or change the password for every user again to let user-defined Engine ID take effect.	
Examples	Specify a user-defined engine ID 0x800021f3051234. `router# configure` `router(config)# snmp-server version v1-v2c-v3` `router(config)# snmp-server engineid 800021f3051234` `router(config)# exit`	
Error Messages	% 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	
	^Incomplete command	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	router # show snmp SNMP Read/Write Settings SNMP Versions : v1-v2c-v3 SNMP Service Port : 161 SNMP Engine ID : 800021f3030090e8a9ed13 SNMP Account Mode : user First Community : ******** Second Community : ******** Admin Auth. Type : md5 Admin Data Encryption Key : Disable User Auth. Type : md5 User Data Encryption Key : Disable Trap Settings Trap Server 1 IP/Name : Trap Server 2 IP/Name : Trap Server 3 IP/Name : Trap Community : ******** Trap Mode Mode : Trap V1 Private MIB information Switch Object ID : enterprise.8691.6.100	
Error Messages	^Parse error ^Incomplete command	
Related Commands	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	

SNMP Account

To configure an SNMP account, use this command.

Synopsis

router# **snmp-server account** <username> **authority** {ro | rw} **auth** { no-auth | md5 | sha | sha256 | sha512 } { auth-password <auth_password> } { priv { des | aes } **encryption-key** <priv_password> }

Option Description	snmp-server	Configure snmp-server parameters
	account	Configure snmp-server user account
	username	Configure user-name for snmp-server user account
	authority	Configure access-right for snmp-server user account
	ro	Configure read-only access-right for the user
	rw	Configure read and write access-right for the user
	auth	Configure authentication-protocol for snmp-server user account
	no-auth	Configure none auth-protocol for the user
	md5	Configure use md5 as auth-protocol
	sha1	Configure use sha as auth-protocol
	sha256	Configure use sha256 as auth-protocol
	sha512	Configure use sha512 as auth-protocol
	auth-passwd	Configure authencation-password for snmp-server user account
	auth_password	Configure authencation-password
	priv	Configure data encryption protocol for snmp-server user account
	des	Use DES as data-encryption protocol
	aes	Use AES as data-encryption protocol
	encryption-key	Configure data encryption-key for snmp-server user account
	priv_password	Configure data encryption-key
Defaults	No user-account table	
Command Modes	Global configuration	
Usage Guidelines	If authentication-type is no-auth, data-encryption method should be disabled. If authentication-type is not-none, must setup authentication password. If data-encryption method is set, must setup data encryption key.	
Examples	• Specify/modify data encryption (DES) key to moxamoxa for admin user-group. `router# configure` `router(config)#  snmp-server account admin authority rw auth md5 auth-password moxamoxa priv des moxamoxa` `router(config)# exit` • Specify/modify authentication type to sha without altering priv and password arguments. `router# configure` `router(config)# snmp-server account admin authority rw auth md5 auth-password moxamoxa` `router(config)# exit`	
Error Messages	% SNMP user must be (admin | user)!!	
	% SNMP authtype must be (no-auth | md5 | sha | sha256 | sha512)!!	
	% Data Encryption must be at least 8 bytes !!!	
	% is an invalid system symbol.	
	^Parse error	
	^Incomplete command	
Related Commands	snmp-servershow snmp-server account	

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}

Option Description	index	First or second community: 1 or 2
	community	SNMP community string. Max. 64 characters. Allowed characters: • a-z • A-Z • numbers 0-9 • special characters _@!#$%&*().-+={}[]|:;,~ • Cannot contain spaces
	ro	Access mode: read-only. Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
	rw	Access mode: read-write. Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects
	no-access	Access mode: no-access
Defaults	Public community is `ro` Private community is `rw`	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Specify/modify rouser as read-only community string. `router# configure` `router(config)# snmp-server 1 rouser ro` `router(config)# exit`	
Error Messages	% Index must be 1 - 2.	
	Access mode must be rw, ro or no-access.	
	% is over length. It must be 1 - 30.	
	% is an invalid system symbol.	
	^Parse error	
	^Incomplete command	
Related Commands	snmp-server version snmp-server user snmp-server host snmp-server trap-mode snmp-server engineid show snmp	

snmp-server service-port

To configure SNMP service port, use the **snmp-server service-port** command.

Synopsis

(config)# **snmp-server service-port** <port>

Option Description	port	The SNMP server port
Defaults	16	
Command Modes	Global configuration	
Usage Guidelines	Valid port numbers are 161 and from 1024 to 65535. Make sure other services do not use the same port in advance.	
Examples	Specify/modify SNMP service port to 1610. router# configure (config)# snmp-server service-port 1610	
Error Messages	^Parse error	
	^Incomplete command	
	% SNMP service port 162 is invaild, the interval is 161 or from 1024 to 65535 !!! <UINT:service_port> 162	
Related Commands	show snmp	

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>

Option Description	time	hh:mm:ss
	month	1 to 12
	day	1 to 31
	year	2000 to 2037: 32-bit (TI) 2000 to 2069: 64-bit (MARVEL, NXP)
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Time setting. Year range is: 2000 - 2037 on 32-bit (TI) 2000 - 2069 on 64-bit (MARVEL, NXP)	
Examples	34568(config)# clock set 15:33:46 6 3 2026 34568(config)# clock set <STRING:time> - hh:mm:ss 34568(config)# clock set 15:33:46 <UINT:month> - 1 - 12 34568(config)# clock set 15:33:46 6 <UINT:day> - 1 - 31 34568(config)# clock set 15:33:46 6 3 <UINT:year> - 2000 - 2037 34568(config)# clock set 15:33:46 6 3 2026	
Error Messages	% Illegal parameters!	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	When configuring the summer time offset, the start-date and end-date must be configured correctly first.	
Examples	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`	
Error Messages	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	
Related Commands	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 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:

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.
Defaults	GMT+8			
Command Modes	Global configuration			
Usage Guidelines	N/A			
Examples	Set system time zone to GMT+01:00 Paris (same timezone as Brussels). `router# configure` `router(config)# clock timezone gmt 1 city Brussels` `router(config)# exit`			
Error Messages	% Hour offset is out of range.			
	% City Name Error - " "			
	^Parse error			
	^Incomplete command			
Related Commands	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**

Option Description	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
Defaults	The default configuration contains one time server "time.nist.gov".	
Command Modes	Global configuration	
Usage Guidelines	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.	
Examples	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`	
Error Messages	^Parse error	
	^Incomplete command	
	% Maximum length of server 1 is 39	
	% Maximum length of server 2 is 39	
Related Commands	ntp server ntp remote-server-auth ntp authentication-key show ntp-auth-keys	

Clock Source Fallback Mode

ntp server {fallback}

Synopsis

(config)# **ntp server** {fallback}

(config)# **no ntp server** {fallback}

Option Description	fallback	Configures fallback function.
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	1. Enable ntp server fallback 2. Disable no ntp server fallback	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# ntp server fallback`	
Error Messages	N/A	
Related Commands	N/A	

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**]

Option Description	auth	Specifies to enable/disable client authentication
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	Use CLI command **ntp authentication-key** to create the entry for client's authentication.	
Examples	• Enable NTP server and client authentication. `router# configure` `router(config)# ntp server` `router(config)# ntp server auth` `router(config)# exit` • Disable NTP server. `router# configure` `router(config)# no ntp server` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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**}

Option Description	1	Specifies NTP Server 1
	2	Specifies NTP Server 2
	key	Specifies the authentication key ID
	key-id	The key ID, integer ranges from 1 to 65535
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	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.	
Examples	• Specify KeyID(3) to first NTP server. `router# configure` `router(config)# ntp remote-server-auth server 1 key 3` `router(config)# exit` • Disable authentication for first NTP server. `router# configure` `router(config)# no ntp remote-server-auth server 1` `router(config)# exit`	
Error Messages	% Invalid Server, should be (1 | 2).	
	% Invalid key ID for the server, should be 1~65535.	
	^Parse error	
	^Incomplete command	
Related Commands	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>

Option Description	key-id	Key ID, integer ranges from 1 to 65535
	key-type	Specifies a string for key type: {MD5 | SHA512}
	key	Key string. Max. 32 characters
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	• Create KeyID(3) and key type "SHA512" with key string "moxa1234". `router# configure` `router(config)# ntp authentication-key 3 SHA512 moxa1234` `router(config)# exit` • Delete keyID(3) for NTP server authentication. `router# configure` `router(config)# no ntp authentication-key 3` `router(config)# exit`	
Error Messages	% 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	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	clock set clock summer-time clock timezone ntp remote-server ntp server ntp remote-server-auth ntp authentication-key	

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

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

sntp query-interval

To confiture SNTP query intervals, use this command.

Synopsis

(config)# **sntp query-interval** <query_interval>

Option Description	<query_interval>	Specifies the SNTP query interval value as a power of 2. Specify 0 to 13, representing query intervals from 1 second (2^0) to 8192 seconds (2^13).
Defaults	9 (512 sec.)	
Command Modes	Global configuration	
Usage Guidelines	This setting configures how often the SNTP client performs time synchronization queries. Query interval helper: 0: 1 sec., 1: 2 sec., 2: 4 sec., 3: 8 sec., 4: 16 sec., 5: 32 sec., 6: 64 sec., 7: 128 sec., 8: 256 sec., 9: 512 sec., 10: 1024 sec., 11: 2048 sec., 12: 4096 sec., 13: 8182 sec.	
Examples	Configure the default query interval. `router# configure` `router(config)# sntp query-interval 9` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
	% Over length. It must be %s - %s.	
Related Commands	[no] warning-notification system-event ntp-sntp-error active warning-notification system-event ntp-sntp-error severity <UINT:type>	

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}

Option Description	timer	Specifies a timeout value to wait confirmation from the user.
	second	A timeout in seconds, integer rangers 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
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	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.	
Examples	Specify a timer (180 seconds) to check firewall policy. `router# configure` `router(config)# settingcheck timer 180` `router(config)# settingcheck l3l7-policy` `router(config)# exit`	
Error Messages	% Timer range must be 10 - 3600.	
	^Parse error	
	^Incomplete command	
Related Commands	show settingcheck	

show settingcheck

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

Synopsis

show settingcheck

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

Custom Default and Configuration Name

The following commands apply to TN-4900 models only.

Configure/Delete Configuration Name

To configure or delete configuration name, use the following commands.

Synopsis

(config)# **config-name** <string(32)>

(config)# **no config-name** <string(32)>

Option Description	no	Delete entry/reset to default value
	configure-name	Configure the configuration name
	<string(32)>	Configuration name
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Specify/modify configuration name to moxa-test. `router# configure` `router(config)# config-name moxa-test` `router(config)# exit`	
Error Messages	% Invalid string	
	^Parse error	
	^Incomplete command	
Related Commands	reload factory-default show config-name show running-config copy startup-config custom-default reload custom-default	

show config-name

To show the configuration name, use this command.

Synopsis

show config-name

Option Description	show	Display information
	configure-name	Configuration name
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# show config-name` `Current Configuration Name: moxa-test` `Saved Configuration Name: No configuration found!`	
Error Messages	% Invalid string	
	^Parse error	
	^Incomplete command	
Related Commands	show running-config config-name <string(32)>	

copy startup-config custom-default

To copy the startup-configuration custom-default information, use this command.

Synopsis

copy startup-config custom-default

Option Description	startup-config	Designated startup-configuration
	custom-default	Custom-default partition
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# show config-name` `Current Configuration Name: moxa-test` `Saved Configuration Name: No configuration found!` `router# copy startup-config custom-default` `router# show config-name` `Current Configuration Name: moxa-test` `Saved Configuration Name: moxa-test`	
Error Messages	% Invalid string	
	^Parse error	
	^Incomplete command	
Related Commands	show running-config config-name <string(32)> reload custom-default	

reload custom-default

To reload the custom-default value, use this command.

Synopsis

reload custom-default

Option Description	reload	Reload the information
	custom-default	Custom-default partition
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	Only workable when startup config had been saved as custom default before.	
Examples	`router# reload custom-default` `Proceed with reload to custom default? [Y/n]`	
Error Messages	% Invalid string: The specified custom-default configuration does not exist.	
	^Parse error	
	^Incomplete command	
Related Commands	Copy startup-config custom-default reload custom-default	

cli-mode port-naming

To create a consistent port identification method, use this command.

Synopsis

(config)# **cli-mode port-naming** { logical | panel }

Option Description	logical	Display port names in logical port format (1/1, 1/2, 1/16)
	panel	Display port names as labeled on the device panel (1, 2, G1, G3)
Defaults	logical	
Command Modes	Privileged EXEC / Global configuration	
Usage Guidelines	N/A	
Examples	`Firewall/ETBN Router 00000# show interfaces ethernet` `Port Link Type Description Speed FDX Flow Ctrl MDI/MDIX` `---- ----- ---------- ---------- --------- ------ ----` `1/1 Down 1000TX -- -- --` `1/2 Down 1000TX -- -- --` `1/3 Down 100TX -- -- --` `1/4 Up 100TX 100M-Full Off MDI` `1/5 Down 1000TX -- -- --` `1/6 Down 1000TX -- -- --` `1/7 Down 100TX -- -- --` `1/8 Down 100TX -- -- --` `Firewall/ETBN Router 00000# configure` `Firewall/ETBN Router 00000(config)# cli-mode port-naming panel` `Firewall/ETBN Router 00000(config)# exit` `Firewall/ETBN Router 00000# show interfaces ethernet` `Port Link Type Description Speed FDX Flow Ctrl MDI/MDIX`	

	---- ----- ---------- ---------- --------- ---------- G1 Down 1000TX -- -- G2 Down 1000TX -- -- 1 Down 100TX -- -- 2 Up 100TX 100M-Full Off MDI G3 Down 1000TX -- -- G4 Down 1000TX -- -- 3 Down 100TX -- -- 4 Down 100TX -- --
Error Message	^Parse error
	^Incomplete command
Related Commands	show cli-mode port-naming

show cli-mode port-naming

Synopsis

show cli-mode port-naming

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	Firewall/ETBN Router 00000# show cli-mode port-naming Port Naming: Panel mode	
	^Parse error	
	^Incomplete command	
Related Commands	cli-mode port-naming	

Software Package Management

show package status

To show packages status, use **show package status** command.

Synopsis

show package status

Option Description	show package status	Show package status
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# show package status` `Package security is enable.(v10.0.21)` `Package mxsecurity is enable.(v3.0.6)`	
Error Messages	^Parse error	
Related Commands	N/A	

package install

To install the package via tftp, use **package install** command. This command can only be used when the package has not been installed.

Synopsis

package install { security | mxsecurity } **tftp** <IPV4ADDR:tftp_ip> <STRING:filename>

Option Description	package install	Install the package
	security	Security Package
	mxsecurity	Mxsecurity Agent Package
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# package install security tftp 192.168.127.115 Security_EDR-G9010_V3.0.14_Build_21122710.pkg Install security package(Security_EDR-G9010_V3.0.14_Build_21122710.pkg) from TFTP Server IP 192.168.127.115 Package transferring... Verified OK Checking Package...All checking are ok. Package is importing now, please wait! Package installed successfully.	
Error Messages	^Parse error	
	Package name is not support.	
	% Invalid parameter!	
	Install failed.	
Related Commands	show package status	

package upgrade

To upgrade the package via tftp, use **package upgrade** command. This command can only be used when the package has been installed.

Synopsis

package upgrade { security | mxsecurity } **tftp** <IPV4ADDR:tftp_ip> <STRING:filename>

Option Description	package upgrade	Upgrade the package
	security	Security Package
	mxsecurity	Mxsecurity Agent Package
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# package upgrade security tftp 192.168.127.115 Security_EDR-G9010_V3.0.14_Build_21122710.pkg Upgrade security package(Security_EDR-G9010_V3.0.14_Build_21122710.pkg) from TFTP Server IP 192.168.127.115 Package transfering... Verified OK Checking Package...All checking are ok. Package is importing now, please wait! Package upgrade successfully.	

Error Messages	^Parse error
	Package name is not support.
	% Invalid parameter!
	Install failed.
Related Commands	show package status

package uninstall

To uninstall the package, use **package uninstall** command. This command can only be used when the package has been installed.

Synopsis

package uninstall { security | mxsecurity }

Option Description	package uninstall	Uninstall the package
	security	Security Package
	mxsecurity	Mxsecurity Agent Package
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# package uninstall security` `Uninstall security package...` `Package uninstall successfully.`	
Error Messages	^Parse error	
	Uninstall failed, package is not supported uninstall.	
Related Commands	show package status	

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}

Option Description	banner	Specifies banner
	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.
Defaults	Empty string.	
Command Modes	Global configuration	
Usage Guidelines	• Maximum length of text-banner or text-fail-message is 512. • The text string comprises characters including **a-z, A-Z, 0-9 or . , - _ @ ! # $ % ^ & * ( ).** Uses **** instead to represent a whitespace character.	
Examples	• 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` • Specify/modify the fail-message to "Login Failed". `router# configure` `router(config)# aaa authentication fail-message Login\\Failed` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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}]

Option Description	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.
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	This command applies to telnet, SSH and the web interface.	
Examples	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`	
Error Messages	% login lockout threshold should between 1~10	
	^Parse error	
	^Incomplete command	
	show running-configuration	
Related Commands		

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>

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

Trusted Access

interface trusted-access (IP Address Allowlist)

To specify or modify the IP list allowlist, 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} |
<ipv6> <prefix_len> {enable | disable}}]

(config)# **no interface trusted-access** [{**lan** |
<ip> <netmask> |
<ipv6> <prefix_len>}]

Option Description	lan	Specifies LAN interface.
	ip	IP address.
	netmask	Subnet mask for this IPv4 address.
	enable	Enables specified accessible IPv4/IPv6 address.
	disable	Disables specified accessible IPv4/IPv6 address.
	ipv6	IPv6 address.
	prefix_len	Prefix length for this IPv6 address.
Defaults	Accessible IP list is enabled by default. Accept all connection from LAN port is enabled by default.	
Command Modes	Global configuration	
Usage Guidelines	When the accessible IP list is enabled, only addresses on the list will be allowed access to the router. To configure Trusted Access for IPv6, enable IPv6 Global Option first.	
Examples	• Disable trusted-access to allow connection from all IP addresses. `router# configure` `router(config)# no interface trusted-access.` `router(config)# exit` • 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` • Specify 2001::1/64 can access this router. `router# configure` `router(config)# interface trusted-access 2001::1 64 enable`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show interfaces trusted-access settingcheck ipv6 global-option	

interface trusted-access (Service Allowlist)

To specify or modify services on the service allowlist, use the **interface trusted-access** global configuration command. To disable trusted access, use the **no** form of this command.

Synopsis

(config)# **interface trusted-access** <ip> <netmask>

(config-trustAccess)# name <name>

(config-trustAccess)# service [{ all |
web|
cli|
snmp|
mxservice}]

(config-trustAccess)# **no service** [{ all|
web|
cli|
snmp|
mxservice}]

(config-trustAccess)# **interface** <interface_name>

Option Description	name	Specifies a name for the Trusted Access entry.
	service	Management services for the Trusted Access entry.
	all	All management services for the Trusted Access entry.
	web	Web management services (HTTP/HTTPS).
	cli	CLI management services (SSH/Telnet).
	snmp	SNMP service.
	mxservice	MOXA proprietary management service. (IPv6 not supported)
	interface	Specifies the incoming interface for the Trusted Access entry.
	interface_name	Interface Name
Command Modes	Trusted Access submode	
Usage Guidelines	• When a Trusted Access rule is configured, only the specified services will be allowed if explicitly defined. • The service `all` option overrides all individual service selections. • The no service commands remove specific services from the allowlist. • If no service is specified, the system shall treat it as allowing all services. • The interface option restricts access to connections originating from the specified interface. • Multiple service commands can be used to enable multiple management services (multi-select behavior).	
Examples	Allow all services for a specific IP `router# configure` `router(config)# interface trusted-access 192.168.127.10 255.255.255.0` `router(config-trusted_access)# service Any` Allow only Web and CLI access `router# configure` `router(config)# interface trusted-access 192.168.127.10 255.255.255.0`	

	router(config-trusted_access)# service Web router(config-trusted_access)# service CLI Allow SNMP only and restrict interface router# configure router(config)# interface trusted-access 192.168.127.10 255.255.255.0 router(config-trusted_access)# service SNMP router(config-trusted_access)# interface LAN1 Remove specific service router(config-trusted_access)# no service Web Save and Exit port-based bridge interface configuration (config-trustAccess)# exit
Error Messages	Invalid system symbol
	vlan interface is invalid
Related Commands	show interfaces trusted-access

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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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` `Index State IPv6 Prefix Length` `----- ------- --------------- --------------------` `1 Disable 2001::1 64`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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

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

sshkeygen

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

Synopsis

sshkeygen

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

Option Description	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.
Defaults	local	
Command Modes	Global configuration	
Usage Guidelines	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.	
Examples	Authentication occurs sequentially in RADIUS and then locally. `router# configure` `router(config)# auth mode radius local` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show auth radius auth radius auth tacacs	

auth radius

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

When the authentication server is set to the local RADIUS server, the original content entered for the authentication server will be cleared.

If the primary auth server is first set to the local RADIUS server, and then the backup auth server is also set to the local RADIUS server, the primary auth server will no longer be set as the local RADIUS server and will revert to default value.

Synopsis

(config)# **auth radius {server** {<server-index> {<server-ip> port <server-port> key <shared-key>} |
primary <server-ip> port <server-port> key <shared-key>|
backup <server-ip> port <server-port> key <shared-key>|
local-radius-server {<server-index> | primary | backup}} |
auth-type {pap |
chap |
peap-mschapv2}}
(config)# **no auth radius server {primary | backup}**

Option Description	**Radius**	Specifies remote RADIUS authentication.
	server	Specifies RADIUS primary or backup servers.
	server-index	Specifies index of RADIUS authentication servers, integer ranges from 1 to 2.
	primary	Specifies primary RADIUS authentication server.
	local-radius-server	Specifies local RADIUS 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.
	key	Specifies a shared-key of the remote RADIUS Server.
	shared-key	Shared key of the RADIUS authentication server.
	backup	Specifies backup RADIUS authentication server.
	auth-type	Specifies type of authentication.
	pap	PAP.
	chap	CHAP.
	peap-mschapv2	PEAP-MSCHAPv2.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	<shared-key>: Max number of characters is 64. <shared-key>: Characters restricted to: • a to z • A to Z • 0 to 9 • Special characters _@!#$%&*().-+={}[]|:;,~, • Cannot contain spaces	
Examples	`Specify and enable the primary remote RADIUS server (192.168.1.5), port (2812) and shared key (radius-key).` `router# configure` `router(config)# auth radius server primary 192.168.1.5 port 2812 key radius-key` `router(config)# auth mode radius` `router(config)# exit` `Specify the first RADIUS server to local RADIUS server.` `router# configure` `router(config)# auth radius server local-radius-server primary` `router(config)# auth mode radius` `router(config)# exit`	
Error Messages	% Radius index must be 1~2	

	% Not in correct format !!! <STRING:server_ip> XXX
	% Over length. It must be 0 - 63 !!! <STRING:server_ip> XXX
	% Over length. It must be 1 - 65535 !!! <UINT:server_port> X
	% Invalid system symbol !!! <STRING:server_key> XXX
	% Over length. It must be 0 - 64 !!! <STRING:server_key> XXX
	^Parse error
	^Incomplete command
Related Commands	show auth radius auth mode

show auth radius

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

Synopsis

show auth radius

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

Option Description	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 - @ ! # $ % & * ( ) . + = { } [ ] | : ; , ~, and no spaces are allowed.
	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
Defaults	N/A	
Command Modes	Global	
Usage Guidelines	N/A	
Examples	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). `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`	
Error Messages	% Invalid parameter!	
	% Port must be greater than 0 and smaller than 65536	
	% Over length. It must be 0 - 64 !!! <STRING:server_key> X	
	% Timeout must be 5~120	
	% Retransmit must be 0~5	
	^Parse error	
	^Incomplete command	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	auth mode auth tacacs	

LDAP

auth mode ldap local

To configure LDAP with a local fallback database, use the **auth mode ldap local** global configuration command.

Synopsis:

(config)# **auth mode ldap** {local}

Option Description	local	(Optional) Local Account Database
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	Use Local Account Database if cannot connect to LDAP Server.	
Examples	`router# configure` `router(config)# auth mode ldap local` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

no auth ldap

To disable LDAP and clear all settings, use the **no auth ldap** global configuration command.

Synopsis:

(config)# **no auth ldap** {<serveridx>}

Option Description	<serveridx>	(Optional) LDAP Auth instance index to clear all settings (e.g. 1 to 2). Defaults to 1 and 2 if serveridx is not provided.
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	Clears all settings of the specified LDAP Auth instance.	
Examples	`router# configure` `router(config)# no auth ldap 1` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

auth ldap serveridx

To configure a specified LDAP service index, use the **auth ldap serveridx** global configuration command.

Synopsis:

(config)# **auth ldap** <serveridx>

Option Description	<serveridx>	LDAP Auth instance index (e.g. 1–2)
Defaults	#	
Command Modes	Global configuration + enter ldap sub mode	
Usage Guidelines	Creates or selects the specified LDAP Auth instance and enters LDAP submode.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap exit

To leave the LDAP Auth submode, use the **exit** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **exit**

Option Description	exit	Exit LDAP authentication submode
Defaults	#	
Command Modes	LDAP mode configuration	
Usage Guidelines	Exits LDAP Auth submode and returns to global configuration mode.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# exit` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap disable

To disable the LDAP instance, use the **disable** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **disable**

Option Description	disable	Disable the LDAP authentication instance.
Defaults	#	
Command Modes	LDAP mode configuration	
Usage Guidelines	Disables the specified LDAP Auth instance.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# disable` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap enable

To enable the LDAP instance, use the **enable** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **enable**

Option Description	enable	Enable the LDAP authentication instance.
Defaults	#	
Command Modes	LDAP mode configuration	
Usage Guidelines	Enables the specified LDAP Auth instance.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# enable` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap server

To specify the LDAP server, use the **server** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **server** <host>

Option Description	server <host>	Specify LDAP server hostname or IP address.
Defaults	#	
Command Modes	LDAP mode configuration	
Usage Guidelines	Configures the LDAP server address.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# server 192.168.1.100` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap port

To specify the LDAP server port, use the **port** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# port <port>

Option Description	<port>	Specify LDAP server port number (e.g. 1 to 65535)
Defaults	389	
Command Modes	LDAP mode configuration	
Usage Guidelines	Configures the LDAP server port number.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# port 389` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap conn-enc none

To disable LDAP encryption, use the **conn-enc none** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **conn-enc none**

Option Description	none	No encryption; use plaintext LDAP connection.
Defaults	conn-enc none	
Command Modes	LDAP mode configuration	
Usage Guidelines	Sets connection encryption to none. The LDAP connection will not use TLS.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# conn-enc none` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap conn-enc ssl

To enable SSL LDAP encryption, use the **conn-enc ssl** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **conn-enc** ssl {ca <file>} {tls-verify}

Option Description	ssl	Use LDAPS (TLS from connection start, typically port 636)
	ca <file>	(Optional) CA certificate file for server verification
	tls-verify	(Optional) Enforce strict TLS certificate verification
Defaults	conn-enc none	
Command Modes	LDAP mode configuration	
Usage Guidelines	Sets connection encryption to SSL (LDAPS). A CA certificate may optionally be specified. When tls-verify is set, the server certificate is validated against the CA.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# conn-enc ssl` `router(config-ldap)# conn-enc ssl ca ca.crt tls-verify` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap conn-enc starttls

To enable STARTTLS LDAP encryption, use the **conn-enc starttls** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **conn-enc** starttls {ca <file>} {tls-verify}

Option Description	starttls	Upgrade plaintext connection to TLS using STARTTLS (typically port 389).
	ca <file>	(Optional) Specify a CA certificate file for server verification.
	tls-verify	(Optional) Enforce strict TLS certificate verification.
Defaults	conn-enc none	
Command Modes	LDAP mode configuration	
Usage Guidelines	Sets connection encryption to STARTTLS. The connection starts as plaintext and is upgraded to TLS. A CA certificate may optionally be specified.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# conn-enc starttls` `router(config-ldap)# conn-enc starttls ca ca.crt tls-verify` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap timeout

To specify an LDAP connection timeout, use the **timeout** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **timeout** <timeout>

Option Description	<timeout>	Connection timeout in seconds (e.g. 1–120)
Defaults	5	
Command Modes	LDAP mode configuration	
Usage Guidelines	Configures the LDAP connection timeout. If the server does not respond within this time, the connection is considered failed.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# timeout 10` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap retry

To specify LDAP connection retry attempts, use the **retry** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# retry <retry>

Option Description	<retry>	Specify number of retry attempts when the LDAP server is unreachable (e.g. 0 to 5).
Defaults	1	
Command Modes	LDAP mode configuration	
Usage Guidelines	Configures the number of retry attempts for failed LDAP connections.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# retry 3` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap base-dn

To specify an LDAP Base Distinguish Name used as a search root, use the **base-dn** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **base-dn** <dn>

Option Description	<dn>	Specify a Base Distinguished Name used as the search root (e.g. dc=example,dc=com).
Defaults	#	
Command Modes	LDAP mode configuration	
Usage Guidelines	Configures the LDAP base DN. All user searches are performed under this DN.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# base-dn dc=example,dc=com` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap auth-upn

To use LDAP UPN direct bind authentication, use the **auth-upn** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **auth-upn** {domain <domain>}

Option Description	auth-upn	Use UPN (User Principal Name) direct bind authentication
	domain <domain>	(Optional) Specify a domain suffix appended to the username to form the UPN (e.g. example.com → user@example.com)
Defaults	auth-upn	
Command Modes	LDAP mode configuration	
Usage Guidelines	Sets authentication mode to UPN bind. The device binds directly to LDAP using username@domain without prior DN lookup. Recommended for Active Directory environments that do not permit anonymous queries.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# auth-upn domain example.com` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap auth-two-phase-bind bind-dn

To use LDAP two-phase bind authentication, use the **auth-two-phase-bind bind-dn** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **auth-two-phase-bind bind-dn** <dn> bind-pwd < pwd> {username-attr < attr>}

Option Description	auth-two-phase-bind	Use 2 phase bind authentication.
	bind-dn <dn>	Specify the bind DN of the read-only service account used to search for the user entry.
	bind-pwd <pwd>	Specify the password of the bind DN account.
	username-attr <attr>	(Optional) Specify the LDAP attribute to match against the login username (e.g. uid, sAMAccountName), default is uid.
Defaults	auth-upn	
Command Modes	LDAP mode configuration	
Usage Guidelines	Sets authentication mode to bind-and-search. The device first binds using the specified service account to locate the user DN, then re-binds using the user's own credentials to verify the password.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# auth-two-phase-bind bind-dn cn=readonly,dc=example,dc=com bind-pw secret username-attr uid` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ldap auth-direct-user-bind

To use LDAP direct user bind authentication, use the **auth-direct-user-bind** LDAP authentication submode configuration command.

Synopsis:

(config-ldap)# **auth-direct-user-bind** {username-attr <attr>}

Option Description	auth-direct-user-bind	Use direct user bind authentication.
	username-attr <STRING:attr>	(Optional) LDAP attribute to match against the login username (e.g. uid, sAMAccountName), default is uid
Defaults	auth-upn	
Command Modes	LDAP mode configuration	
Usage Guidelines	Sets authentication mode to direct user bind. The device binds directly to LDAP using (username-attr)=username,(base-DN) without prior DN lookup.	
Examples	`router# configure` `router(config)# auth ldap 1` `router(config-ldap)# auth-direct-user-bind username-attr uid` `router(config-ldap)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

auth ldap role-mapping list

To display all LDAP role mapping entires, use the **auth ldap role-mapping list** privileged EXEC configuration command.

Synopsis:

(config)# **auth ldap role-mapping list**

Option Description	list	Display all LDAP role mapping entries.
Defaults	#	
Command Modes	Privileged EXEC	
Usage Guidelines	Displays all configured LDAP role mapping entries, including index, type, parameter, assigned role, and enable/disable status.	
Examples	`router# configure` `router(config)# auth ldap role-mapping list` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

auth ldap role-mapping matching-policy

To specify LDAP role assignment policy, use the **auth ldap role-mapping matching-policy** privileged EXEC configuration command.

Synopsis:

(config)# **auth ldap role-mapping matching-policy** <policy>

Option Description	<policy>	Specify a policy to assign on matching policy: first-hit | highest-privilege
Defaults	auth ldap role-mapping matching-policy first-hit	
Command Modes	Privileged EXEC	
Usage Guidelines	Role mapping entries matching policy. The first-hit takes the first rule that matches your profile and ignores the rest. The highest-privilege checks all matching rules and gives you the highest rank (most power).	
Examples	`router# configure` `router(config)# auth ldap role-mapping matching-policy first-hit` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

auth ldap role-mapping matching-policy

To specify LDAP role assignment policy, use the **auth ldap role-mapping matching-policy** global configuration command.

Synopsis:

(config)# **auth ldap role-mapping** {index <index>} privilege <privilege> attribute <parameter> {disable}

Option Description	index <index>	(Optional) Specify a role mapping entry insertion index (1–16)，Append to the end if index is not provided.
	privilege <privilege>	Specify the privilege to assign on match: admin | supervisor | user
	attribute <parameter>	Value to match
	disable	(Optional) Create the entry in disabled state; default is enabled
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	Creates or updates an LDAP role mapping entry. When a user authenticates via LDAP, the device evaluates all enabled role mapping entries in index order.	
Examples	router# configure router(config)# auth ldap role-mapping index 1 privilege admin attribute memberOf=cn=vpnusers,ou=Group,dc=example,dc=com router(config)# exit	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

no auth ldap role-mapping

To delete LDAP role mapping settings, use the **no auth ldap role-mapping** global configuration command.

Synopsis:

(config)# **no auth ldap role-mapping** {index < index>}

Option Description	index <index>	(Optional) Specify the index of the role mapping entry to delete. Default to delete all if index is not provided.
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	Permanently deletes the specified LDAP role mapping entry.	
Examples	`router# configure` `router(config)# no auth ldap role-mapping index 1` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

auth ldap role-mapping index disable

To disable an LDAP role mapping entry, use the **auth ldap role-mapping index disable** global configuration command.

Synopsis:

(config)# **auth ldap role-mapping** {index <index>} disable

Option Description	index <index>	(Optional) Specify the index of the role mapping entry to disable. Default to disable all if index is not provided.
	disable	Disable the specified role mapping entry
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	Disables the specified LDAP role mapping entry. The entry is retained but not evaluated during authentication.	
Examples	`router# configure` `router(config)# auth ldap role-mapping index 1 disable` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

auth ldap role-mapping enable

To enable an LDAP role-mapping entry, use the **auth ldap role-mapping index enable** global configuration command.

Synopsis:

(config)# **auth ldap role-mapping** {index <index>} **enable**

Option Description	index <index>	(Optional) Index of the role mapping entry to enable. Default to enable all if index is not provided.
	enable	Enable the specified role mapping entry
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	Enables the specified LDAP role mapping entry.	
Examples	`router# configure` `router(config)# auth ldap role-mapping index 1 enable` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

auth ldap test

To test LDAP authentication, use the **auth ldap test** global configuration command.

Synopsis:

(config)# **auth ldap test** <serveridx> **username** <username> **password** <password>

Option Description	<serveridx>	Specify the index of the LDAP Auth instance to test settings (e.g. 1 to 2).
	username <username>	Specify the user name used for LDAP test.
	password <password>	Specify the password for the LDAP test.
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	Test the specified LDAP server authentication.	
Examples	`router# configure` `router(config)# auth ldap test 1 username testuser password testpassword` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

show auth ldap

To show LDAP authentication configuration, use the **show auth ldap** global configuration command.

Synopsis:

show auth ldap

Option Description	show	Display all configured LDAP.
Defaults	#	
Command Modes	Privileged EXEC	
Usage Guidelines	Displays all configured LDAP.	
Examples	`router# show auth ldap`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

show auth ldap role-mapping

To show LDAP authentication configuration, use the **show auth ldap** global configuration command.

Synopsis:

show auth ldap role-mapping

Option Description	show	Display all configured LDAP role mapping entry
Defaults	#	
Command Modes	Privileged EXEC	
Usage Guidelines	Displays all configured LDAP role mapping entries.	
Examples	`router# show auth ldap role-mapping`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

2FA

2fa

To enable 2FA, use the **2fa** global configuration command. To disable 2FA device-wide, use the **no** form of this command.

Synopsis:

(config)# [no] **2fa**

Option Description	2fa	Configure 2-Factor Authentication.
	no	Reset 2fa to default values.
Defaults	Disable	
Command Modes	Global configuration	
Usage Guidelines	Determine the Desired Action: Decide whether you want to enable or disable the 2FA mode.	
Examples	Enable 2FA. `router# configure` `router(config)# 2fa` `router(config)# exit` Disable 2FA. `router# configure` `router(config)# no 2fa` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show users username <name> password <pwd-string> [privilege <privilege>] username <name> 2fa <mode> username <name> 2fa type { totp [secret <code> recovery <code>] | email <email-address> [recovery <code>] } 2fa { http | https | telnet | ssh } { disable | enable } 2fa totp-timeout <timeout> 2fa totp-tolerance { enable | disable } 2fa algorithm { SHA1 | SHA256 | SHA512 } 2fa { http | https | telnet | ssh } { disable | enable } show 2fa	

2fa totp-timeout

To configure the timeout of TOTP codes for all accounts using 2FA, use the type **2fa totp-timeout** global configuration command.

Synopsis:

(config)# **2fa totp-timeout** <timeout>

Option Description	2fa	2-Factor Authentication
	totp-timeout	Global TOTP timeout setting for all account using 2FA type - totp.
	timeout	Specify timeout value in seconds. Default 30 seconds. This parameter only applies to TOTP and is not used for email-based 2FA. Valid range: 30 to 120 seconds.
Defaults	timeout-seconds: 30	
Command Modes	Global configuration	
Usage Guidelines	Determine the Desired Timeout Value: Decide the timeout value in seconds for TOTP codes. Execute the Command: Use the command format to set the desired timeout value for TOTP codes.	

	Verify the Configuration: Ensure that the TOTP timeout value has been correctly set by checking the system's 2FA settings. Note the Scope: Remember that this parameter only applies to TOTP and is not used for email-based 2FA.
Examples	Set TOTP timeout. `router# configure` `router(config)# 2fa totp-timeout 60` `router(config)# exit`
Error Messages	% Over length. It must be %s - %s
	^Parse error
	^Incomplete command
Related Commands	show users username <name> password <pwd-string> [privilege <privilege>] username <name> 2fa <mode> username <name> 2fa type { totp [secret <code> recovery <code>] | email <email-address> [recovery <code>] } [no] 2fa 2fa { http | https | telnet | ssh } { disable | enable } 2fa totp-tolerance { enable | disable } 2fa algorithm { SHA1 | SHA256 | SHA512 } 2fa { http | https | telnet | ssh } { disable | enable } show 2fa

2fa totp-tolerance

To enable or disable the tolerance for TOTP code timeout, use the **2fa totp-tolerance** global configuration command.

Synopsis:

(config)# **2fa totp-tolerance** { enable | disable }

Option Description	2fa	2-Factor Authentication
	totp-tolerance	Global TOTP timeout tolerance setting for all account using 2FA type - totp
	enable	Enables tolerance. The system will validate the TOTP codes for the previous, current, and next time windows. If any of these three codes is correct, the authentication is accepted.
	disable	Disables tolerance. The system strictly validates only the TOTP code generated for the current time window.
Defaults	Enable	
Command Modes	Global configuration	
Usage Guidelines	Purpose: This command is used to compensate for slight time synchronization drifts between the system and the user's authenticator device. Default Behavior: The default setting is enable, which increases fault tolerance and improves user experience by accepting codes from adjacent time windows (±1 step). Security Consideration: While enabling tolerance reduces login failures caused by minor time delays, disabling it (disable) provides stricter security by ensuring the code is only valid within its exact time window. Scope: This setting applies globally to all accounts using the TOTP 2FA method.	
Examples	Set TOTP timeout tolerance to disable. `router# configure` `router(config)# 2fa totp-tolerance disable` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show users username <name> password <pwd-string> [privilege <privilege>] username <name> 2fa <mode> username <name> 2fa type { totp [secret <code> recovery <code>] | email <email-	

	address> [recovery <code>] } [no] 2fa 2fa totp-timeout <timeout> 2fa { http | https | telnet | ssh } { disable | enable } 2fa algorithm { SHA1 | SHA256 | SHA512 } show 2fa

2fa (Service)

To configure the services that use 2FA, use the **2fa (Service)** global configuration command.

Synopsis:

(config)# **2fa** { http | https | telnet | ssh } { disable | enable }

Option Description	2fa	2-Factor Authentication
	http	Toggle 2FA for HTTP.
	https	2FA for the specified services HTTPS.
	telnet	2FA for the specified services Telent.
	ssh	2FA for the specified services SSH.
	disable	Disables 2FA for the specified services.
	enable	Enables 2FA for the specified services.
Defaults	All disabled	
Command Modes	Global configuration	
Usage Guidelines	Determine the Desired Action: Decide whether you want to enable or disable the 2FA service for a specific protocol. Execute the Command: Use the command format to set the desired 2FA service for the specified protocol. Verify the Configuration: Ensure that the 2FA service has been correctly set by checking the system's 2FA settings. Permissions: Ensure that users who need to change 2FA settings have the necessary permissions to do so.	
Examples	Enable service http. `router# configure` `router(config)# 2fa http enable` `router(config)# exit` Disable service http. `router# configure` `router(config)# 2fa http disable` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show users username <name> password <pwd-string> [privilege <privilege>] username <name> 2fa <mode> username <name> 2fa type { totp [secret <code> recovery <code>] | email <email-address> [recovery <code>] } [no] 2fa 2fa totp-timeout <timeout> 2fa totp-tolerance { enable | disable } 2fa algorithm { SHA1 | SHA256 | SHA512 } show 2fa	

2fa algorithm

To configure the algorithm that generates 2FA codes, use the **2fa algorithm** global configuration command.

Synopsis:

(config)# **2fa algorithm** { SHA1 | SHA256 | SHA512 }

	2fa	Configure 2-Factor Authentication.

Option Description	algorithm	Configure 2FA Algorithm.
	SHA1	Specify SHA1 Algorithm.
	SHA256	Specify SHA256 Algorithm.
	SHA512	Specify SHA512 Algorithm.
Defaults	SHA1	
Command Modes	Global configuration	
Usage Guidelines	Changing the algorithm may require users to re-configure their authenticator, depending on implementation. It is recommended to use SHA256 or SHA512 for stronger security, unless compatibility with older authenticators requires sha1.	
Examples	Set 2FA algorithm to SHA1 `router# configure` `router(config)# 2fa algorithm SHA1` `router(config)# exit` Set 2FA algorithm to SHA256 `router# configure` `router(config)# 2fa algorithm SHA256` `router(config)# exit` Set 2FA algorithm to SHA512 `router# configure` `router(config)# 2fa algorithm SHA512` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show users username <name> password <pwd-string> [privilege <privilege>] username <name> 2fa <mode> username <name> 2fa type { totp [secret <code> recovery <code>] | email <email-address> [recovery <code>] } [no] 2fa 2fa totp-timeout <timeout> 2fa totp-tolerance { enable | disable } 2fa { http | https | telnet | ssh } { disable | enable } show 2fa	

show 2fa

To show 2FA settings, used the **show 2fa** command.

Synopsis:

show 2fa

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	Show 2FA Current Setting `router# show 2fa` `Status: Enabled` `Applied Service:` `  HTTP:  Enabled` `  HTTPS:  Enabled` `  TELNET: Enabled` `  SSH:  Enabled` `TOTP Code Timeout:`	

	30 seconds TOTP Timeout Tolerance: 0 step
Error Messages	^Parse error
	^Incomplete command
Related Commands	show users username <name> password <pwd-string> [privilege <privilege>] username <name> 2fa <mode> username <name> 2fa type { totp [secret <code> recovery <code>] | email <email-address> [recovery <code>] } [no] 2fa 2fa totp-timeout <timeout> 2fa totp-tolerance { enable | disable } 2fa { http | https | telnet | ssh } { disable | enable } show 2fa

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**

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

dot1x radius

To specify or modify warning notification for RADIUS server events, use the **warning-notification system-event** global configuration command.

To return to default settings, use the **no** form of this command.

Synopsis

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

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

Option Description	**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.
	shared-key	Specifies the shared key of the RADIUS authentication server.
	key	Shared key.
	local-radius-server	Specifies local RADIUS server.
	both	Disables both first and second RADIUS servers.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	<key> Max number of characters is 64. <key> Only can contain the letters a-z, A-Z, numbers 0-9 and special characters _@!#$%&*().-+={}[]|:;,~, and cannot have any spaces.	
Examples	`Specify the first RADIUS server (192.168.1.6), port (3812) and shared key (radiuskey).` `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 radiuskey` `router(config)# exit` `Specify the first RADIUS server to local RADIUS server.` `router# configure` `router(config)# dot1x radius 1st-server local-radius-server` `router(config)# exit`	
Error Messages	% Not in correct format !!! <IPV4ADDR:server_ip> X.X.X.X	
	% Over length. It must be 1 - 65535 !!! <UINT:server_port> X	
	% Invalid system symbol !!! <STRING:server_key>	
	% Over length. It must be 0 - 64 !!! <STRING:server_key> X	
	^Parse error	
	^Incomplete command	
Related Commands	show dot1x show dot1x all show dot1x interfaces show dot1x local-userdb show dot1x radius	

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}

Option Description	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.
Defaults	Local	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Specify Radius server as database for authentication. `router# configure` `router(config)# dot1x auth radius` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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>

Option Description	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 - _ @ ! # $ % & * ( ) . + = { } [ ] | : ; , ~, and no spaces are allowed.
Defaults	Local	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	% Username is not in database	
	% Username or password exceed maximum length	
	^Parse error	
	^Incomplete command	
Related Commands	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** <UNIT: <second>]

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

Option Description	period	Specify the re-authentication period (in seconds).
	second	Ranges from 60 to 65535 seconds
Defaults	3600	
Command Modes	Global configuration	
Usage Guidelines	Enables re-auth before specifies re-authentication period.	
Examples	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`	
Error Messages	% Over length. It must be 60 - 65535 !!! <UINT:seconds> X	
	^Parse error	
	^Incomplete command	
Related Commands	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}]

Option Description	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
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`router # show dot1x` `Dot1x Info` `Database Option : RADIUS Server` `Re-Auth : Enable` `Re-Auth Period : 3600` `1st Auth server`	

	`` ---------------------- IP/name : Local RADIUS server Port : **** Shared key : ******** 2nd Auth server ---------------------- IP/name : 192.168.127.253 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 router # show dot1x local-userdb Index User Name ----- -------------------- 1 test ```
Error Messages	^Parse error
	^Incomplete command
	% Illegal parameter
	% Unavailable module
Related Commands	dot1x radius dot1x auth dot1x local-userdb dot1x reauth

RADIUS Server Configuration

radius-server enable

To configure RADIUS Server, use the **radius-server enable** global configuration command. To disable RADIUS Server, use the **no** form of this command.

Synopsis

(config)# **radius-server** enable

(config)# **no radius-server** enable

Option Description	**radius-server**	Configure RADIUS server
	enable	Enables the RADIUS server.
Defaults		
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	N/A	
Error Messages	^Parse error	
	^Incomplete command	

Related Commands	show radius-server show dot1x all show radius-server clientdb show radius-server userdb

show radius-server clientdb

To check the client table of RADIUS server, use the **show radius-server clientdb** command.

Synopsis

(config)# **show radius-server clientdb**

Option Description	N/A
Defaults	N/A
Command Modes	Privileged EXEC / User EXEC
Usage Guidelines	N/A
Examples	router# show radius-server clientdb RADIUS Server Client List Index Status Client Name IP Address Subnet Mask ----- ------ ----------- --------------- ------------- 1 Enable client1 192.168.127.254 255.255.255.0
Error Messages	^Parse error
	^Incomplete command
Related Commands	radius-server client <clientname> { ip <ipaddr> netmask <subnetmask> sharekey <key> | enable | disable } no radius-server client <clientname>

show radius-server userdb

To check the user table of RADIUS server, use the **show radius-server userdb** command.

Synopsis

(config)# **show radius-server clientdb**

Option Description	N/A
Defaults	N/A
Command Modes	Privileged EXEC / User EXEC
Usage Guidelines	N/A
Examples	router# show radius-server userdb RADIUS Server Authentication User List Index Status User Name Authority ------ -------- -------------------- ---------- 1 Enable user1 System admin 2 Disable user2 User
Error Messages	^Parse error
	^Incomplete command
Related Commands	radius-server user <username> { password <key> authority <authority-level> | enable | disable } no radius-server user <username>

radius-server client

To add or modify allowed RADIUS client for RADIUS server, use the **radius-server client** command.

To delete a client from the client database, use the **no** form of this command.

Synopsis

(config)# **radius-server**
client <clientname> { ip <ipaddr> netmask <subnetmask> sharekey <key> | enable | disable }

(config)# **no radius-server client <clientname>**

Option Description	**client**	Specifies RADIUS client name in client database.
	clientname	RADIUS client name in the client database, max length is 30 characters.
	ip	Specifies the RADIUS client ip address.
	ipaddr	The IP address of the RADIUS client ip address, the ip shall be unicast.
	netmask	Specify the subnet mask for this IP address to allow all RADIUS clients within the subnet to authenticate through this RADIUS server.
	subnetmask	Subnet mask for this IP address.
	sharekey	Specifies the shared key of the RADIUS client.
	key	Shared key of the RADIUS client, max length is 30 characters.
	enable	Enables this RADIUS client entry.
	disable	Disables this RADIUS client entry.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Add or modify the client rule (the client is enabled by default): router# configure router(config)# radius-server client client1 ip 192.168.127.254 netmask 255.255.255.0 sharekey radiuskey router(config)# exit Enable or disable the client rule: router# configure router(config)# radius-server client client1 enable/disable router(config)# exit	
Error Messages	% Over length. It must be 1 - 30 !!! <STRING:clientname> <clientname>	
	% Invalid system symbol !!! <STRING:clientname> <clientname>	
	% Invalid client name !!! <STRING:clientname> localhost	
	% Invalid Unicast IP !!! <IPV4ADDR:ip> <ipaddr>	
	% Invalid Netmask !!! <IPV4ADDR:netmask> <subnetmask>	
	% Same network range with other setting !!! <IPV4ADDR:ip> <ipaddr>	
	% Over length. It must be 1 - 30 !!! <STRING:sharekey> <key>	
	% Invalid system symbol !!! <STRING:sharekey> <key>	
	% Setting list is full	
	% <clientname> is not existed in list !!! RADIUS Server Client Table list <STRING:clientname> <clientname>	
	^Parse error	
	^Incomplete command	
Related Commands	show radius-server clientdb	

radius-server user

To add or modify user for RADIUS server, use the **radius-server user** command.

To delete a user from the client database, use the **no** form of this command.

Synopsis

(config)# **radius-server user <username> { password <key> authority <authority-level> | enable | disable }**

(config)# **no radius-server user <username>**

Option Description	**user**	Specifies username in user database.
	username	Username in the user database, max length is 30 characters.
	password	Specifies the password of the user.
	key	Password of the user, max length: 30 characters.
	authority	Specifies user authority.
	authority-level	Specify an integer: { system admin(1) | user(3) }
	enable	Enables user entry.
	disable	Disables user entry.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Add or modify the user rule (the user is enabled by default): router# configure router(config)# radius-server user user1 password pwd authority 1 router(config)# exit Enable or disable the user rule: router# configure router(config)# radius-server user user1 enable/disable router(config)# exit	
Error Messages	% Over length. It must be 1 - 30 !!! <STRING:username> <username>	
	% Invalid system symbol !!! <STRING:username> <username>	
	% Over length. It must be 1 - 30 !!! <STRING:password> <password>	
	% Invalid system symbol !!! <STRING:password> <password>	
	% Invalid Setting !!!	
	% Setting list is full	
	% <username> is not existed in list !!! RADIUS Server User Table list <STRING:username> <username>	
	^Parse error	
	^Incomplete command	
Related Commands	show radius-server userdb	

radius-server auth-port

To specify or modify the authentication port settings for RADIUS server, use the radius-server auth-port command.

Synopsis

(config)# **radius-server auth-port <authenticationPort>**

Option Description	**auth-port**	Specifies authentication port for RADIUS client.
	authenticationPort	Port number, integer ranges from 1 to 65535.
Defaults	Default authenticationPort is 1812.	
Command Modes	Global configuration	
Usage Guidelines	The use of 18120 as the authentication port is prohibited, as these are reserved for internal use.	
Examples	`router# configure` `router(config)# radius-server auth-port 1812` `router(config)# exit`	
Error Messages	% Over length. It must be 1 - 65535 !!! <UINT:auth_port> <authenticationPort>	
	% Authentication port cannot be 18120 !!!	
	^Parse error	
	^Incomplete command	
Related Commands	show radius-server	

radius-server client

To add or modify allowed RADIUS client for RADIUS server, use the **radius-server client** command.

To delete a client from the client database, use the **no** form of this command.

Synopsis

(config)# **radius-server**
client <clientname> { ip <ipaddr> netmask <subnetmask> sharekey <key> | enable | disable }

(config)# **no radius-server client <clientname>**

Option Description	**client**	Specifies RADIUS client name in client database.
	clientname	RADIUS client name in the client database, max length is 30 characters.
	ip	Specifies the RADIUS client ip address.
	ipaddr	The IP address of the RADIUS client ip address, the ip shall be unicast.
	netmask	Specify the subnet mask for this IP address to allow all RADIUS clients within the subnet to authenticate through this RADIUS server.
	subnetmask	Subnet mask for this IP address.
	sharekey	Specifies the shared key of the RADIUS client.
	key	Shared key of the RADIUS client, max length is 30 characters.
	enable	Enables this RADIUS client entry.
	disable	Disables this RADIUS client entry.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Add or modify the client rule (the client is enabled by default): router# configure router(config)# radius-server client client1 ip 192.168.127.254 netmask 255.255.255.0 sharekey radiuskey router(config)# exit Enable or disable the client rule: router# configure router(config)# radius-server client client1 enable/disable router(config)# exit	
Error Messages	% Over length. It must be 1 - 30 !!! <STRING:clientname> <clientname>	
	% Invalid system symbol !!! <STRING:clientname> <clientname>	
	% Invalid client name !!! <STRING:clientname> localhost	
	% Invalid Unicast IP !!! <IPV4ADDR:ip> <ipaddr>	
	% Invalid Netmask !!! <IPV4ADDR:netmask> <subnetmask>	
	% Same network range with other setting !!! <IPV4ADDR:ip> <ipaddr>	
	% Over length. It must be 1 - 30 !!! <STRING:sharekey> <key>	
	% Invalid system symbol !!! <STRING:sharekey> <key>	
	% Setting list is full	
	% <clientname> is not existed in list !!! RADIUS Server Client Table list <STRING:clientname> <clientname>	
	^Parse error	
	^Incomplete command	
Related Commands	show radius-server clientdb	
	% <username> is not existed in list !!! RADIUS Server User Table list <STRING:username> <username>	
	^Parse error	
	^Incomplete command	
	show radius-server userdb	

show radius-server

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

Synopsis

(config)# **show radius-server**

Option Description	N/A
Defaults	N/A
Command Modes	Privileged EXEC / User EXEC
Usage Guidelines	N/A
Examples	`router# show radius-server` `RADIUS Server Global Setting` `RADIUS Server Enable: Enable` `Authentication Port:  1812`
Error Messages	^Parse error
	^Incomplete command
Related Commands	radius-server enable no radius-server enable radius-server auth-port <authenticationPort>

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}

Option Description	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
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Enable security notification for Login fail event. `router# configure` `router(config)# security-notification event-loginfail` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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**]

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

Option Description	setting	Specifies to display security notification settings
	status	Specifies to display security notification status
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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 ==	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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

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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	Display packet counter information for all ports. `Firewall/ETBN Router 00000# show interfaces counters` `  Port     Tx Packets     Rx Packets` `  ---- ------------------ ------------------` `   1/1                239                2290` `   1/2                  0                   0` `   1/3                  0                   0` `   1/4                  0                   0` `   1/5                  0                   0` `   1/6                  0                   0` `   1/7                  0                   0` `   1/8                  0                   0` `   1/9                  0                   0` `  1/10                  0                   0` `  Trk1                  0                   0` `  Trk2                  0                   0` `  Trk3                  0                   0`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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**}

Option Description	enable	Enables/disables LLDP feature
	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
Defaults	LLDP is enabled in factory default. Transmission frequency of LLDP updates is 30 seconds.	
Command Modes	Global configuration	
Usage Guidelines	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.	
Examples	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`	
Error Messages	^Parse error	
	^Incomplete command	
	% Time interval must be 5 - 32768	
Related Commands	show lldp	

show lldp

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

Synopsis

show lldp [**entry**]

Option Description	entry	LLDP entries
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	lldp	

show arp

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

Synopsis

show arp

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

Option Description	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) | Device-Lockdown(5) | 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.
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	• When selecting method "TFTP(1)", there is no need for <account> and <password> to complete the command. • When selecting method "USB(2)", there is no need for <ip>, <account> and <password> to complete the command.	
Examples	• 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#` • 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#`	
Error Messages	% 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	
Related Commands	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**

Option Description	events	Specifies one of below event names: {**cold-start** | **warm-start** | **config-changed** | **pwr1-trans-on** | **pwr2-trans-on** | **pwr1-trans-off** | **pwr2-trans-off** | **auth-fail** | **topology-changed** | **coupling-changed** | **master-changed** | **vrrp-state-changed** | **dot1x-auth-fail** | **poe-pd-on** | **poe-pd-off** | **poe-exceed-system-threshold** | **poe-fetbad** | **poe-over-temperature** | **poe-vee-uvlo** | **poe-pd-over-current** | **poe-pd-check-fail** | **poe-exceed-power-budget** | **vpn-connected** | **vpn-disconnected** | **firewall-policy-changed** | **firmware-upgrade-success** | **firmware-upgrade-failure** | **log-service-ready** }
	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
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	• 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) } • 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) } • 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) }	
Examples	Enable "warm start" event notification and send warning message to the Syslog server with severity DEBUG. `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`	
Error Messages	% Invalid severity type	
	% Invalid action value or non-support this combination action	
	^Parse error	

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

warning-notification system-event license-notification-ips

Set IPS license event configuration including enabling, notification targets, and event severity.

Synopsis

(config)# **warning-notification system-event license-notification-ips { threshold <UINT:threshold> | frequency daily | weekly | monthly | action <UINT:combination> | severity <UINT:type> | active }**

(config)# **no warning-notification system-event license-notification-ips**

Option Description	**threshold**	License notification threshold
	<UINT:threshold>	Threshold 30/60/90/180 points before depleted
	frequency	License notification frequency
	daily	Daily notification
	weekly	Weekly notification
	monthly	Monthly notification
	action	Enable Action setting, combination between SNMP Trap / Email / Syslog
	severity	Severity setting
	active	Activate
Defaults	threshold: default 90 frequency: default daily action: default None(0) severity: default Emergency(0) active: deactivated (0)	
Command Modes	Global configuration	
Usage Guidelines	only supervisor privilege (or above) is applicable.	
Examples	`router# configure` `router(config)# warning-notification system-event license-notification-ips frequency weekly` `router(config)# warning-notification system-event license-notification-ips threshold 60` `router(config)# warning-notification system-event license-notification-ips active` `router(config)# warning-notification system-event license-notification-ips action 7` `router(config)# warning-notification system-event license-notification-ips severity 5`	
Error Messages	^Parse error	
	^Incomplete command	
	% Invalid Setting !!! <UINT:threshold> 1111	
	% Over length. It must be 0 - 7 !!! <UINT:type> 11	
	% Invalid action value or non-support this combination action !!!	
Related Commands	(config)# show warning-notification system-event license-notification-ips	

warning-notification system-event radius-server-auth-log

To specify or modify warning notification for RADIUS server 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 radius-server-auth-log {action | severity | active}**

(config)# **no warning-notification system-event radius-server-auth-log active**

Option Description	**action**	Configure actions of events.
	action-index	Specifies an integer for: {Syslog only(4) | None(0)}
	severity	Specifies the password of the user.
	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.
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification system-event radius-server-auth-log action 4` `router(config)# warning-notification system-event radius-server-auth-log severity 7` `router(config)# warning-notification system-event radius-server-auth-log active` `router(config)# no warning-notification system-event radius-server-auth-log active` `router(config)# exit`	
Error Messages	% Invalid severity type	
	% Invalid action value or non-support this combination action	
	^Parse error	
	^Incomplete command	
Related Commands	N/A	

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 Description	action	Enable Action setting
	combination	• SNMP Trap Server only(1) • Email only(2) • SNMP Trap Server+Email(3) • Syslog only(4) • SNMP Trap Server+Syslog Server(5) • Email+Syslog Server(6) • SNMP Trap Server+Email+Syslog Server(7) • Relay1 only(8) • SNMP Trap Server+Relay1(9) • Email+Relay1(10)

		• SNMP Trap Server+Email+Relay1(11) • Syslog+Relay1(12) • SNMP Trap Server+Syslog Server+Relay1(13) • Email+Syslog Server+Relay1(14) • SNMP Trap Server+Email+Syslog Server+Relay1(15) • SMS(32) • SNMP Trap Server+SMS(33) • Email+SMS(34) • SNMP Trap Server+Email+SMS(35) • Syslog Server+SMS(36) • SNMP Trap Server+Syslog Server+SMS(37) • Email+Syslog Server+SMS(38) • SNMP Trap Server+Email+Syslog Server+SMS(39) • Relay1+SMS(40) • SNMP Trap Server+Relay1+SMS(41) • Email+Relay1+SMS(42) • SNMP Trap Server+Email+Relay1+SMS(43) • Syslog Server+Relay1+SMS(44) • SNMP Trap Server+Syslog Server+Relay1+SMS(45) • Email+Syslog Server+Relay1+SMS(46) • SNMP Trap Server+Email+Syslog Server+Relay1+SMS(47) • None(0)
	severity	Severity setting
	type	• Emergency(0) • Alert(1) • Critical(2) • Error(3) • Warning(4) • Notice(5) • Information(6) • Debug(7)
	active	Activate
	no	Negate command or set to default
Defaults	N/A	
Command Modes	Configuration mode	
Usage Guidelines	N/A	
Examples	`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`	
Error messages	% Invalid action value or non-support this combination action	
	% Invalid severity type	
Related Commands	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**}}

Option Description	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)}
Defaults	Disabled	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• 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) } • 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) } • 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) }	
Examples	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`	
Error Messages	% Invalid severity type	
	% Invalid action value or non-support this combination action	
	^Parse error	
	^Incomplete command	
Related Commands	show interfaces ethernet snmp-server host snmp-server trap-mode email-warning	

	logging <ip-addr>

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>}

Option Description	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 | device-lockdown | 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.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	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. `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`	
Error Messages	^Parse error	
	^Incomplete command	
	% Event log capacity threshold should between 50~100	
	% Error Name:	
Related Commands	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> <recv-email> |
account <name> [<password>]
from <sender-email>}

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

Option Description	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
	recv-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
	from	Specifies sender's email
	sender-email	Sender's email address
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	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. `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 from user1@example.com` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
	% Invalid Port	
	% Invalid Mail Index	
	% Invalid Email Address	
	% Invalid User Name Length	
Related Commands	show email-warning config	

SMTP in Email Settings

To configure the SMTP email settings, use the following commands.

Synopsis

(config)# **email-warning server** <STRING:servaddr> { <UINT:smtpPort> }

Option Description	server	SMTP server.
	servaddr	SMTP server domain name.
	smtpPort	SMTP server port number.
Defaults	SMTP port: 25 Sever address: N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# email-warning server smtp.gmail.com 587`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To configure email warnings account and password, use this command.

Synopsis

(config)# **email-warning account** <STRING:name> { <STRING:password> }

Option Description	account	SMTP server account.
	name	SMTP server account.
	password	SMTP server password.
Defaults	Name: N/A Password: N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# email-warning account test@moxa.com 1234567890`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To toggle whether email warnings are sent with TLS, use this command.

Synopsis

(config)# **email-warning tls** <enable | disable>

Option Description	tls	TLS mode for STARTTLS.
	enable	Enable TLS.
	disable	Disable TLS.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	To enable TLS: `router# configure` `router(config)# email-warning tls enable` • To disable TLS: `router# configure` `router(config)# email-warning tls disable`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To configure TLS, use this command.

Synopsis

(config)# **email-warning tls enable_with_ca** <STRING:ca_file_name>

Option Description	tls	TLS mode for STARTTLS.
	enable_with_ca	Enable TLS with CA mode.
	ca_file_name	CA file name for STARTTLS TLS check.
Defaults	ca_file_name: N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# email-warning tls enable_with_ca cacert.pem`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To configure recipient email address for sending email warnings, use this command.

Synopsis

(config)# **email-warning mail-address** <UINT:mailIdx> <STRING:mailAddress>

Option Description	mail-address	Configure email warning mail address
	mailIdx	Recipient address index in config table (1 to 4)
	mailAddress	Recipient address
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)#email-warning mail-address 1 test@moxa.com`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To clear email warning sender address, use this command.

Synopsis

(config)#no email-warning sender <STRING:mailAddress>

Option Description	no	Reset/Remove/Factory Default
	mail-address	Configure email warning mail address
	sender	Email warning sender
	mailAddress	Sender address
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)#email-warning sender test@moxa.com`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To clear all SMTP server configuration, use this command.

Synopsis

(config)# **no email-warning server**

Option Description	server	SMTP server
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# no email-warning server`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To clear the specific (index) smtp mail address configuration, use this command.

Synopsis

(config)# **no email-warning mail-address** <UINT:mailIdx>

Option Description	mail-address	Configure email warning mail address
	mailIdx	smtp Recipient address index in cfg table
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)#no email-warning mail-address 1`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To clear all SMTP account and password configuration, use this command.

Synopsis

(config)# **no email-warning account**

Option Description	account	smtp account
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)#no email-warning account`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

To clear SMTP sender email address configuration, use this command.

Synopsis

(config)# **no email-warning sender**

Option Description	sender	SMTP sender.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)#no email-warning sender`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

RX Discard

This section describes the commands used for configuring RX discard notifications on the specific port.

warning-notification port-event rx-discard action

Synopsis

(config)# **interface ethernet** <mod_port>

(config-if)# **warning-notification port-event rx-discard action** {UINT:combination}

Option Description	warning-notification	Warning notification
	port-event	Port event setting
	rx-discard	The volume of RX Discard in the past 30 seconds
	action	Enable Action setting
	<combination>	None(0) SNMP Trap Server only(1) Syslog only(4) SNMP Trap Server+Syslog Server(5) LocalStorage(64) SNMP Trap Server+Local Storage(65) Syslog Server+Local Storage(68) SNMP Trap Server+Syslog Server+Local Storage(69)
Defaults	None(0)	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	Removing SYSLOG from actions of "RX Discard" by giving single value of 0: `Firewall/VPN Router 00000(config)# warning-notification port-event rx-discard action 0` Adding SYSLOG into actions of "RX Discard" by giving single value of 1,4,5: `Firewall/VPN Router 00000(config)# warning-notification port-event rx-discard action 4`	
Error Messages	% Invalid action value or non-support this combination action. (if target rule does not exist)	
Related Commands	N/A	

warning-notification port-event rx-discard severity

Synopsis

(config)# **interface ethernet** <mod_port>

(config-if)# **warning-notification port-event** rx-discard severity {UINT:severity}

Option Description	warning-notification	Warning notification
	port-event	Port event setting
	rx-discard	The volumn of RX Discard in the past 30 seconds
	severity	Setting severity
	<severity>	<0> Emergency <1> Alert <2> Critical <3> Error <4> Warning <5> Notice <6> Informational <7> Debug
Defaults	(6) Informational	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	Set up rx-discard log severity to <4>Warning N/A `Firewall/VPN Router 00000(config)# warning-notification port-event rx-discard severity 4` Set up rx-discard log severity to <6>Informational `Firewall/VPN Router 00000(config)# warning-notification port-event rx-discard severity 6`	
Error Messages	% Invalid action value or non-support this severity value. (if target rule does not exist)	
Related Commands	N/A	

warning-notification port-event rx-discard enable

Synopsis

(config)# **interface ethernet** <mod_port>

(config-if)# **warning-notification port-event rx-discard enable**

Option Description	warning-notification	Warning notification
	port-event	Port event setting
	rx-discard	The volumn of RX Discard in the past 30 seconds
	enable	Enable RX Discard log
Defaults	Disabled	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	Enable rx-discard log Firewall/VPN Router 00000(config)# warning-notification port-event rx-discard enable Disable rx-discard log Firewall/VPN Router 00000(config)# no warning-notification port-event rx-discard enable	
Error Messages	N/A	
Related Commands	N/A	

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 |
l3l7-policy}

(config)# **no logging** [{**dos** [{**flash** |
syslog |
trap}] |
ipsec [{**syslog** |
flash |
trap}] |
trusted-access [{**flash** |
syslog |
trap}] |
firewall |
l3l7-policy }]

	dos	Enables/disables event logging for DoS function

Option Description	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
	l3l7-policy	Enables/disables event logging for Layer 3-7 policy
	firewall	Enables/disables event logging for Firewall function (**No longer supported after version 3.0**.)
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	• Configure SNMP Trap in advance when sending event logs via SNMP trap. • Configure Syslog server in advance when sending event logs to syslog server.	
Examples	• Enable logging for Trusted-Access function. Specify the severity to DEBUG and write logs into internal Flash storage. `router# configure` `router(config)# logging trusted-access severity 7` `router(config)# logging trusted-access flash` `router(config)# logging trusted-access` `router(config)# exit` • Disable logging for Layer 3-7 policy function. `router# configure` `router(config)# no logging l3l7-policy`	
Error Messages	% Severity level is out of range!	
	% The firewall configuration is not compatible with firmware versions prior to V2.0.	
	^Parse error	
	^Incomplete command	
Related Commands	logging-capacity show logging event-log show logging event-log snmp-server host snmp-server trap-mode logging <ip-addr>	

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>}

Option Description	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
Defaults	N/A	

Command Modes	Global configuration
Usage Guidelines	• Max. number of Syslog server is 3. • If necessary, the certificate must be installed via web GUI when utilizing TLS authentication with the Syslog server.
Examples	• Specify the first Syslog server (192.168.1.2), port (5145) and enable it. `router# configure` `router(config)# logging 192.168.1.2 5145 1` `router(config)# exit` • Disable the first Syslog server entry. `router# configure` `router(config)# no logging enable 1` `router(config)# exit`
Error Messages	% This server is not existed in the list.
	% Server list is full.
	^Parse error
	^Incomplete command
Related Commands	logging warning-notification system-event interface ethernet warning-notification

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 }]

Option Description	vpn	VPN event logs
	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
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	Clear all system event logs. `router# clear logging event-log system`	

	router#
Error Messages	^Parse error
	^Incomplete command
Related Commands	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**}

Option Description	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
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• A local storage (ABC-02) has to be plugged in advance. • Hardware interface (USB) has to be enabled in advance.	
Examples	• 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` • 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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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>]

Option Description	trap-ip	IP address for SNMP trap notification
	trap-community	SNMP trap community string, 1 to 64 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # $ % & * ( ) . + = { } [ ] | : ; , ~, no spaces are allowed.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• 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. • When Specify/modify trap community, {trap-community} should come after {trap-ip}. • 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. • 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.	
Examples	Specify a trap target IP address and modify the trap community string to "newTrap". `router# configure` `router(config)# snmp-server host 192.168.127.10 newTrap` `router(config)# exit`	
Error Messages	% Invalid IP Address.	
	% Host or Community is incorrect!!!	
	% Trap servers are full, please remove at least one first.	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	trap-v1	SNMP v1 trap notification
	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
Defaults	The default mode is "trap-v1"	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Specify/modify SNMP v2c trap notification. `router# configure` `router(config)# snmp-server trap-mode trap-v2c` `router(config)# exit`	
Error Messages	% Invalid Retries Value. It must be 1 - 99.	
	% Invalid Timeout Value. It must be 1 - 300.	
	^Parse error	
	^Incomplete command	
Related Commands	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>]]}

Option Description	trap-v3	Specifies SNMP v3 trap notifications
	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 | sha256 | sha512 }
	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.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Only one user is permitted. Executing the command again will overwrite the existing settings.	
Examples	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`	
Error Messages	^Parse error	
	^Incomplete command	
	% SNMP authtype must be (no-auth | md5 | sha | sha256 | sha512)!!	
Related Commands	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** | **l3l7-policy** | **trust-access** | **malformed** | **dos** | **dpi** | **adp** | **ips** | **session-control** | **l2-policy**}] [**severity** <level-range>]

Option Description	vpn	Specifies all VPN event logs
	system	Specifies all System event logs
	l3l7-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
	l2-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, ...
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`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 <0>  [Configuration Change] DHCP Relay Agent, Bootup:132, Startup:0d5h20m48s` `----------` `2  2017/10/14 12:04:11 <0>  [Configuration Change] DHCP Relay Agent, Bootup:132, Startup:0d5h20m44s`	
Error Messages	% Severity level is out of range!	
	^Parse error	
	^Incomplete command	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC /User EXEC	
Usage Guidelines	N/A	
Examples	`# 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 :`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	email-warning	

show logging-capacity

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

Synopsis

show logging-capacity

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	logging-capacity	

show warning-notification port-event

To show port usage alarm and other port event configuration and status, use this command.

Synopsis

show warning-notification port-event

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC /User EXEC	
Usage Guidelines	N/A	
Examples	Firewall/VPN Router 00000# show warning-notification port-event Event : Link-on Port Status Action Severity ---- ------- ------ -------- 1 Disable 0 0 2 Disable 0 0 3 Disable 0 0 4 Disable 0 0 5 Disable 0 0 6 Disable 0 0 7 Disable 0 0 8 Disable 0 0 9 Disable 0 0 10 Disable 0 0 11 Disable 0 0 12 Disable 0 0 13 Disable 0 0 14 Disable 0 0 15 Disable 0 0 16 Disable 0 0 Event : Link-off Port Status Action Severity ---- ------- ------ -------- 1 Disable 0 0 2 Disable 0 0 3 Disable 0 0 4 Disable 0 0 5 Disable 0 0 6 Disable 0 0 7 Disable 0 0 8 Disable 0 0 9 Disable 0 0 10 Disable 0 0 11 Disable 0 0 12 Disable 0 0 13 Disable 0 0 14 Disable 0 0 15 Disable 0 0 16 Disable 0 0 Event : Traffic-Overload Port Status ---- ------- 1 Disable	

```
2       Disable
3       Disable
4       Disable
5       Disable
6       Disable
7       Disable
8       Disable
9       Disable
10      Disable
11      Disable
12      Disable
13      Disable
14      Disable
15      Disable
16      Disable
Port    Status    Event   Threshold   Duration   Action   Severity
----    -------   -----   ---------   --------   ------   --------
1       Disable    Tx         50         10        0         4
2       Disable    Tx         50         10        0         4
3       Disable    Tx         50         10        0         4
4       Disable    Tx         50         10        0         4
5       Disable    Tx         50         10        0         4
6       Disable    Tx         50         10        0         4
7       Disable    Tx         50         10        0         4
8       Disable    Tx         50         10        0         4
9       Disable    Tx         50         10        0         4
10      Disable    Tx         50         10        0         4
11      Disable    Tx         50         10        0         4
12      Disable    Tx         50         10        0         4
13      Disable    Tx         50         10        0         4
14      Disable    Tx         50         10        0         4
15      Disable    Tx         50         10        0         4
16      Disable    Tx         50         10        0         4
Port    status    event   threshold   duration   action   severity
----    -------   -----   ---------   --------   ------   --------
1       Disable    Rx         50         10        0         4
2       Disable    Rx         50         10        0         4
3       Disable    Rx         50         10        0         4
4       Disable    Rx         50         10        0         4
5       Disable    Rx         50         10        0         4
6       Disable    Rx         50         10        0         4
7       Disable    Rx         50         10        0         4
8       Disable    Rx         50         10        0         4
9       Disable    Rx         50         10        0         4
10      Disable    Rx         50         10        0         4
11      Disable    Rx         50         10        0         4
12      Disable    Rx         50         10        0         4
13      Disable    Rx         50         10        0         4
14      Disable    Rx         50         10        0         4
15      Disable    Rx         50         10        0         4
16      Disable    Rx         50         10        0         4
```

Error Messages	N/A
Related Commands	warning-notification port-event event traffic-overload {active | tx | rx | severity |action}

warning-notification port-event event traffic-overload <active>

To enable/disable port usage alarm, use this command.

Synopsis

(config-if)# **warning-notification port-event event traffic-overload <active>**

Option Description	active	Enable the port event traffic overload warning notification
Defaults	Disabled	
Command Modes	Port Interface Configuration	
Usage Guidelines	1.Enable warning-notification port-event event traffic-overload active 2.Disable no warning-notification port-event event traffic-overload active	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# warning-notification port-event event traffic-overload active`	
Error Messages	N/A	
Related Commands	show warning-notification port-event	

warning-notification port-event event traffic-overload <tx/rx active>

To enable/disable Tx/Rx port, use this command.

Synopsis

(config-if)# **warning-notification port-event event traffic-overload <tx/rx active>**

Option Description	tx/rx active	Enable the Tx/Rx function
Defaults	Disabled	
Command Modes	Port Interface Configuration	
Usage Guidelines	1. Tx Enable warning-notification port-event event traffic-overload tx active 2. Tx Disable no warning-notification port-event event traffic-overload tx active 3. Rx Enable warning-notification port-event event traffic-overload rx active 4. Rx Disable no warning-notification port-event event traffic-overload rx active	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# warning-notification port-event event traffic-overload rx active`	
Error Messages	N/A	
Related Commands	warning-notification port-event event traffic-overload rx {active | threshold} warning-notification port-event event traffic-overload tx {active | threshold} show warning-notification port-event	

warning-notification port-event event traffic-overload <tx/rx> threshold <1-100> duration <1-300>

To configure Tx/Rx port threshold and duration settings, use this command.

Synopsis

(config-if)# **warning-notification port-event event traffic-overload <tx/rx> threshold <1-100> duration <1-300>**

Option Description	tx/rx threshold number	Threshold for tx/rx as a percentage: 1 to 100
	tx/rx threshold duration	Threshold duration for tx/rx in seconds: 1 to 300
Defaults	Threshold Number: 50, Duration Number: 10	
Command Modes	Port Interface Configuration	
Usage Guidelines	N/A	
Examples	Tx example: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# warning-notification port-event event traffic-overload tx threshold 20 duration 30` Rx example: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# warning-notification port-event event traffic-overload rx threshold 10 duration 10`	
Error Messages	If <Threshold> contains an invalid value. Invalid! Threshold should be between 1 and 100 (%).	
	If <Duration> contains an invalid value. Invalid! Duration should be between 1 and 300 (seconds).	
Related Commands	warning-notification port-event event traffic-overload rx {active | threshold} warning-notification port-event event traffic-overload tx {active | threshold} show warning-notification port-event	

warning-notification port-event event traffic-overload severity <0-7>

To configure traffic overload severity settings, use this command.

Synopsis

(config-if)# **warning-notification port-event event traffic-overload severity <0-7>**

Option Description	severity	Configure severity level
Defaults	Severity Level: 4	
Command Modes	Port Interface Configuration	
Usage Guidelines	Specified <Severity level> must be a number and ranged of 0~7, where severity levels: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Information (6), Debug (7)	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# warning-notification port-event event traffic-overload severity 5`	
Error Messages	If <Severity level> contains an invalid value. Invalid severity type! Range of severity should be 0 – 7.	

Related Commands	show warning-notification port-event

warning-notification port-event event traffic-overload action

To configure traffic overload actions, use this command.

Synopsis

(config-if)# **warning-notification port-event event traffic-overload action**

Option Description	N/A	
Defaults	Action Number: 0	
Command Modes	Global Configuration	
Usage Guidelines	Specified <Action number> must be 1, 2, 3, 4, 5, 6, 7, where the action number corresponds to the output types: SNMP-Trap (1), E-mail (2), Syslog (4). The accumulation of the numbers represents choosing multiple output types, for instance, action number 6 represents the Email (2) and Syslog (4).	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# warning-notification port-event event traffic-overload action 6`	
Error Messages	If <Action number> input wrong value (not one of 1, 2, 3, 4, 5, 6, 7) Invalid action value or non-support this combination action	
Related Commands	show warning-notification port-event	

warning-notification system-event dhcp-error-log <active)

Synopsis

(config)# **warning-notification system-event dhcp-error-log <active)**

Option Description	active	Enable the dhcp-error log warning notification
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	1.Enable warning-notification system-event dhcp-error-log active 2.Disable no warning-notification system-event dhcp-error-log active	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event dhcp-error-log active`	
Error Messages	N/A	
Related Commands	show warning-notification port-event	

warning-notification system-event dhcp-error-log severity <0-7>

To configure DHCP error log severity, use this command.

Synopsis

(config)# **warning-notification system-event dhcp-error-log severity** <0-7>

Option Description	N/A	
Defaults	Severity Level: 0	
Command Modes	Port Interface Configuration	
Usage Guidelines	Specified <Severity level> must be a number and ranged of 0~7, where severity levels: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Information (6), Debug (7)	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event dhcp-error-log severity 0`	
Error Messages	% Invalid severity type! Range of severity should be 0 – 7.	
	^Parse error	
	^Incomplete command	
Related Commands	show warning-notification port-event	

warning-notification system-event dhcp-error-log action (0/1/2/4)

To configure DHCP error log actions, use this command.

Synopsis

Option Description	N/A	
Defaults	Action Number: 0	
Command Modes	Global Configuration	
Usage Guidelines	Specified <Action number> must be 0 or 4, where the action number corresponds to the output types: SNMP-Trap (1), E-mail (2), Syslog (4). The DHCP error log function only supports Syslog (4).	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event dhcp-error-log action 4`	
Error Messages	% Invalid action value or non-support this combination action	
	^Parse error	
	^Incomplete command	
Related Commands	show warning-notification port-event	

warning-notification system-event igmp-snooping-error-log

To configure the IGMP Snooping error log, use this command.

Synopsis

(config)# **warning-notification system-event igmp-snooping-error-log** <active>

Option Description	active	Enable the dhcp-error log warning notification
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	1.Enable warning-notification system-event igmp-snooping-error-log active 2.Disable no warning-notification system-event igmp-snooping-error-log active	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event igmp-snooping-error-log active`	
Error Messages	N/A	
Related Commands	show warning-notification port-event	

warning-notification system-event igmp-snooping-error-log severity <0-7)

To configure IGMP Snooping error log severity, use this command.

Synopsis

(config)# **warning-notification system-event igmp-snooping-error-log severity** <0-7>

Option Description	N/A	
Defaults	Severity Level: 0	
Command Modes	Global Configuration	
Usage Guidelines	Specified <Severity level> must be a number with the range of 0~7, where severity levels: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Information (6), Debug (7)	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event igmp-snooping-error-log severity 0`	
Error Messages	% Invalid severity type! Range of severity should be 0 – 7.	
	^Parse error	
	^Incomplete command	
Related Commands	show warning-notification port-event	

warning-notification system-event igmp-snooping-error-log action <0/1/2/4>

To configure IGMP Snooping error log actions, use this command.

Synopsis

(config)# **warning-notification system-event igmp-snooping-error-log action** <0/1/2/4>

Option Description	N/A	
Defaults	Action Number: 0	
Command Modes	Global Configuration	
Usage Guidelines	Specified <Action number> must be 0 or 4, where the action number corresponds to the output types: SNMP-Trap (1), E-mail (2), Syslog (4). The DHCP error log function only supports Syslog (4).	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event igmp-snooping-error-log action 4`	
Error Messages	% Invalid action value or non-support this combination action	
	^Parse error	
	^Incomplete command	
Related Commands	show warning-notification port-event	

warning-notification system-event duplicate-ip-detection severity <type>

To configure duplicate IP detection action warning notification, use this command.

Synopsis

(config)# **warning-notification system-event duplicate-ip-detection severity** <type>

Option Description	Type	Specify severity type
Defaults	4	
Command Modes	Configuration mode	
Usage Guidelines	Specified <Severity level> must be a number and ranged of 0~7.,where severity levels: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Information (6), Debug (7)	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event duplicate-ip-detection severity 5`	
Error Messages	If <Severity level> input wrong value.	
	Over length. It must e 0 - 7 !!!	
Related Commands	N/A	

warning-notification system-event duplicate-ip-detection action <Action number>

To configure duplicate IP detection action number warning notification, use this command.

Synopsis

(config)#warning-notification system-event duplicate-ip-detection action <Action number>

Option Description	action (Action number)	Specify action number
Defaults	0	
Command Modes	Configuration mode	
Usage Guidelines	Specified <Action number> must be 1, 2, 3, 4, 5, 6, 7Where the action number corresponds to the output types: E-mail (2), Syslog (4), Trap(1). The accumulation of the numbers represents the multiple choices of the output types, for instance, action number 6 represents the Email (2) and Syslog (4).	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event duplicate-ip-detection action 6`	
Error Messages	If <Action number> input wrong value (not one of 1, 2,3,4,5,6,7).	
	Invalid action value or non-support this combination action	
Related Commands	N/A	

warning-notification system-event ntp-sntp-error-log active

To enable or disable the ntp sntp error log warning notification, use these commands.

(config)# warning-notification system-event ntp-sntp-error-log active

(config)# no warning-notification system-event ntp-sntp-error-log active

Option Description	warning-notification system-event ntp-sntp-error-log active	Enable the warning notification
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	**Service Impact:** Enabling this feature will cause the system to generate warning notifications when NTP/SNTP system events occur.	
Examples	Enable the notification: `router# configure` `router(config)# warning-notification system-event ntp-sntp-error-log active` `router(config)# exit` Disable the notification: `router# configure` `router(config)# no warning-notification system-event ntp-sntp-error-log active` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	warning-notification system-event ntp-sntp-error-log action <UINT:combination> warning-notification system-event ntp-sntp-error-log severity <UINT:type>	

warning-notification system-event ntp-sntp-error-log active

To configure or disable the ntp sntp error log warning notification, use these commands.

(config)# warning-notification system-event ntp-sntp-error-log action <UINT:combination>

Option Description	warning-notification system-event ntp-sntp-error-log action <UINT:combination>	Enable the warning notification
Defaults	None (0)	
Command Modes	Global configuration	
Usage Guidelines	**Protocol Limitation:** While the system generally supports multiple notification actions such as SNMP-Trap (1), E-mail (2), Relay (8), and SMS (32), the NTP/SNTP error log notification action supports Syslog (4) or None (0) only. Even when the notification action is set to None (0), the local event log shall still be recorded.	
Examples	Configure syslog notification for NTP/SNTP: `router# configure` `router(config)# warning-notification system-event ntp-sntp-error-log action 4` `router(config)# exit` Disable NTP/SNTP notification (None): `router# configure` `router(config)# warning-notification system-event ntp-sntp-error-log action 0` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	warning-notification system-event ntp-sntp-error-log active no warning-notification system-event ntp-sntp-error-log active warning-notification system-event ntp-sntp-error-log severity <UINT:type>	

warning-notification system-event ntp-sntp-error-log severity

To configure the ntp sntp error log warning notification severity, use these commands.

(config)# warning-notification system-event ntp-sntp-error-log severity <UINT:type>

Option Description	warning-notification system-event ntp-sntp-error-log severity <UINT:type>	Enable the warning notification
Defaults	Error (3)	
Command Modes	Global configuration	
Usage Guidelines	This setting configures the severity level of the NTP/SNTP error log notification.	
Examples	Configuring the severity level to Warning (4): `router# configure` `router(config)# warning-notification system-event ntp-sntp-error-log severity 4` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	warning-notification system-event ntp-sntp-error-log active no warning-notification system-event ntp-sntp-error-log active warning-notification system-event ntp-sntp-error-log action <UINT:combination>	

show logging

To show syslog settings about syslog server IP addresses, port, TLS, and message format, users need to be in normal mode.

Synopsis

show logging

Option Description	show	Display configuration/status information
	logging	Log information
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000# show logging` `Syslog Setting` `  Syslog Server 1: 192.168.127.1, port: 514, TLS: --, Message Format: RFC5424` `  Syslog Server 2: 192.168.127.2, port: 514, TLS: --, Message Format: RFC5424` `  Syslog Server 3: 192.168.127.3, port: 514, TLS: --, Message Format: RFC5424`	
Error Messages	N/A	
Related Commands	N/A	

Configure Syslog Message Format Settings

To configure syslog message format setting, use this command.

Synopsis

(config)# **logging** <STRING:hostaddr> [{<UINT:port> [{<UINT:index> [{authentication tls <STRING:

local_cert> **|message-format {rfc3164 | rfc5424} | connection-protocol {udp | tcp}}] | authentication tls** <STRING:local_cert> | **enable | disable** }] | **authentication tls** <STRING:local_cert>}]

(config)# **no logging** [{enable <UINT:index> |

<STRING:hostaddr>}]

Option Description	logging	Configure log settings
	<STRING:hostaddr>	IP Address or Domain Name
	<UINT:port>	Port of the syslog server
	<UINT:index>	Index of syslog entries
	message-format	Configure format of the message
	rfc3164	Message format supports RFC 3164
	rfc5424	Message format supports RFC 5424
Defaults	rfc3164	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	To enable syslog message format which supports RFC 3164 on Syslog 1: `Firewall/VPN Router 00000(config)# logging 192.168.127.100 514 1 message-format rfc3164`	

	To enable syslog message format which supports RFC 3164 on Syslog 2: `Firewall/VPN Router 00000(config)# logging 192.168.127.101 514 2 message-format rfc3164` To enable syslog message format which supports RFC 3164 on Syslog 3: `Firewall/VPN Router 00000(config)# logging 192.168.127.102 514 3 message-format rfc3164` To enable syslog message format which supports RFC 5424 on Syslog 1: `Firewall/VPN Router 00000(config)# logging 192.168.127.100 514 1 message-format rfc5424` To enable syslog message format which supports RFC 5424 on Syslog 2: `Firewall/VPN Router 00000(config)# logging 192.168.127.101 514 2 message-format rfc5424` To enable syslog message format which supports RFC 5424 on Syslog 3: `Firewall/VPN Router 00000(config)# logging 192.168.127.102 514 3 message-format rfc5424`
Error Messages	N/A
Related Commands	N/A

show warning-notification system-event cpu-usage-alarm

To show CPU usage alarm configuration and status, use this command.

Synopsis

show warning-notification system-event cpu-usage-alarm

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC /User EXEC	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000# show warning-notification system-event cpu-usage-alarm` `Status  Event  Threshold  Duration  Action  Severity` `-------  --------  ---------  --------  ------  --------` `Disable  CPU Usage Alarm  80  1  0  4`	
Error Messages	N/A	
Related Commands	warning-notification system-event cpu-usage-alarm {active | threshold | severity |action}	

show warning-notification system-event license-notification-ips

To show IPS License alarm configuration and status, use this command.

Synopsis

(config)# **show warning-notification system-event license-notification-ips**

Option Description	N/A	N/A
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	`router# show warning-notification system-event license-notification-ips` `Status  Event  Threshold (points)` `-------  ----------  ----------` `Enable  IPS License Depletion  180` `Frequency  Action  Severity` `---------  ------  --------` `daily  7  4`	
Error Messages	^Incomplete command	
Related Commands	(config)# warning-notification system-event license-notification-ips ...	

warning-notification system-event cpu-usage-alarm

To configure CPU usage alarm parameters, use this command.

Synopsis

(config)# **warning-notification system-event cpu-usage-alarm**

Option Description	N/A	
Defaults	Disabled	

Command Modes	Global Configuration
Usage Guidelines	1. Enable warning-notification system-event cpu-usage-alarm active 2. Disable no warning-notification system-event cpu-usage-alarm active
Examples	Firewall/VPN Router 00000# configure Firewall/VPN Router 00000(config)# warning-notification system-event cpu-usage-alarm active
Error Messages	N/A
Related Commands	show warning-notification system-event cpu-usage-alarm

warning-notification system-event cpu-usage-alarm threshold <60-90> duration <10-60>

To configure threshold and duration settings, use this command.

Synopsis

(config)# **warning-notification system-event cpu-usage-alarm threshold <60-90> duration <10-60>**

Option Description	N/A	
Defaults	Threshold number: 80, Duration number: 10	
Command Modes	Global Configuration	
Usage Guidelines	1. First specified <Threshold number> must be a number and ranged of 60~90. 2. <Duration number>must be a number and ranged of 10~60.	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event cpu-usage-alarm threshold 80 duration 10`	
Error Messages	% Invalid! Threshold should be between 60 and 90 (%).	
	% Invalid! Duration should be between 10 and 60 (seconds).	
	^Parse error	
	^Incomplete command	
Related Commands	show warning-notification system-event cpu-usage-alarm	

warning-notification system-event cpu-usage-alarm severity <0-7>

To configure severity, use this command.

Synopsis

(config)# **warning-notification system-event cpu-usage-alarm severity <0-7)**

Option Description	N/A	
Defaults	Severity Level value is 4.	
Command Modes	Global Configuration	
Usage Guidelines	1. Specified <Severity level> must be a number and ranged of 0~7,where severity levels: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Information (6), Debug (7)	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# warning-notification system-event cpu-usage-alarm severity 4`	
Error Messages	% Invalid severity type! Range of severity should be 0 – 7.	
	^Parse error	
	^Incomplete command	
Related Commands	show warning-notification system-event cpu-usage-alarm	

warning-notification system-event cpu-usage-alarm action <2/4/6>

To configure the action number, use this command.

Synopsis

(config)# **warning-notification system-event cpu-usage-alarm action <2/4/6>**

Option Description	N/A	
Defaults	Action Number value is 0.	
Command Modes	Global Configuration	
Usage Guidelines	Specified <Action number> must be 2 or 4 or 6Where the action number corresponds to the output types: SNMP-Trap (1), E-mail (2), Syslog (4). The accumulation of the numbers represents the multiple choices of the output types, for instance, action number 6 represents the Email (2) and Syslog (4).	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000n`	
Error Messages	% Invalid action value or non-support this combination action	
	^Parse error	
	^Incomplete command	
Related Commands	show warning-notification system-event cpu-usage-alarm	

Neighbor MAC Change

This section describes the commands used for MAC learning management.

show mac-address-table

Synopsis

show mac-address-table

Option Description	show	Show System DB
	mac-address-table	Display MAC address table (MAX:1000 items)
Defaults	N/A	
Command Modes	Privilege EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 000000# show mac-address-table` `Log : Disable` `Severity : <0> Emergency` `Local : Enable` `Syslog : Disable` `Trap : Disable` `Idx MAC Type VLAN Port` `----- ----------------- -------- ---- ----------` `---------` `1 9C-2D-CD-10-10-AE ucast(l) 1 1/1,`	
Error Messages	N/A	
Related Commands	N/A	

logging mac-table severity

Synopsis

(config)# **logging mac-table severity** <severity-level> { flash | syslog | trap }

(config)# **no logging mac-table**

Option Description	logging	Set log
	mac-table	Enable to log when a MAC address is added or removed from the mac table.
	severity	Severity setting
	severity-level	Emergency(0) Alert(1) Critical(2) Error(3) Warning(4) Notice(5) Information(6) Debug(7)
	flash	Save log in Local Storage
	syslog	Send log in Syslog Server
	trap	Send log in SNMP Trap Server
Defaults	mac-table log: disabled. mac-table log severity: Informational. mac-table log destination: none.	
Command Modes	Global Configuration	
Usage Guidelines	Specified <Action number> must be 2 or 4 or 6Where the action number corresponds to the output types: SNMP-Trap (1), E-mail (2), Syslog (4). The accumulation of the numbers represents the multiple choices of the output types, for instance, action number 6 represents the Email (2) and Syslog (4).	
Examples	Enable change log of mac table: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# logging mac-table` Set mac table change log Severity to Critical: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# logging mac-table severity 2` Store mac table change log into Flash: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# logging mac-table flash` Disable logging capacity of mac table change: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# no logging mac-table` Cancel syslog from log destination of mac table change: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# no logging mac-table syslog`	
Error Messages	N/A	
Related Commands	show warning-notification system-event cpu-usage-alarm	

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**}

Option Description	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
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• Traffic send/receive by a source port (Monitored port) will be mirrored to the destination port (Mirror port) • Multiple port selection is acceptable.	
Examples	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`	
Error Messages	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	
Related Commands	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

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

ping

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

Synopsis

ping <ip-address>

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

show ping_src

Lists all active network interfaces that can be specified as the source interface when performing a ping.

Synopsis

show ping_src

Option Description	ping_src	List the network interfaces currently available to be used as a source when performing a ping command.
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	Simply enter show ping_src to display all available network interfaces that can be used with the ping <ip-addr|FQDN> src <option> command.	
Examples	# show ping_src To perform a ping using a specific source interface, use the "Option" value as the src parameter: ping <host> src <Option> e.g. ping www.moxa.com src WAN1 Interface Type Option Interface Name IP Address ---------- ---------- ---------- ---------- WAN WAN1 192.168.100.174 Bridge BRG1 BRG_LAN 192.168.126.254 GRE GRE1 GRE_TUN 192.168.1.174 OpenVPN OVPN 172.27.224.239 The The results are shown in the following format: To perform a ping using a specific source interface, use the "Option" value as the src parameter: ping <host> src <Option> e.g. ping www.moxa.com src WAN1 Interface Type Option Interface Name IP Address ---------- ---------- ---------- ---------- <Type> <Option> <Alias> <IpAddr> ... <Type>include WAN, Cellular, LAN, Bridge, Zone-Bridge, OpenVPN, PPTP, GRE, MRC, VRRP, L2TP, OOB MGMT <Option>The src value for the ping command. <Alias>User-recognizable interface name, only shown when the interface is user-configurable. <IpAddr>IP Address of the interface.	
Error Messages	N/A	
Related Commands	ping <ip-address|FQDN> { src <option> }: Use one of the listed interfaces as the source for a ping test.	

Execute Ping

To send an ICMP Echo Request (ping) to a specified IP or FQDN, or optionally allow users to specify a source interface, use this command.

Synopsis

ping <ip-addr|FQDN> {src <option>}

Option Description	ip-addr	The IP address of the target host, for example, 192.168.127.1
	FQDN	The fully qualified domain name of the target host, for example, www.moxa.com
	src	Specifies source interface for the ping
	option	<Option> in the result of the command show ping_src, for example, WAN1, LAN1
Defaults	If **src <option>** is not specified, the system uses the default interface chosen by its routing table.	
Command Modes	Privileged EXEC	
Usage Guidelines	ping **<ip-addr|FQDN>** is the basic ping test. If specifying a source interface, use **ping <ip-addr|FQDN> src <option>** .	
Examples	`# ping moxa.com` `Ping to moxa.com:` `Packets: Sent = 4, Received = 0, Lost = 4` `# ping moxa.com src WAN` `Ping to moxa.com via WAN(60.250.30.154):` `Packets: Sent = 4, Received = 0, Lost = 4`	
Error Messages	^Parse Error	
	^Incomplete command	
	% Invalid Hostname or IP Address.	
	% Invalid interface name.	
Related Commands	For listing available source interfaces, you might use **ping src_list** to see all active interfaces before specifying one in the ping command.	

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>]

Option Description	-c <count>	Exit after receiving count packets
	-i <interface>	Network interface to be used to capture packets. E.g. **eth0**
	-n	Do"t convert host addresses to names.
	expression	Common pcap-filter syntax
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	• Typing **tcpdump** command and pressing enter will get a prompt message and then type applicable arguments. • Only incoming packets will be displayed on the terminal console.	
Examples	Capture and display incoming icmp packets. `router# tcpdump` `Please set tcpdump parsing parameter` `-i eth0 icmp`	

	Press ESC or q to exit tcpdump 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 > 192.168.127.254: ICMP echo request, id 1, seq 2282, length 40 01:15:50.760035 IP 192.168.127.1 > 192.168.127.254: ICMP echo request, id 1, seq 2283, length 40
Error Messages	^Parse error
	^Incomplete command
Related Commands	N/A

traceroute

To trace the route that the IP packets will follow, use the **traceroute** command.

Synopsis

traceroute <ip-address|FQDN>

Option Description	ip-address	IP address
	FQDN	Fully qualified domain name
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Type "traceroute" followed by the destination address to initiate the traceroute process. It continues until it reaches the correct destination reply or a maximum of 30 hops. Users can end the process early by pressing ESC or typing 'q'.	
Examples	Firewall/VPN Router 00000# traceroute 192.168.111.111 Press ESC or q to exit traceroute traceroute to 192.168.127.253 (192.168.127.253), 30 hops max, 46 byte packets 1 192.168.127.253 (192.168.127.253) 0.011 ms 0.007 ms 0.005 ms	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show ip flow export	

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>}

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

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

Related Commands	show ip flow export

Synopsis

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

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

Synopsis

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

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

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

Synopsis

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

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

Synopsis

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

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

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

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

Option Description	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
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show ip flow export	

Synopsis

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

Option Description	no	Reset or disable configuration
	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
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show ip flow export	

Tech Support File

copy tech-support-file

To copy technical support file, use this command.

Synopsis

(config)# **copy tech-support-file** { usb | xmodem } <STRING:password>

(config)# **copy tech-support-file tftp** <STRING:password> <IPV4ADDR:ip>

Option Description	copy	Copy file
	tech-support-file	Run technical support file
	tftp	Copy via TFTP
	usb/xmodem	Copy via USB drive or modem
	password	Password for the USB drive, modem, or TFTP
	IPV4ADDR	TFTP IP address
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	Copy technical support file via TFTP. `(config)# copy tech-support-file tftp <12345678> <192.168.1.2>`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show ip flow export	

copy diagnostic-logging

To import a diagnostic logging profile, use the **copy diagnostic-logging** privileged command.

Synopsis

router# **copy** {tftp <server-IP> diagnostic-logging <file-name> |

scp <account> <password> <server-IP> diagnostic-logging <file-name> |

sftp <account> <password> <server-IP> diagnostic-logging <file-name> |

usb diagnostic-logging <file-name>}

Option Description	<server-IP>	server IP address
	<account>	Account to access remote server
	<password>	Password to access remote server
	diagnostic-logging	Import Diagnostic Logging Profile
Defaults	n/a	
Command Modes	User EXEC	
Usage Guidelines	N/A.	
Examples	`router# copy tftp 192.168.127.100 diagnostic-logging my_debug_settings`	
Error Messages	^Incomplete command	
Related Commands	show diagnostic-logging no diagnostic-logging	

no diagnostic-logging

To reset the diagnostic logging profile to default, use the **no diagnostic-logging** command.

Synopsis

router# **no diagnostic-logging**

Option Description	diagnostic-logging	Reset Diagnostic Logging Profile to default
Defaults	n/a	
Command Modes	User EXEC	
Usage Guidelines	N/A.	
Examples	`router# no diagnostic-logging`	
Error Messages	^Incomplete command	
Related Commands	show diagnostic-logging copy tftp 192.168.127.100 diagnostic-logging my_debug_settings	

show diagnostic-logging

To display diagnostic logging information use the

Synopsis

router# **show diagnostic-logging**

Option Description	diagnostic-logging	Display Diagnostic Logging settings
Defaults	n/a	
Command Modes	User EXEC	
Usage Guidelines	N/A.	
Examples	`router# show diagnostic-logging`	
Error Messages	^Incomplete command	
Related Commands	no diagnostic-logging copy tftp 192.168.127.100 diagnostic-logging my_debug_settings	

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**

Option Description	auto-assign	Enables DHCP server mode as Port-based IP assignment
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Command service dhcp enables DHCP server mode as DHCP/MAC-based assignment.	
Examples	• Enable DHCP server mode to Port-based IP assignment. `router# configure` `router(config)# service dhcp auto-assign` `router(config)# exit` • Enable DHCP server mode to DHCP/MAC-based assignment. `router# configure` `router(config)# service dhcp` `router(config)# exit` • Disable DHCP server mode. `router# configure` `router(config)# no service dhcp` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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 (General DHCP Pool Configuration)

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

Option Description	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
	syslog-server	Specifies syslog servers.
	syslog-ip1	The IP address of the first Syslog server. Default is 0.0.0.0
	syslog-ip2	The IP address of the second Syslog 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-ip1	The IP address of the first NTP server Default is 0.0.0.0
	ntp-ip2	The IP address of the second 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
Defaults	Enabled	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Maximum number of port-based IP pool is 16. • IP-port binding takes precedence over DHCP relay agent.	
Examples	Create a port-based IP assignment: Prerequisites: • TN router: - Interface LAN7: static IP = 192.168.7.252/24, VLAN ID=7 - PORT7: VLAN ID=7 - DHCP server mode: IP-port binding	

	• Device(A) connected on PORT7: - IP: DHCP client Scenario: a) TN router DHCP port-based IP settings: i. IP addresses: from 192.168.7.22 ii. Netmask: 255.255.255.0 iii. Lease time: 1440 minutes iv. Default gateway: 192.168.7.252 v. DNS server 1: 8.8.8.8 vi. DNS server 2: 192.168.8.8 vii. NTP server 1: 192.168.8.9 viii. NTP server 2: 192.168.8.10 ix.Syslog Server 1: 192.168.1.1 x:Syslog Server 2: 192.168.2.2 b) Device(A) can get an DHCP IP: 192.168.7.22 through PORT7. Commands: `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 192.168.8.9 192.168.8.10` `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)# ip syslog-server 192.168.1.1 192.168.2.2` `router(config-if)# exit`
Error Messages	% Invalid parameter!
	^Parse error
	^Incomplete command
Related Commands	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

Set NTP Server (MAC-based Pool Configuration)

(dhcp-config)# **ntp-server** <ntp-ip1> <ntp-ip2>

Option Description	name	A name of the static IP assignment in the DHCP pool. Maximum length is 63.
	lease	Specifies DHCP lease time.
	minutes	A number, 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
	network	Specifies a range of IP addresses in a DHCP pool.
	netmask	Netmask of a DHCP pool. 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 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
	syslog-server	Specifies syslog servers.
	syslog-ip1	The IP address of the first Syslog server. Default is 0.0.0.0
	syslog-ip2	The IP address of the second Syslog 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-ip1	The IP address of the first NTP server Default is 0.0.0.0
	ntp-ip2	The IP address of the second 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
Defaults	Enabled	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Maximum number of static IP in the DHCP pool is 256. • Types a valid name to enter sub-level configuration mode to modify IP assignment settings. • Specify host <ip-addr> <netmask> first before setting lease, hardware-address, dns-server, default-router or ntp-server. Otherwise, error message % Please configure host IP and netmask first will be displayed. • Static IP assignment takes precedence over the dynamic IP assignment as well as DHCP relay agent. • Exits the sub-level configuration mode to let settings take effect.	
Examples	Create a static IP assignment: Prerequisites: • TN router: - Interface LAN6: static IP = 192.168.6.254/24, VLAN ID=6 - PORT6: VLAN ID=6 - DHCP server mode: Dynamic/Static IP assignment • Device(A) connected on PORT6: - IP: DHCP client Scenario: a) TN router DHCP static IP settings: i. Name: P6-static ii. IP addresses: from 192.168.6.1 iii. Netmask: 255.255.255.0 iv. MAC address: 00:90:e8:00:f2:ac v. Lease time: 2880 minutes vi. Default gateway: 192.168.6.254 vii. DNS server 1: 8.8.8.8 viii. DNS server 2: 192.168.8.8 ix. NTP server: 192.168.8.9 x. NTP server: 192.168.8.10 xi.Syslog Server 1: 192.168.1.1 xii:Syslog Server 2: 192.168.2.2 b) Device(A) can get an DHCP IP: 192.168.6.1 through PORT6. Commands:	

	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 192.168.8.9 192.168.8.10 router(dhcp-config)# syslog-server 192.168.1.1 192.168.2.2 router(dhcp-config)# exit
Error Messages	% Invalid parameter!
	% Can not find the entry
	^Parse error
	^Incomplete command
Related Commands	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

Set NTP Server (Port-based Pool Configuration)

(dhcp-config)# **ntp-server** <ntp-ip1> <ntp-ip2>

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	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.
	syslog-server	Specifies syslog servers.
	syslog-ip1	The IP address of the first Syslog server. Default is 0.0.0.0
	syslog-ip2	The IP address of the second Syslog server. Default is 0.0.0.0
	default-router	Specifies the default router.
	dr-ip	The IP address of the default router.
	ntp-server	Specifies the NTP server.
	ntp-ip1	The IP address of the first NTP server Default is 0.0.0.0
	ntp-ip2	The IP address of the second NTP server Default is 0.0.0.0
	lease	Specifies DHCP lease time
	minutes	A number, ranges from 5 to 527039
	dhcp-relay	Specifies to enable/disable dhcp-relay function.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Maximum number of static IP in the DHCP pool is 256. • Types a valid name to enter sub-level configuration mode to modify IP assignment settings. • Specify host <ip-addr> <netmask> first before setting lease, hardware-address, dns-server, default-router or ntp-server. Otherwise, error message % Please configure host IP and netmask first will be displayed. • Static IP assignment takes precedence over the dynamic IP assignment as well as DHCP relay agent. • • Exits the sub-level configuration mode to let settings take effect.	
Examples	Create a static IP assignment: Prerequisites:	

	• TN router: - Interface LAN6: static IP = 192.168.6.254/24, VLAN ID=6 - PORT6: VLAN ID=6 - DHCP server mode: Dynamic/Static IP assignment • Device(A) connected on PORT6: - IP: DHCP client Scenario: a) TN router DHCP static IP settings: i. Name: P6-static ii. IP addresses: from 192.168.6.1 iii. Netmask: 255.255.255.0 iv. MAC address: 00:90:e8:00:f2:ac v. Lease time: 2880 minutes vi. Default gateway: 192.168.6.254 vii. DNS server 1: 8.8.8.8 viii. DNS server 2: 192.168.8.8 ix. NTP server: 192.168.8.9 x. NTP server: 192.168.8.10 xi.Syslog Server 1: 192.168.1.1 xii:Syslog Server 2: 192.168.2.2 b) Device(A) can get an DHCP IP: 192.168.6.1 through PORT6. Commands: `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 192.168.8.9 192.168.8.10` `router(dhcp-config)# syslog-server 192.168.1.1 192.168.2.2` `router(dhcp-config)# exit`
Error Messages	% Invalid parameter!
	% Can not find the entry
	^Parse error
	^Incomplete command
Related Commands	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

Save and Exit DHCP pool configuration

(dhcp-config)# **exit**

Enable / Disable the DHCP pool

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

Set syslog server

(config-if)# **syslog-server** <syslog-ip1> <syslog-ip2>

Option Description	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
	syslog-server	Specifies syslog servers.
	syslog-ip1	The IP address of the first Syslog server. Default is 0.0.0.0
	syslog-ip2	The IP address of the second Syslog 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
Defaults	Enabled.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Maximum number of pools is 32. • No modification function is provided. In case modification on a specific index is required, remove it first and then add a new setting. • Type a valid index to enter sub-level configuration mode. • Specify **network** <first-ip> <last-ip> <netmask> first before setting **lease**, **dns-server**, **default-router** or **ntp-server**. Otherwise, error message **% Please configure offered network first** will be displayed. • Static IP assignment takes precedence over the dynamic IP assignment as well as DHCP relay agent. • Exit the sub-level configuration mode to let settings take effect.	
Examples	Create a DHCP pool for dynamic IP assignment: Prerequisites: • TN router: - Interface LAN5: static IP = 192.168.5.254/24, VLAN ID=5; - PORT5: VLAN ID=5 - DHCP server mode: Dynamic/Static IP assignment • Device(A) connected on PORT5: - IP: DHCP client Scenario: a) TN router DHCP pool settings: i. IP addresses: from 192.168.5.1 to 192.168.5.10 ii. Netmask: 255.255.255.0 iii. Lease time: 2880 minutes iv. Default gateway: 192.168.5.254 v. DNS server 1: 8.8.8.8 vi. DNS server 2: 192.168.8.8 vii. NTP server: 192.168.8.9 viii.Syslog Server 1: 192.168.1.1 ix:Syslog Server 2: 192.168.2.2 b) Device(A) can get an DHCP IP: 192.168.5.1 through PORT5.	

	Commands: `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)# syslog-server 192.168.1.1 192.168.2.2` `router(dhcp-config)# exit`
Error Messages	% Invalid parameter!
	% Can not find the entry
	^Parse error
	^Incomplete command
Related Commands	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

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**}

Set syslog server

(dhcp-config)# **syslog-server** <syslog-ip1> <syslog-ip2>

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
	syslog-server	Specifies syslog servers.
	syslog-ip1	The IP address of the first Syslog server. Default is 0.0.0.0
	syslog-ip2	The IP address of the second Syslog 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.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Maximum number of static IP in the DHCP pool is 256. • Types a valid name to enter sub-level configuration mode to modify IP assignment settings. • Specify host <ip-addr> <netmask> first before setting **lease**, **hardware-address**, **dns-server**, **default-router** or **ntp-server**. Otherwise, error message **% Please configure host IP and netmask first** will be displayed. • Static IP assignment takes precedence over the dynamic IP assignment as well as DHCP relay agent. • Exits the sub-level configuration mode to let settings take effect.	
Examples	Create a static IP assignment: Prerequisites: • TN router: - Interface LAN6: static IP = 192.168.6.254/24, VLAN ID=6 - PORT6: VLAN ID=6 - DHCP server mode: Dynamic/Static IP assignment • Device(A) connected on PORT6: - IP: DHCP client Scenario: a) TN router DHCP static IP settings: i. Name: P6-static ii. IP addresses: from 192.168.6.1 iii. Netmask: 255.255.255.0 iv. MAC address: 00:90:e8:00:f2:ac v. Lease time: 2880 minutes vi. Default gateway: 192.168.6.254 vii. DNS server 1: 8.8.8.8	

	viii. DNS server 2: 192.168.8.8 ix. NTP server: 192.168.8.9 x.Syslog Server 1: 192.168.1.1 xi:Syslog Server 2: 192.168.2.2 b) Device(A) can get an DHCP IP: 192.168.6.1 through PORT6. Commands: `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)# syslog-server 192.168.1.1 192.168.2.2` `router(dhcp-config)# exit`
Error Messages	^Parse error
	^Incomplete command
	% Please configure host IP and netmask first.
Related Commands	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

ip dhcp-relay

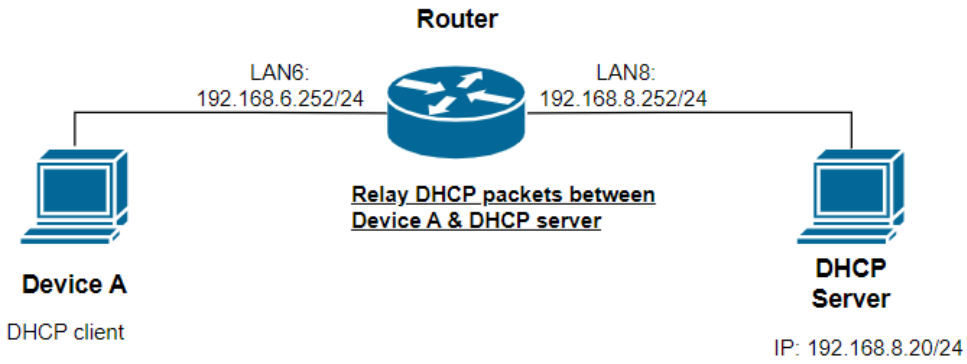
To enable a DHCP relay agent, use the **ip dhcp-relay** global configuration command. To disable DHCP relay agent, use **no** form of this command.

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}

Option Description	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
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• If dynamic/static IP assignment or IP-port binding is specified, DHCP relay agent will not take effect in this case. • Static IP assignment takes precedence over the dynamic IP assignment as well as DHCP relay agent. • For DHCP option 82 feature, the CLI command (config)# ip dhcp-relay option82 remote-id-type **ip** is replaced with (config)# ip dhcp-relay option82 remote-id-type **interface WAN**.	
Examples	DHCP relay agent: Prerequisites: • TN router: - LAN6: 192.168.6.252/24, VLAN ID=6, interface used for DHCP clients - LAN8: 192.168.8.252/24, VLAN ID=8, interface used for the DHCP server • Device(A) on subnet 192.168.6.0/24: - IP: DHCP client • DHCP Server on subnet 192.168.8.0/24: - IP: 192.168.8.20/24 - Server settings: 1) IP pool: 192.168.6.11 to 192.168.6.15 2) Circuit-ID: 0x01000606 3) Remote-ID: 0x31323334 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)#`
Error Messages	% Invalid parameter!
	% Invalid outbound Interface Name.
	% Invalid interface!
	% Please configure offered network first.
	^Parse error
	^Incomplete command
Related Commands	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**

Set syslog server

(config-if)# **ip syslog-server** <syslog-ip1> <syslog-ip2>

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	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.
	syslog-server	Specifies syslog servers.
	syslog-ip1	The IP address of the first Syslog server. Default is 0.0.0.0
	syslog-ip2	The IP address of the second Syslog server. Default is 0.0.0.0
	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	

Usage Guidelines	• Maximum number of port-based IP pool is 16. • IP-port binding takes precedence over DHCP relay agent.
Examples	Create a port-based IP assignment: Prerequisites: • TN router: - Interface LAN7: static IP = 192.168.7.252/24, VLAN ID=7 - PORT7: VLAN ID=7 - DHCP server mode: IP-port binding • Device(A) connected on PORT7: - IP: DHCP client Scenario: a) TN router DHCP port-based IP settings: i. IP addresses: from 192.168.7.22 ii. Netmask: 255.255.255.0 iii. Lease time: 1440 minutes iv. Default gateway: 192.168.7.252 v. DNS server 1: 8.8.8.8 vi. DNS server 2: 192.168.8.8 vii. NTP server: 192.168.8.9 viii.Syslog Server 1: 192.168.1.1 ix:Syslog Server 2: 192.168.2.2 b) Device(A) can get an DHCP IP: 192.168.7.22 through PORT7. Commands: `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)# ip syslog-server 192.168.1.1 192.168.2.2` `router(config-if)# exit`
Error Messages	% Illegal parameter
	^Parse error
	^Incomplete command
Related Commands	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

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**}]

Option Description	static	Specifies to display static DHCP client list
	binding	Specifies to display dynamic DHCP client list
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	• Display static DHCP client list. (MAC-based) `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 1 : 192.168.8.9 NTP Server 2 : 192.168.8.10` `DNS Server 1 : 8.8.8.8 DNS Server 2 : 192.168.8.8` `Syslog Server 1 : 192.168.1.1 Syslog Server 2 : 192.168.2.2` • Display dynamic DHCP client list. (General) `router# show ip dhcp` `DHCP Server Mode : Dynamic/Static IP Assignment` `Dynamic DHCP Pool List` `----------` `Index : 1 State : Enable` `First IP Address : 192.168.127.150 Last IP Address: 192.168.127.160` `Netmask : 255.255.255.0 Lease Time(min) : 1440` `Default Gateway : 192.168.127.249` `NTP Server 1 : 1.2.3.4 NTP Server 2 : 1.2.3.5` `DNS Server 1 : 8.8.8.8 DNS Server 2 : 168.95.1.1` `Syslog Server 1 : 1.1.1.1 Syslog Server 2 : 2.2.2.2` `----------`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ip dhcp static pool interface ethernet ip	

show ip dhcp classless-static-route

To check the IP DHCP classless static route, use the **show ip dhcp classless-static-route** command.

Synopsis

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	

Examples	Firewall/ETBN Router 00000# show ip dhcp classless-static-route Classless Static Route Table --- Name IP Address Subnet Mask Gateway Member Port --- TEST 192.168.128.42 255.255.255.254 1.1.1.1 1/10,1/12,1/13
Error Messages	^Parse error ^Incomplete command
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	router# show ip auto-assign Port-based IP Pool List --- Port : 9 State : Enable Static IP Address : 192.168.127.170 Netmask: 255.255.255.0 Lease Time(min) : 1440 Default Gateway : 0.0.0.0 NTP Server 1 : 1.2.3.5 NTP Server 2 : 1.2.3.5 DNS Server 1 : 0.0.0.0 DNS Server 2 : 0.0.0.0 Syslog Server 1 : 0.0.0.0 Syslog Server 2 : 0.0.0.0 ---	
Error Messages	^Parse error ^Incomplete command	
Related Commands	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

Option Description	N/A	
Defaults	N/A	

Command Modes	Privileged EXEC / User EXEC
Usage Guidelines	N/A
Examples	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
Error Messages	^Parse error
	^Incomplete command
Related Commands	interface ethernet ip

duplicate-ip-detection

To enable or disable duplicate IP detection function, use the **duplicate-ip-detection** configuration mode command. To disable, use the **no** form of the command.

Synopsis

(config)# **duplicate-ip-detection enable**

(config)# **no duplicate-ip-detection enable**

Option Description	enable	Enable IP detection function
Defaults	Enabled	
Command Modes	Configuration mode	
Usage Guidelines	N/A	

Examples	Enable `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config-if)# duplicate-ip-detection enable` Dinable `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config-if)# no duplicate-ip-detection enable`
Error Messages	N/A
Related Commands	N/A

DNS Server

The following commands apply to TN-4900 models only.

show ip dns-server

To show DNS server configuration and status, use the **show ip dns-server** command.

Synopsis

show ip dns-server [zone [<zone-index(1-16)>]]

Option Description	show	Display configuration/status information
	Ip	Display IP information
	dns-server	DNS server configuration
	zone	zone configuration
	<zone-index(1-16)>	zone index number
Default	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000# show ip dns-server` `DNS Server: Enable` `DNS Reverse Lookup: Enable` `Firewall/VPN Router 00000# show ip dns-server zone` `Zone Table:` `----------` `Index  Domain Name` `ZONE-1  a` `ZONE-2  b` `ZONE-10  k` `----------` `Total zones: 3` `Firewall/VPN Router 00000# show ip dns-server zone 1` `ZONE-1` `Domain name: a` `DNS table:` `----------`	

	FQDN IP Address 1.door.ext.a 10.1.2.1 2.door.ext.a 10.1.2.2 --- Total entries: 2
Error Message	N/A
Related Commands	N/A

dns-server [{enable | disable}]

To enable or disable DNS server global function, use the **dns-server [{enable | disable}]** command.

Synopsis

(config)# **dns-server [{ enable | disable }]**

Option Description	dns-server	DNS server configuration
	enable	Enable assignment
	disable	Disable assignment
Defaults	disabled	
Command Modes	Configuration Mode	
Usage Guidelines	N/A	
Examples	Firewall/VPN Router 00000(config)# dns-server enable	
Error Messages	N/A	
Related Commands	N/A	

ip dns-server reverse-lookup

To enable DSN server reverse lookup function, use the **ip dns-server reverse-lookup** command.

Synopsis

(config)# **ip dns-server reverse-lookup**

Option Description	ip	Display IP information
	dns-server	DNS server configuration
	reverse-lookup	Enable DNS reverse-lookup
Defaults	disabled	
Command Modes	Configuration Mode	
Usage Guidelines	N/A	
Examples	Firewall/VPN Router 00000(config)# ip dns-server reverse-lookup	
Error Messages	N/A	
Related Commands	no ip dns-server reverse-lookup	

no ip dns-server reverse-lookup

To disable DSN server reverse lookup function, use the **no ip dns-server reverse-lookup** command.

Synopsis

(config)# **ip dns-server reverse-lookup**

Option Description	no	Disable the configuration/reset to default value
	ip	Display IP information
	dns-server	DNS server configuration
	reverse-lookup	Enable DNS reverse-lookup
Defaults	disabled	
Command Modes	Configuration Mode	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000(config)# no ip dns-server reverse-lookup`	
Error Messages	N/A	
Related Commands	ip dns-server reverse-lookup	

ip dns-server zone

To configure DNS server zone parameters, use the **ip dns-server zone** command.

Synopsis

(config)# **ip dns-server zone** <**zone-index** (1-16)> [**domain-name** <string(63)>

Option Description	ip	Configure IP parameters
	dns-server	DNS server configuration
	zone	Zone configuration
	<zone-index(1-16)>	Zone index as an integer between 1-16.
	domain-name	Domain name option for the zone.
	<string(63)>	Specify domain name.as a string. Permitted characters： [a-zA-Z0-9.-]. Additionally, the following may be used as any character but the first or last: '.' & '-' Maximum 63 characters long.
Defaults	Disabled	
Command Modes	Configuration Mode	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000(config)# ip dns-server zone 3 domain-name xxx`	
Error Messages	% Incomplete command.	
	% Invalid: The given Domain Name does not represent a valid Domain Name.	
	% Invalid Index. It must be 1 - 16	
	% Invalid: The same zone domain has already been used by another entry.	
	% Invalid: This domain is already used by a DNS forwarding entry. Use a different domain, or a more specific sub-domain.	
	% Invalid: <FQDN> is also used by a DNS forwarding entry.	
Related Commands	no ip dns-server zone { <zone-index(1-16)> | all }	

no ip dns-server zone

To clear zone command, use **no ip dns-server zone** command.

Synopsis

(config)# **no ip dns-server zone** { <zone-index(1-16)> | all }

Option Description	no	Delete the entry/reset to the default value
	ip	Configure IP parameters
	dns-server	DNS server configuration
	zone	Zone configuration option
	<zone-index(1-16)>	Zone index as an integer between 1-16..
	all	Clear all zone configurations
Defaults	disabled	
Command Modes	Configuration Mode	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000(config)# no ip dns-server zone 3` `Firewall/VPN Router 00000(config)# no ip dns-server zone all`	
Error Messages	% this zone is not created, domain name of this zone should be set first	
Related Commands	ip dns-server zone <zone-index (1-16)> [domain-name <string(63)>]	

hostname <hostname(63)> ip <ucast_addr>

To edit zone entry command, use **hostname** command.

Synopsis

(config-dns-server-zone)# **hostname** <hostname(63)> ip <ucast_addr>

Option Description	hostname	Hostname for DNS entry
	<string(63)>	<hostname(63)> only accept [a-zA-Z0-9.-], while '.' & '-' cannot be at the begin or end. Maximum 63 characters of <hostname(63)> length. if not, error message
	ip	IP address for DNS entry
	A.B.C.D(<ip_addr>)	Unicast IP address
Defaults	N/A	
Command Modes	Zone submode configuration	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000(config)# ip dns-server zone 3` `Firewall/VPN Router 00000(config-dns-server-zone)# hostname test ip 1.1.1.1` `Firewall/VPN Router 00000(config-dns-server-zone)# exit`	
Error Messages	% Invalid: The given IP Address does not represent a valid IPv4 address.:	
	% Invalid: The given Hostname does not represent a valid Hostname.	
	% Invalid: The same hostname has already existed	
	% Invalid: can't set more than 256 DNS entries	
Related Commands	no hostname <hostname(63)>	

no hostname <hostname(63)>

To remove zone entry by hostname command, use the **no hostname** command.

Synopsis

(config-dns-server-zone)# **no hostname** <hostname(63)>

Option Description	no	Delete the entry/reset to default value
	hostname	Hostname for DNS entry
	<string(63)>	Hostname
Defaults	N/A	
Command Modes	Zone submode configuration	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000(config-dns-server-zone)# no hostname test`	
Error Messages	N/A	
Related Commands	no hostname <hostname(63)> ip <ucast_addr>	

no ip <ucast_addr>

To remove zone entry by IP command, use **no ip** command.

Synopsis

(config-dns-server-zone)# **no ip** <ucast_addr>

Option Description	no	Delete the entry/reset to default value
	ip	IP address for DNS entry
	A.B.C.D(<ip_addr>)	Unicast IP address
Defaults	N/A	
Command Modes	Zone submode configuration	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000(config)# ip dns-server zone 3` `Firewall/VPN Router 00000(config-dns-server-zone)# no ip 1.1.1.1` `Firewall/VPN Router 00000(config-dns-server-zone)# exit`	
Error Messages	N/A	
Related Commands	hostname <hostname(63)> ip <ucast_addr>	

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**

Option Description	service	Specifies a DDNS service
	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
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	% Password Length should <= 45	
	% Server Name Error	
	^Parse error	
	^Incomplete command	
Related Commands	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

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

Other Commands

terminal

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

Synopsis

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

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

Option Description	install	Specifies to install designated package
	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
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	• <pkg-name> is case-sensitive. • If the package is already present, utilize the "upgrade" command instead of the "install" command. • 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.	
Examples	• Upgrade security package via TFTP `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 transfering...` `Verified OK` `Checking Package...Package is importing now, please wait!` `All checking are ok.` `Package upgrade successfully.` `router#` • Upgrade security package via built-in firmware `router# package upgrade security firmware` `Upgrade to security buildin package` `Buildin package upgrade successfully.` `router#`	
Error Messages	% 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	
Related Commands	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

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

Option Description	secret-seed	A set of characters without a whitespace. The length must range from 4 to 8.
Defaults	Disabled	
Command Modes	Privileged EXEC	
Usage Guidelines	• This command is exclusively intended for troubleshooting by Moxa staff. • The engineering mode will be disabled after system reboot. • The <secret-seed> will become invalid after the next reboot . • CLI command “show moxasupport” displays default status.	
Examples	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.	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

show integrity

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

Synopsis

show integrity

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	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.	
Examples	Display status of integrity check. `router # show integrity` `Application: OK` `Configuraion: OK` `router #`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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** <string: code (1024)>

Option Description	<string: code (1024)>	activation code
Defaults	n/a	
Command Modes	Global configuration	
Usage Guidelines	Limited to supervisor privilege or above.	
Examples	`router# configure` `router(config)# license activation {YOUR_ACTIVATION_CODE}`	
Error Messages	License activation failed – Internal error!	
	License activation failed – Invalid activation code!	
	License activation failed – Invalid license!	
	License activation failed – The {NUMBER}-month grace period has expired! where {NUMBER} = 6 for now.	
	License activation failed – Duplicated activation code!	
	License activation failed – License point over limit ({NUMBER})! where {NUMBER} = 3650 for now.	
	License activation failed – Combination violation when license import!	
	^Incomplete command	
Related Commands	show license overview <feature ID> show license history <feature ID>	

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>

Option Description	**Overview**	Specifies to display overview information
	History	Specifies to display historical information
	feature-id	Feature IDs: IPS: 1
Defaults	N/A	
Command Modes		
Usage Guidelines	N/A	
Examples	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`	
Error Messages	% Invalid feature ID!	
	^Parse error	
	^Incomplete command	
Related Commands	N/A	

2. 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 **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information. • Enter configuration mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	(config)#	To exit to privileged EXEC mode, enter **exit**.	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example **interface ethernet** <mod-port> command and press enter	(config-if)#	To exit to global configuration mode, enter **exit**.	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**

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	exit	Commit new settings and exit sub-level configuration mode.
	shutdown	Disables the Ethernet port.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	• Disable PORT9: `router# configure` `router(config)# interface ethernet 1/9` `router(config-if)# shutdown` `router(config-if)# exit` • Enable PORT9: `router# configure` `router(config)# interface ethernet 1/9` `router(config-if)# no shutdown` `router(config-if)# exit`	
Error Messages	% Illegal parameter	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• The port's name is composed of a maximum of 5 tokens, with a whitespace positioned between each token. • The format of the token must be a-z, A-Z, 0-9 or . - _ @ ! # $ % ^ & * ( ). / • Maximum length of port name including whitespaces is 127.	
Examples	Set PORT9's name to "DCU 2". In this example, token1=DCU token2=2 `router# configure` `router(config)# interface ethernet 1/9` `router(config-if)# name DCU 2` `router(config-if)# exit`	
Error Messages	% Length of port name is too long	
	% Not in correct format	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	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.
Defaults	Auto.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	% Illegal parameter	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	flowcontrol	Enables flow control for this port when the port's Speed is set to Auto.
Defaults	Disabled.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	Set speed-duplex to Auto before enabling flow control.	
Examples	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`	
Error Messages	% Illegal parameter	
	% Force speed can not be set flow control!!	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	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
Defaults	Auto	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	% Illegal parameter	
	^Parse error	
	^Incomplete command	
Related Commands	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}]

Option	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
Description	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
Defaults	N/A	

Command Modes	Global configuration, sub-level configuration
Usage Guidelines	• To proceed with PD Failure Check or Scheduling mentioned in this instruction, it's necessary to have PoE power output enabled beforehand. • To proceed with Scheduling mentioned in this instruction, it's necessary to create a scheduling rule beforehand.
Examples	• Specifies Output mode to Force and allocate 30 watts power for PORT4: `router# configure` `router(config)# interface ethernet 1/4` `router(config-if)# poe enable` `router(config-if)# poe force budget 30` `router(config-if)# exit` • Enable PD Failure Check and reboot PD after 5 cycles attempt (20 seconds per cycle) without success for PORT4: `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` • Apply schedule rule "rule-example" for PORT4: `router# configure` `router(config)# interface ethernet 1/4` `router(config-if)# poe scheduling rule-example` `router(config-if)# exit`
Error Messages	% 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
Related Commands	show interfaces ethernet poe system poe scheduling

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}

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	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.
Defaults	• Default native vlan is 1. • Default access vlan is 1.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command • Make sure the VLAN ID is created in advance before using it.	
Examples	• Set access VLAN ID (10) to PORT7: `router# configure` `router(config)# interface ethernet 1/7` `router(config-if)# switchport access vlan  10` `router(config-if)# exit` • For Trunk-group 2, change port type from "Access" to "Trunk" and return access VLAN ID to default value 1. `router# configure` `router(config)# interface trunk 2` `router(config-if)# no switchport trunk native vlan` `router(config-if)# exit` • For Trunk-group 2, add a tagged VLAN 5 when trunk type is specified. `router# configure` `router(config)# interface trunk 2` `router(config-if)# switchport trunk fixed vlan add 5` `router(config-if)# exit`	

	• For Trunk-group 2, remove all tagged VLAN when trunk type is specified. `router# configure` `router(config)# interface trunk 2` `router(config-if)# no switchport trunk fixed vlan` `router(config-if)# exit`
Error Messages	% VLAN id is out of range!
	vlan id does not exist!!
	^Parse error
	^Incomplete command
Related Commands	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**]]

Option Description	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.
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	• Display overall port settings and status. `router# show interfaces ethernet` `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                --        --            --` • Display general settings for port 2. `router# show interfaces ethernet 1/2 config` `Port Enable Type   Description    Speed    FDX Flow Ctrl MDI/MDIX` `---- ------ ------ -------------- -------- ------------- --------` `1/2  Yes    100TX  100TX          Auto     Disable       Auto` • Display rate-limit settings for port 2. `router# # show interfaces ethernet 1/2 rate-limit` `Port 1/2:` `    Ingress Limit Rate: Not Limited` `    Egress Limit Rate : Not Limited` • Display packet counter information for port 2. `router# show interfaces ethernet 1/2 counters` `Port 1/2 (last sample time: 604613 secs ago)` `  - TX -` `    Unicast Packets      : 421628          +421628` `    Multicast Packets    : 20056           +20056`	

	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
Error Messages	^Parse error
	^Incomplete command
Related Commands	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**

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	% Trunk ID is only allowed from 1 to 4	
	^Parse error	
	^Incomplete command	

Related Commands	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**

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command.	
Examples	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`	
Error Messages	% There is no member in Trunk	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• The trunk port name is composed of a maximum of 5 tokens, with a whitespace positioned between each token. • The format of the token must be a-z, A-Z, 0-9 or . - _ @ ! # $ % ^ & * ( ). / • Maximum length of trunk port's name including whitespaces is 127. • Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command	
Examples	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`	
Error Messages	% Length of port name is too long.	
	% Not in correct format	
	^Parse error	
	^Incomplete command	
Related Commands	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}

<table>
<tr><td rowspan="15">Option Description</td><td>trunk-id</td><td>Trunk group ID. Maximum number of trunk groups differs among different models.</td></tr>
<tr><td>switchport</td><td>Specifies VLAN types</td></tr>
<tr><td>access vlan</td><td>Specifies VLAN type: Access. Connects single devices without tags.</td></tr>
<tr><td>vlan-id</td><td>Ranges from 1 to 4094.</td></tr>
<tr><td>trunk</td><td>Specifies VLAN type: Trunk. Connects another 802.1Q VLAN aware switch.</td></tr>
<tr><td>fixed vlan</td><td>Specifies other VLAN ID for tagged devices that connect to the port.</td></tr>
<tr><td>vlan-ids</td><td>Ranges from 1 to 4094. Use commas to separate different VLAN IDs.</td></tr>
<tr><td>add</td><td>Specifies to add tagged VLAN.</td></tr>
<tr><td>remove</td><td>Specifies to remove tagged VLAN.</td></tr>
<tr><td>tag</td><td>Specifies tagged VLAN IDs</td></tr>
<tr><td>untag</td><td>Specifies untagged VLAN IDs</td></tr>
<tr><td>native vlan</td><td>Specifies the default VLAN ID for untagged devices that connect to the port</td></tr>
<tr><td>hybrid</td><td>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.</td></tr>
<tr><td>Defaults</td><td colspan="2">• Default native vlan is 1.
• Default access vlan is 1.</td></tr>
<tr><td>Command Modes</td><td colspan="2">Global configuration, sub-level configuration</td></tr>
<tr><td>Usage Guidelines</td><td colspan="2">• Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command.
• Make sure the VLAN ID is created in advance before using it.</td></tr>
<tr><td>Examples</td><td colspan="2">• 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>• 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>• 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></td></tr>
<tr><td rowspan="4">Error Messages</td><td colspan="2">% VLAN id is out of range!</td></tr>
<tr><td colspan="2">vlan id does not exist!!</td></tr>
<tr><td colspan="2">^Parse error</td></tr>
<tr><td colspan="2">^Incomplete command</td></tr>
<tr><td>Related Commands</td><td colspan="2">interface ethernet
show interfaces trunk</td></tr>
</table>

show interfaces trunk

To show Link Aggregation settings, use the **show interfaces trunk** command.

Synopsis

show interfaces trunk { <LF> | <STRING:trunk_id_range> | lacp }

Option Description	show	Display configuration/status information
	interfaces	Display interface status and configuration
	trunk	Display interface trunk configuration
	<STRING:trunk_id_range>	Channel ID
	lacp	Display LACP status
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	To show Link Aggregation settings: `Firewall/VPN Router 00000# show interfaces trunk` `Trk#  Type  Enable Description  Speed` `----  -----  ------- -------------  -------` `1  Static  Yes  Auto` `2  LACP  Yes  Auto` Only show Link Aggregation settings on trunk 2: `Firewall/VPN Router 00000# show interfaces trunk 2` `Trunk-2` `Name :` `Type : LACP` `Member  Status` `------ ----------` `1/3  Success` `1/4  Success` `Trunk-1 Port 3` `Type: LACP` `Actor  Partner` `System Priority: 1  1` `System ID: 00:90:e8:a9:ed:0d  00:00:00:00:00:00` `Key (Channel ID): 1  0` `Port Priority: 1  1` `Port: 3  0` `LACP Activity: Active  Passive` `LACP Timeout: Long Timeout  Long Timeout` `Aggregation: Aggregatable  Individual` `Synchronization: In Sync  Out Of Sync` `Collecting: Disabled  Disabled` `Distributing: Disabled  Disabled` `Defaulted: True  True` `Expired: False  False` `Trunk-1 Port 4` `Type: LACP` `Actor  Partner` `System Priority: 1  1` `System ID: 00:90:e8:a9:ed:0d  00:00:00:00:00:00` `Key (Channel ID): 1  0`	

	Port Priority: 1 1 Port: 3 0 LACP Activity: Active Passive LACP Timeout: Long Timeout Long Timeout Aggregation: Aggregatable Individual Synchronization: In Sync Out Of Sync Collecting: Disabled Disabled Distributing: Disabled Disabled Defaulted: True True Expired: False False To show Link Aggregation port settings: Firewall/VPN Router 00000# show interfaces trunk lacp Port Mode Timeout (sec.) Wait Time (sec.) Port Channel (Trunk) ---- ------- ------------ ------------ -------- ------- 1/1 Active 90 2 1 1/2 Active 90 2 1 1/3 Active 90 2 -- 1/4 Active 90 2 -- 1/5 Active 90 2 -- 1/6 Active 90 2 -- 1/7 Active 90 2 -- 1/8 Active 90 2 -- •
Error Messages	N/A
Related Commands	N/A

trunk-mode lacp

To configure Link Aggregation for LACP mode, use the **trunk-mode lacp** command.

Synopsis

(config-if)# **trunk-mode lacp**

Option Description	trunk-mode	Trunk mode configuration
	lacp	LACP mode
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	To configure LACP mode: Firewall/VPN Router 00000# configure Firewall/VPN Router 00000(config)# interface ethernet 1/1 Firewall/VPN Router 00000(config-if)# trunk-mode lacp	
Error Messages	N/A	
Related Commands	N/A	

trunk-mode lacp timeout

To configure Link Aggregation for LACP timeout, use the **trunk-mode lacp timeout** command.

Synopsis

(config-if)# **trunk-mode lacp timeout** { short | long }

Option Description	trunk-mode	Trunk mode configuration
	lacp	LACP mode
	timeout	LACP timeout
	short	short timeout (3 seconds)
	long	long timeout (90 seconds)
Defaults	long	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	To configure LACP timeout short: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# trunk-mode lacp timeout short` To configure LACP timeout long: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# trunk-mode lacp timeout long`	
Error Messages	N/A	
Related Commands	N/A	

trunk-mode lacp wait-time

To configure Link Aggregation for LACP wait time, use the **trunk-mode lacp wait-time** command.

Synopsis

(config-if)# **trunk-mode lacp wait-time** <UINT:seconds>

Option Description	trunk-mode	Trunk mode configuration
	lacp	LACP mode
	wait-time	LACP wait time
	<UINT:seconds>	Time in seconds
Defaults	2	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	To configure LACP wait time for 5 seconds: `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# interface ethernet 1/1` `Firewall/VPN Router 00000(config-if)# trunk-mode lacp wait-time 5`	
Error Messages	If wait-time option is not in 0 to 10 seconds, the error message is shown:	
	% Invalid: LACP wait time is invalid. It must be 0-10 seconds.	
Related Commands	N/A	

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**}]

Option Description	enable	Specifies to enable PoE power output
	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
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• To proceed with threshold or cutoff settings, it's necessary to have PoE power output enabled beforehand. • When Auto Power Cutt-off is disabled, the router will calculate power budget based on the Power Allocation settings of all ports. • Adjustability of the PoE power budget varies across different models.	
Examples	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`	
Error Messages	% Power threshold should be between 30 and 95.	
	% System power budget should be between 95 and 95.	
	^Parse error	
	^Incomplete command	
Related Commands	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>}

Option Description	rule-name	Specifies a name for the scheduling rule. Max. length is 63.
	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.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	To proceed with scheduling settings, it's necessary to have PoE power output enabled beforehand.	
Examples	• Create a rule-example to schedule 8 a.m. to 6 p.m. on weekdays: `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` • Delete the rule "rule-example": `router# configure` `router(config)# no poe scheduling rule-example` `router(config)# exit`	
Error Messages	% 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	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	Output only available on PoE models.	
Examples	Firewall/ETBN Router 00000# 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 : 0 Watts** ** Sum of measured power : 0 Watts** ** PSE input voltage (VEE): 54 Volts** ** ** +----------+ | Power Consumption Voltage Current PD Failure PD Status | |Port Status Output Class (W) (V) (mA) Check Description| +---- ------- ------ ------ ----------- ------- ------- ------------+ ** 1/1 Disable Off N/A N/A N/A N/A Disable Disabled** ** 1/2 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/3 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/4 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/5 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/6 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/7 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/8 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/11 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/12 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/15 Enable Off N/A N/A N/A N/A Disable Not Present** ** 1/16 Enable Off N/A N/A N/A N/A Disable Not Present**	
Error Messages	% Not support POE on this switch	
	^Parse error	
	^Incomplete command	
Related Commands	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}

Option Description	rstp	Rapid Spanning Tree
	turbo-ring-v2	Turbo ring version 2
Defaults	The default redundancy protocol mode is RSTP.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	* An illustrative example can be found in the command "**redundancy spanning-tree**" and "**redundancy turbo-ring-v2**".	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show redundancy mode	

show redundancy mode

To check the redundancy mode on the router, use the **show redundancy mode** command.

Synopsis

show redundancy mode

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`router# show redundancy mode` `  Current redundancy mode  : Turbo Ring V2`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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.

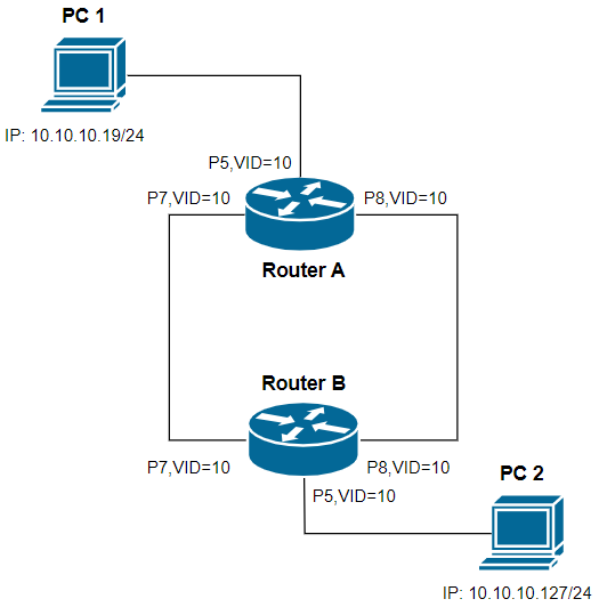
Synopsis

(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}

Option Description	exit	Commit new settings and exit sub-level configuration mode
	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
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• 2*(hello-time + 1.0 sec) <= max-age <= 2*(forward-delay - 1.0 sec) • Enable spanning-tree feature in the command "**interface ethernet**" to let RSTP take effect.	
Examples	Specify RSTP on two routers: Prerequisites: • TN router A: - P5: VLAN ID=10 - RSTP ports: P7 and P8 • TN router B: - P5: VLAN ID=10 - RSTP ports: P7 and P8 • PC-1: - IP: 10.10.10.19/24 • PC-2 : - IP: 10.10.10.127/24	

Network topology:



Scenario:
a) 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.
b) PC (1) and PC (2) can communicate with each other via Router (A) and Router (B).
c) 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 x (Hello Time + 1 sec) <= Max age <= 2 x (Forward Delay - 1 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
Related Commands	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 }]

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A.	
Examples	* An illustrative example can be found in the command "**redundancy spanning-tree**".	
Error Messages	% 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	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error messages	^Parse error	
	^Incomplete command	
Related Commands	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	

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.

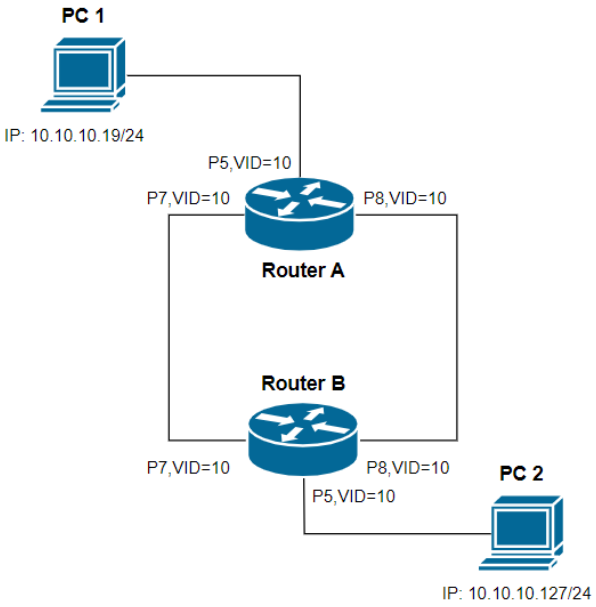
Synopsis

(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}

Option Description	exit	Commit new settings and exit sub-level configuration mode
	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
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	At least enable one turbo-ring domain or coupling. But cannot enable two turbo-ring domains and coupling at the same time.	
Examples	Specify Turbo Ring v2 on two routers: Prerequisites: • TN router A: - P5: VLAN ID=10 - P7: VLAN ID=10, 1st redundant port - P8: VLAN ID=10, 2nd redundant port - Ring 1 is enabled. • TN router B: - P5: VLAN ID=10 - P7: VLAN ID=10, 1st redundant port - P8: VLAN ID=10, 2nd redundant port - Ring 1 is enabled. • PC-1: - IP: 10.10.10.19/24 • PC-2 : - IP: 10.10.10.127/24	

Network topology:



Scenario:
a) Router (A) and Router (B) both enable Moxa Turbo Ring v2 to provide redundancy for communication.
b) PC (1) and PC (2) can communicate with each other via Router (A) and Router (B).
c) 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
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	Firewall/ETBN Router 00000# show redundancy turbo-ring-v2 Turbo Ring V2 settings: Ring 1: Enabled Set as master: Disabled 1st port: 1/9 2nd port: 1/7 Ring 2: Disabled Set as master: Disabled 1st port: 1/5 2nd port: 1/6 Ring Coupling: Disabled Primary Port:1/3 Backup Port:1/4 Turbo Ring V2 status: Ring 1: Status:Break Master/Slave:Master 1st Ring Port Status:1/9 Link down 2nd Ring Port Status:1/7 Link down Ring 2: Status:--- Master/Slave:--- 1st Ring Port Status:--- 2nd Ring Port Status:--- Coupling: Mode:--- Coupling Port Status: --- Firewall/ETBN Router 00000# show redundancy turbo-ring-v2 Turbo Ring V2 settings: Ring 1: Enabled	

	Set as master: Disabled 1st port: 1/9 2nd port: 1/7 Ring 2: Disabled Set as master: Disabled 1st port: 1/5 2nd port: 1/6 Ring Coupling: Disabled Primary Port:1/3 Backup Port:1/4 Turbo Ring V2 status: Ring 1: Status:Break Master/Slave:Master 1st Ring Port Status:1/9 Link down 2nd Ring Port Status:1/7 Link down Ring 2: Status:--- Master/Slave:--- 1st Ring Port Status:--- 2nd Ring Port Status:--- Coupling: Mode:--- Coupling Port Status: ---
Error Messages	^Parse error
	^Incomplete command
Related Commands	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**

Option Description	**turbo-chain**	Turbo chain
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Firewall/VPN Router 00000# configure Firewall/VPN Router 00000(config)# redundancy mode turbo-chain	
Error messages	^Incomplete command	
	^Parse error	
Related Commands	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>**

Option Description	**role**	Role of this switch in Turbo Chain
	head	Turbo Chain head switch
	member	Turbo Chain member switch
	tail	Turbo Chain tail switch
	primary	Turbo Chain primary port
	secondary	Turbo Chain secondary port
	interface	Interface of Turbo Chain
	ethernet-port-id	Ethernet port ID. e.g. 1/1
Defaults	N/A	
Command Modes	Redundancy Configuration Sub-mode	
Usage Guidelines	• Chain ports cannot be the same port. • Trunk ports cannot be set as chain ports.	
Examples	`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`	
Error messages	% Interface <ethernet-port-id> not exist	
	% Identical Turbo Chain ports.	
Related Commands	show redundancy turbo-chain	

show redundancy turbo-chain

Show Turbo Chain configuration and status.

Synopsis

show redundancy turbo-chain

Option Description	**show**	Show system information
	redundancy	Display redundancy protocol status
	turbo-chain	Display turbo chain status
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	`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 ---`	
Error messages	N/A	
Related Commands	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.

High Availability

show ha

Use the **show ha** EXEC command to show High Availability status.

Synopsis

show ha

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	Use this command to view the current HA status summary.	
Examples	router# show ha High Availability Status Mode : Active-Passive --------------------------- Self Role : Primary Self State : Synchronization Self Serial Number : TAHCB1168803 Self HA Link I/F : HA Self HA Link Ethernet port: 1/8 --------------------------- Peer 1 Role : Backup Peer 1 State : Synchronization Peer 1 Serial Number : TBDEB1086502 Peer 1 HA Link I/F : HA Peer 1 HA Link Ethernet port: 1/8 Peer 1 Uptime Time : 2d12h35m7s Peer 1 Link Up Ethernet port: 1/2, 1/3, 1/5, 1/8, ---------------------------	
Error Messages	^Parse error ^Incomplete command	
Related Commands	show ha detail show ha peer system	
Command Modes	Privileged EXEC	

show ha detail

Use the **show ha detail** EXEC command to show detailed High Availability status.

Synopsis

show ha detail

Option Description	N/A — Display detailed HA Configuration.
Defaults	N/A
Command Modes	EXEC mode
Usage Guidelines	Use this command to view detailed HA configuration.
Examples	router# show ha detail High Availability Setting Operation : Enable Mode : Active-Passive Preferred Role : Primary Link type : Dedicated

	Link encrypted : Enable Link I/F : HA HA Link Ethernet port: 1/8 HA Link VID mode : Auto HA Link VID : 4089 Heartbeat Interval (ms) : 100 Heartbeat Lost Threshold : 3 Priority : 100 Auth mode : Password Auth Password : moxamoxa HA Event mode : Link Status HA Event port : 1/5,
Error Messages	^Parse error ^Incomplete command
Related Commands	show ha show ha peer system

show ha peer system

Use the **show ha peer system** EXEC command to show High Availability status from peer system.

Synopsis

show ha detail

Option Description	show	Show system information
	ha	Show High Availability Information
	peer system	Display HA information retrieved from peer system.
Defaults	N/A	
Command Modes	EXEC mode	
Usage Guidelines	Use this command to view system information of the HA peer device.	
Examples	router# show ha peer system !!! REMOTE CONFIG !!! System Information System Name : Firewall/VPN Router 86502 System Location : Device Location System Description : Maintainer Information : Host Name : Firewall-VPN-Router-86502 MAC Address : 00:90:E8:C7:22:FC Serial No. : TBDEB1086502 System Uptime : 2d12h42m45s CPU Frequency : 1600 MHz	
Error Messages	^Parse error ^Incomplete command	
Related Commands	show ha show ha detail	
Defaults	N/A	

ha enable

Use the **ha enable** global configuration command to disable High Availability.

Synopsis

(config)# **ha enable**

Option Description	ha	Configure High Availability
	enable	Enable High Availability
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to enable the HA function on the device.	
Examples	router(config)# ha enable	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha disable ha mode active-passive ha mode active-active-no-load-balancing	

ha disable

Use the **ha disable** global configuration command to disable High Availability.

Synopsis

(config)# **ha disable**

Option Description	ha	Configure High Availability
	disable	Disable High Availability
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to disable the HA function on the device.	
Examples	`router(config)# ha disable`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha enable ha mode active-passive ha mode active-active-no-load-balancing	

ha mode active-passive

Use the **ha mode active-passive** global configuration command to set High Availability to Active-Passive mode.

Synopsis

(config)# **ha mode active-passive**

Option Description	ha	Configure High Availability
	mode	Configure High Availability mode
	active-passive	Set High Availability to Active-Passive mode
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to set the HA operating mode to active-passive.	
Examples	`router(config)# ha mode active-passive`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha enable ha disable ha mode active-active-no-load-balancing	
Defaults	N/A	

ha mode active-active-no-load-balancing

Use the **ha mode active-active-no-load-balancing** global configuration command to set High Availability to active-active mode without load balancing.

Synopsis

(config)# **ha mode active-active-no-load-balancing**

Option Description	ha	Configure High Availability
	mode	Configure High Availability mode
	active-active-no-load-balancing	Set High Availability to active-active mode without load balancing.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to set the HA operating mode to active-active without load balancing.	
Examples	`router(config)# ha mode active-active-no-load-balancing`	

Error Messages	^Parse error ^Incomplete command
Related Commands	ha enable ha disable ha mode active-passive
Defaults	N/A

ha role primary

Use the **ha role primary** global configuration command to configure the device role as primary in the HA pair. To clear the configured primary HA role, use the **no** form of this command.

Synopsis

(config)# **ha role primary**

Option Description	ha	Configure High Availability
	role	Configure High Availability mode
	primary	Set High Availability to active-active mode without load balancing.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use the no form of this command to clear the configured primary HA role. Use the no form of this command to clear the configured primary HA role.	
Examples	`router(config)# ha role primary`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	no ha role primary ha enable	
Defaults	N/A	

ha hb-interval

Use the **ha hb-interval** global configuration command to specify the high availability heartbeat interval in milliseconds.

Synopsis

(config)# **ha hb-interval <UINT:interval_ms>**

Option Description	ha	Configure High Availability
	hb-interval	Configure heartbeat interval
	<UINT:interval_ms>	Specify the HA heartbeat interval in milliseconds.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to configure the interval between HA heartbeat messages.	
Examples	`router(config)# ha hb-interval 1000`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha hb-lost-threshold <UINT:lost_threshold> ha enable	

ha hb-lost-threshold

Use the **ha hb-lost-threshold** global configuration command to specify the number of missed heartbeats before the peer is considered lost

Synopsis

(config)# **ha hb-lost-threshold <UINT:lost_threshold>**

Option Description	ha	Configure High Availability
	hb-lost-threshold	Configure heartbeat threshold.
	<UINT:lost_threshold>	Specify the number of missed heartbeats before the peer is considered lost.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to configure the heartbeat loss threshold for HA failover detection.	
Examples	`router(config)# ha hb-lost-threshold 3`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha hb-interval <UINT:interval_ms> ha enable	

ha switchmode failover

Use the **ha switchmode failover** global configuration command to configure High Availability to operate in failover switching mode.

Synopsis

(config)# **ha switchmode failover**

Option Description	ha	Configure High Availability
	switchmode	Configure switching mode.
	failover	Configure HA to operate in failover switching mode.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to configure the HA switching behavior as failover mode.	
Examples	`router(config)# ha switchmode failover`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha switchmode failback ha enable	

ha switchmode failback

Use the **ha switchmode failback** global configuration command to configure High Availability to operate in failback switching mode.

Synopsis

(config)# **ha switchmode failback**

Option Description	ha	Configure High Availability
	switchmode	Configure switching mode.
	failback	Configure HA to operate in failover switching mode.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to configure the HA switching behavior as failback mode.	
Examples	`router(config)# ha switchmode failback`	
Error Messages	^Parse error ^Incomplete command	

Related Commands	ha switchmode failover ha enable

ha interface type dedicated

Use the **ha interface type dedicated** global configuration command to configure the High Availability interface type as a dedicated interface.

Synopsis

(config)# **ha interface type dedicated**

Option Description	ha	Configure High Availability
	interface type	Configure High Availability interface.
	dedicated	Configure High Availability interface type as a dedicated interface.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to specify that HA communication uses a dedicated interface.	
Examples	`router(config)# ha interface type dedicated`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha interface alias <STRING:alias> ha enable	

ha interface alias

Use the **ha interface alias** global configuration command to configure the High Availability interface alias.

Synopsis

(config)# **ha interface alias <STRING:alias>**

Option Description	ha	Configure High Availability
	interface-alias	Configure High Availability interface alias.
	<STRING:alias>	Specify the interface alias used for HA communication.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to assign the interface alias for the HA interface.	
Examples	`router(config)# ha interface alias wan1`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha interface type dedicated ha enable	

ha interface HA vid auto ethernet

Use the **ha interface HA vid auto ethernet** global configuration command to configure High Availability to automatically assign the VLAN ID for the HA interface, while also specifing the Ethernet port used for the HA interface.

Synopsis

(config)# **ha interface HA vid auto ethernet <STRING:mod_port>**

Option Description	ha	Configure High Availability
	interface	Configure High Availability interface.
	HA vid auto	Automatically assign the VLAN ID for the HA interface.

	ethernet <STRING:mod_port>	Specify the Ethernet port used for the HA interface.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to configure the HA interface with an automatically assigned VLAN ID on the specified Ethernet port.	
Examples	`router(config)# ha interface HA vid auto ethernet 1/1`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha interface HA vid manual <UINT:vid> ethernet <STRING:mod_port> ha interface type dedicated	

ha interface HA vid manual ethernet

Use the **ha interface HA vid manual ethernet** global configuration command to configure High Availability to manually assign the VLAN ID for the HA interface, while also specifying the Ethernet port used for the HA interface.

Synopsis

(config)# **ha interface HA vid manual <UINT:vid> ethernet <STRING:mod_port>**

Option Description	ha	Configure High Availability
	interface	Configure High Availability interface.
	HA vid manual <UINT:vid>	Manually specify the VLAN ID for the HA interface.
	ethernet <STRING:mod_port>	Specify the Ethernet port used for the HA interface.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to configure the HA interface with a manually assigned VLAN ID on the specified Ethernet port.	
Examples	`router(config)# ha interface HA vid manual 100 ethernet 1/1`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha interface HA vid auto ethernet <STRING:mod_port> ha interface type dedicated	

ha event link ethernet

Use the **ha event link ethernet** global configuration command to configure monitoring of the specified Ethernet port link for High Availability events. To remove the event monitoring, use the **no** form of this command.

Synopsis

(config)# **ha event link ethernet <STRING:mod_port>**

(config)# **no ha event**

Option Description	ha	Configure High Availability
	event	Configure High Availability events.
	link ethernet <STRING:mod_port>	Monitor the specified Ethernet port link event for HA.
Defaults	N/A	
Command Modes	Global configuration mode	

Usage Guidelines	Use this command to configure an HA event trigger based on the link status of the specified Ethernet port.
Examples	`router(config)# ha event link ethernet 1/2`
Error Messages	^Parse error ^Incomplete command
Related Commands	no ha event ha enable

ha auth password

Use the **ha auth password** global configuration command to configure password authentication for High Availability. To remove the password, use the **no** form of this command.

Synopsis

(config)# **ha auth password <STRING:password>**

(config)# no **ha auth password**

Option Description	ha	Configure High Availability
	auth	Configure High Availability interface authentication.
	password <STRING:password>	Configure the password used for HA authentication.
Defaults	N/A	
Command Modes	Global configuration mode	
Usage Guidelines	Use this command to configure the authentication password for HA peer communication.	
Examples	`router(config)# ha auth password mypassword` `router(config)# no ha auth`	
Error Messages	^Parse error ^Incomplete command	
Related Commands	ha enable show ha detail	

Warning Notification command

Use the **ha auth password** global configuration command to configure password authentication for High Availability. To remove the password, use the **no** form of this command.

Synopsis

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

(config)# **no warning-notification system-event ha-role-changed active**

Option Description	warning-notification	Warning notification
	system-event	System event setting
	ha-role-changed	HA Role changed setting
	action	Enable Action setting
	combination	SNMP Trap Server only(1) Email only(2) SNMP Trap Server+Email(3) Syslog only(4) SNMP Trap Server+Syslog Server(5) Email+Syslog Server(6) SNMP Trap Server+Email+Syslog Server(7) Relay1 only(8) SNMP Trap Server+Relay1(9) Email+Relay1(10)

		SNMP Trap Server+Email+Relay1(11) Syslog+Relay1(12) SNMP Trap Server+Syslog Server+Relay1(13) Email+Syslog Server+Relay1(14) SNMP Trap Server+Email+Syslog Server+Relay1(15) SMS(32) SNMP Trap Server+SMS(33) Email+SMS(34) SNMP Trap Server+Email+SMS(35) Syslog Server+SMS(36) SNMP Trap Server+Syslog Server+SMS(37) Email+Syslog Server+SMS(38) SNMP Trap Server+Email+Syslog Server+SMS(39) Relay1+SMS(40) SNMP Trap Server+Relay1+SMS(41) Email+Relay1+SMS(42) SNMP Trap Server+Email+Relay1+SMS(43) Syslog Server+Relay1+SMS(44) SNMP Trap Server+Syslog Server+Relay1+SMS(45) Email+Syslog Server+Relay1+SMS(46) SNMP Trap Server+Email+Syslog Server+Relay1+SMS(47) None(0)
	severity	Severity setting
	type	Emergency(0) Alert(1) Critical(2) Error(3) Warning(4) Notice(5) Information(6) Debug(7)
	active	Activate
	no	Negate Command or Set to Default
Defaults	N/A	
Command Modes	Configuration mode	
Usage Guidelines	N/A	
Examples	Firewall/VPN Router 00000 `# configure` Firewall/VPN Router 00000 `(config)# warning-notification system-event ha-role-changed action 0` Firewall/VPN Router 00000 `(config)# warning-notification system-event ha-role-changed severity 4` Firewall/VPN Router 00000 `(config)# warning-notification system-event ha-role-changed active` Firewall/VPN Router 00000 `(config)# no warning-notification system-event ha-role-changed active`	
Error Messages	% Invalid action value or non-support this combination action % Invalid severity type	
Related Commands	N/A	

warning-notification system-event duplicate-ip-detection

To enable or disable duplicate IP detection, use these the **warning-notification system-event duplicate-ip-detection** configuration mode command. To disable notifications, use the **no** form of this command.

Synopsis

(config-if) **warning-notification system-event duplicate-ip-detection active**

(config-if) **no warning-notification system-event duplicate-ip-detection active**

Option Description	active	Enable the warning notification for system event duplicate ip detection function
Defaults	Disabled	
Command Modes	Configuration mode	
Usage Guidelines	Use this command to configure the authentication password for HA peer communication.	
Examples	Enable `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config-if)# warning-notification system-event duplicate-ip-detection active` Disable `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config-if)# no warning-notification system-event duplicate-ip-detection active`	
Error Messages	N/A	
Related Commands	N/A	

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>

Option Description	string-vlan-ids	A VLAN ID or a list of VLAN IDs separated by comma.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• VLAN ID ranges from 1 to 4094. • 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. • The removal command won't take effect if you attempt to remove a managed VLAN ID. • 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.	
Examples	• Specify VLAN ID 55: `router# configure` `router(config)# vlan create 55` `router(config)# exit` • Remove VLAN ID 55 (and associated LAN interface if any): `router# configure` `router(config)# no vlan create 55` `router(config)# exit`	
Error Messages	% vlan is invalid!! Should be range from 1 to 4094	
	^Parse error	
	^Incomplete command	
Related Commands	show vlan interface vlan	

show vlan

Use the **show vlan** user EXEC command to display VLAN status information.

Synopsis

show vlan

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`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:`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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,	
Error Messages	^Parse error ^Incomplete command	
Related Commands	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>}]

Option Description	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
Defaults	IGMP snooping is globally disabled.	
Command Modes	Global configuration	
Usage Guidelines	• IGMP snooping function will be enabled automatically as soon as the first VLAN is configured. • Use **ip igmp-snooping querier vlan** <vlan-id> **v3** can make the switch to send IGMP V3 query, otherwise the default is V2 query. • Make sure the VLAN ID is created in advance before using it.	
Examples	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`	
Error Messages	% Please check the multicast mac address's type !!!	
	% Vlan IGMP Function is Disabled !!!	
	% Vlan entry not found!!!	
	^Parse error	
	^Incomplete command	
Related Commands	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}]

Option Description	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
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	Firewall/ETBN Router 00000# show ip igmp VID | Group | Port | Version |Filter Mode |Source --- 1 224. 0. 0.251 1/1 V2 224. 0. 0.252 1/1 V2 239.194. 0. 0 1/1 V2 2 4040 VID | Stream Group | Stream Source | Port | Member Ports --- 1 239.194. 0. 0 10. 1. 63.254 1/1 1/1 2 4040	
Examples	N/A	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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> **vlan** <vlanid>

(config)# **no ip igmp static-group** {mac-address {**interface** <module-port>{**vlan** <vlanid>}}}

Option Description	mac-address	MAC address XX:XX:XX:XX:XX:XX
	interface	Specifies binding ports
	module-port	Port (Trunk) ID or list. Ex. 1/1,2,4-5,2/1,Trk1,Trk2-Trk
	vlan	Specifies VLAN
	vlanid	VLAN ID as a number
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Adding a Rule: 1. When adding a rule, users must input three parameters: static-group address, interface port, and VLAN ID. 2. If an existing rule has the same address and VLAN ID, the port will be added to the original rule in an OR fashion. Deleting a Rule: 3. When deleting a rule, users can choose to input the following three parameters based on their needs: static-group address, interface port, and VLAN ID (see the example below). The scope of deletion will narrow as more parameters are provided. 4. If no parameters are provided, the entire table will be deleted. 5. If only the static-group address is provided, the rule mapped to this address will be deleted. 6. If both the static-group address and interface port are provided, the rule mapped to the specified address will have the specified port deleted. If no ports remain after deletion, the rule will be removed. 7. If the static-group address, interface port, and VLAN ID are all provided, the rule mapped to the specified address and VLAN ID will have the specified port deleted. If no ports remain after deletion, the rule will be removed. Modifying a Rule: 8. If user wishes to modify the rule, they need to delete the rule and add it again.	
Examples	`router(config)# ip igmp static-group 01:00:5E:01:01:08 interface 1/8` `router(config)# no ip igmp static-group` `router(config)# no ip igmp static-group 01:00:5E:01:01:08`	
Error Messages	%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!!!	
	% Please select a VLAN ID!	
	% Static multicast MAC address NOT found !!!	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	weighted-fair	Weighted fair queuing
	strict	Strict queuing
Defaults	Default QoS strategy is Weighted-fair queuing.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Specify QoS mode to "strict" : `router# configure` `router(config)# qos mode strict` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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}

Option Description	cos-to-queue	CoS to traffic queue
	cos-value	CoS value (0~7)
	queue	Traffic queue (port priority). Ranges from 0(Low) to 7(High)
	dscp-to-queue	DSCP to traffic queue
	dscp-value	DSCP value (0~63)
Defaults	Cos (queue) : 0 (0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7) DSCP(Cos) : 0-15(0), 16-31(1), 32-47(2), 48-63(3)	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Specify CoS (1) to queue Normal (1): `router# configure` `router(config)# qos mapping cos-to-queue 1 1` `router(config)# exit`	
Error Messages	% Invalid parameter. CoS value must be 0~7 and queue number must be 0~7	
	% Invalid parameter. DSCP value must be 0~63 and queue value must be 0~3	
	^Parse error	
	^Incomplete command	
Related Commands	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}

Option Description	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
Defaults	CoS is enabled; DSCP is enabled.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Member ports existing in the specified trunked port is required before entering sub-level configuration mode of this command • The priority of an ingress frame is determined in the following order: 1. CoS 2. DSCP 3. Port priority	
Examples	Disable CoS on trk1 and change port priority to 7(High): `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`	
Error Messages	% CoS value is out of range! The allowed value range is 0 to 7	
	^Parse error	
	^Incomplete command	
Related Commands	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}

Option Description	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
Defaults	CoS is enabled; DSCP is enabled.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	The priority of an ingress frame is determined in the following order: 1. CoS 2. DSCP 3. Port priority	
Examples	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`	
Error Messages	% CoS value is out of range! The allowed value range is 0 to 7	
	^Parse error	
	^Incomplete command	
Related Commands	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**}]

Option Description	qos	Display QoS configuration
	cos-to-queue	CoS to traffic queue mappings
	dscp-to-queue	DSCP to traffic queue mappings
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	qos mode qos mapping interface trunk qos interface ethernet qos	

show qos dscp-remark

To show DSCP remark configuration, use the **showqos dscp-remark** command.

Synopsis

show qos dscp-remark

Option Description	N/A	N/A
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	Firewall/ETBN Router 00000# show qos dscp-remark Port-based Configuration Port Status DSCP --- 1/1 Disabled 0 1/2 Disabled 0 1/3 Disabled 0 1/4 Disabled 0 1/5 Disabled 0 1/6 Disabled 0 1/7 Disabled 0 1/8 Disabled 0 1/9 Disabled 0 1/10 Disabled 0 1/11 Disabled 0 1/12 Disabled 0 1/13 Disabled 0 1/14 Disabled 0 1/15 Disabled 0 1/16 Disabled 0	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	qos dscp-remark-subnet qos dscp-remark-port	

interface ethernet

To configure the DSCP remarking port-based settings by applying settings to individual Ethernet interfaces, use the **interface ethernet** command to enter interface configuration mode.

Synopsis

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

qos

To enabled or disabled DSCP remark-port based feature, use the **qos** or **no qos dscp-remark-port** command.

(config-if)# **qos** {dscp-remark-port <dscp-value>}

(config-if)# **no qos dscp-remark-port**

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5
	DSCP-remark-port	Specifies DSCP-remark port-based function
	dscp-value	Integer for DSCP value.
Defaults	1. Default function is disabled. 2. DSCP value is 0.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	1.<dscp-value> allow 0,8,16,24,32,40,48,56 means CS0,CS1,CS2,CS3,CS4,CS5,CS6,CS7 2."no qos DSCP-remark-port" will set function disabled and DSCP value as 0.	
Examples	Enable the Ethernet PORT1 and assign the DSCP value as CS7: `router# configure` `router(config)# interface ethernet 1/1` `router(config-if)# qos dscp-remark-port 56` `router(config-if)# exit`	
Error Messages	% The allowed DSCP values are 0,8,16,24,32,40,48,56 (CS0,CS1,CS2,CS3,CS4,CS5,CS6,CS7)	
	^Parse error	
	^Incomplete command	
Related Commands	qos dscp-remark-subnet	

qos

To configure or delete a DSCP remark subnet-based rule, use **qos** or **no qos dscp-remark-subnet** command.

Synopsis

(config)# **qos** {dscp-remark-subnet <rule-index> <ip-addr> <netmask> <dscp-value>}

(config)# **no qos dscp-remark-subnet** <rule-index>

Option Description	DSCP-remark-subnet	Specify DSCP-remark subnet-based function
	rule-index	Specify rule index from 1 to 12.
	ip-addr	The Source IP address to be assigned to this rule.
	netmask	Netmask.
	dscp-value	Integer for DSCP value.
Defaults	1. Default function is disabled. 2. subnet information is empty. 3. DSCP value is 0.	
Command Modes	Global configuration	
Usage Guidelines	1.<rule-index> is range from 1 to 12. 2.<dscp-value> allow 0,8,16,24,32,40,48,56 means CS0,CS1,CS2,CS3,CS4,CS5,CS6,CS7 3."no qos DSCP-remark-subnet <rule-index>" will delete rule.	
Examples	Create and enable two subnet rules and assign DSCP value CS6: `router# configure` `router(config)# qos dscp-remark-subnet 1 192.168.127.220 255.255.255.0 48` `router(config)# qos dscp-remark-subnet 2 10.0.1.1 255.255.255.0 48`	
Error Messages	% Invalid parameeter	
	% The allowed DSCP values are 0,8,16,24,32,40,48,56 (CS0,CS1,CS2,CS3,CS4,CS5,CS6,CS7)	
	^Parse error	
	^Incomplete command	
Related Commands	qos dscp-remark-report	

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}

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,.
	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)}
Defaults	Not limited	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A.	
Examples	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`	
Error Messages	% Illegal parameter	
	^Parse error	
	^Incomplete command	
Related Commands	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>

Option Description	mode	Specifies the mode
	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.
Defaults	Limit broadcast frames/Drop Packeet	
Command Modes	Global configuration	
Usage Guidelines	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.	
Examples	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`	
Error Messages	% Invalid Period Value. It must be 0 - 65535.	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	second	Ranges from 5 to 300 seconds.
Defaults	300	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Specify the aging-time to 200 seconds: `router# configure` `router(config)# mac-address-table aging-time 200` `router(config)# exit`	
Error Messages	% Age time should between 5~300s!	
	^Parse error	
	^Incomplete command	
Related Commands	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>}

Option Description	static	Retrieve static MAC addresses
	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.
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	router# show mac-address-table Idx MAC Type VLAN Port ----- ------------------ ---------- ------ ---------- 1 01-00-5E-7F-FF-FA mcast(s) 1 1/1,1/2, 2 50-7B-9D-E1-82-5A ucast(l) 1 1/2, router# show mac-address-table aging-time MAC address aging time: 300 sec	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	mac-address-table aging-time	

3. Interfaces and Routing Functions

This chapter describes the interface and routing functions.

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 **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information. • Enter configuration mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	(config)#	To exit to privileged EXEC mode, enter **exit**.	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example **interface lan** command and press enter	(config-if)#	To exit to global configuration mode, enter **exit**.	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 **Error! Bookmark not defined.**.

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}

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	This command only applies to LAN interface using the management VLAN.	
Examples	Change interface name to LAN-M. `router# configure` `router(config)# interface lan` `router(config-if)# name LAN-M` `router(config-if)# exit`	
Error Messages	% is over length. It must be 1 - 12.	
	^Parse error	
	^Incomplete command	
Related Commands	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**]

Option Description	no	Disable
	static	Specifies static IP address
	lan-ip	IP address
	netmask	Netmask of the static IP address
	secondary	Specifies a secondary IP address
Defaults	IP address of default LAN is 192.168.127.254	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the management VLAN.. • DHCP option is not applicable to this entry LAN interface.	
Examples	• 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` • `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` • `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`	
Error Messages	% No match entry for Secondary IP, mask for LAN	
Related Commands	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}]

Option Description	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
Defaults	• metric : 1 • h-interval : 10 • d-interval : 40 • pri-number : 1	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	This command only applies to LAN interface using the management VLAN.	
Examples	• Specify Auth type to "none". `router# configure` `router(config)# interface lan` `router(config-if)# no ip ospf auth` `router(config-if)# exit` `router(config)# exit` • Delete OSPF LAN interface. `router# configure` `router(config)# interface lan` `router(config-if)# no ip ospf` `router(config-if)# exit` `router(config)# exit`	

	• Return hello interval to default. `router# configure` `router(config)# interface lan` `router(config-if)# no ip ospf hello-interval` `router(config-if)# exit` `router(config)# exit` • * An illustrative example can be found in the chapter "Unicast Route".
Error Messages	% 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
Related Commands	route ospf show interfaces lan

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**

Option Description	source-ip	Specifies to overwrite source IP
Defaults	Directed broadcast is disabled by default.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the management VLAN. • This feature supports directed broadcast for UDP packets only; ICMP is not included.	
Examples	Enable directed broadcast. `router# configure` `router(config)# interface lan` `router(config-if)# ip directed-broadcast` `router(config-if)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show ip directed-broadcast	

interface lan ip ospf passive-interface

To enable passive interface, use **interface lan ip ospf passive-interface** 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>} **passive-interface** <STRING:name>|

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

Option Description	passive-interface	Enable passive-interface
Defaults	Directed broadcast is disabled by default.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the management VLAN. • This feature supports directed broadcast for UDP packets only; ICMP is not included.	
Examples	Enable directed broadcast. `router# configure` `router(config)# interface lan` `router(config-if)# ip ospf passive-interface` `router(config-if)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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**

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

Option Description	vlan-id	Ranges from 1 to 4094.
Defaults	Default management VLAN ID is 1.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• ▪ This command only applies to LAN interface using the management VLAN. • ▪ Make sure the VLAN ID is created in advance before using it.	
Examples	Specify management VLAN ID (2). `router# configure` `router(config)# interface lan` `router(config-if)# bind vlan 2` `router(config-if)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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}

Option Description	mac-addr	The virtual MAC address.
	default	Return to default value 00:00:00:00:00:00
Defaults	00:00:00:00:00:00	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	This command only applies to LAN interface using the management VLAN.	
Examples	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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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

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

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

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

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

Option Description	vlan-id	Ranges from 1 to 4094.
	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the non-management VLAN. • The IP address of the LAN interface should be configured before using this command. • Make sure the VLAN ID is created in advance before using it.	
Examples	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`	
Error Messages	% 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	
Related Commands	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>

Option Description	vlan-id	VLAN ID to be removed.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• Range of VLAN ID is 1 to 4094. • 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.	
Examples	Remove the interface which binds VLAN ID (5) from the router. `router# configure` `router(config)# no interface vlan 5` `router(config)# exit`	
Error Messages	% interface vlan is not exist	
	^Parse error	
	^Incomplete command	
Related Commands	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}

Option Description	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
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the non-management VLAN. • Make sure the LAN interface is created in advance before using it. • The maximum number of secondary IPs allowed is 640. • When deleting the non-management VLAN directly, any associated secondary IP addresses will be automatically removed.	
Examples	• Create LAN3's interface IP 30.0.0.1 and secondary IP addresses 30.0.0.2 and 20.0.0.2. `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` • Remove secondary IP 30.0.0.2 of LAN3. `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)#` • Remove the static IP address as well as all the secondary IP addresses of LAN3. `router# configure` `router(config)# no interface vlan 3` `router(config)# exit`	
Error Messages	% 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	
	^Incomplete command	
Related Commands	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}]

Option Description	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
Defaults	• metric : 1 • h-interval : 10 • d-interval : 40 • pri-number : 1	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the non-management VLAN. • Make sure the VLAN ID is created in advance before using it.	
Examples	• Specify Auth type to "none" with LAN interface (VLAN ID=3). `router# configure` `router(config)# interface vlan 3` `router(config-vif)# no ip ospf auth` `router(config-vif)# exit` `router(config)# exit` • Delete OSPF WAN interface. `router# configure` `router(config)# interface vlan 3` `router(config-vif)# no ip ospf`	

	router(config-vif)# exit router(config)# exit • Return hello interval to default. router# configure router(config)# interface vlan 3 router(config-vif)# no ip ospf hello-interval router(config-vif)# exit router(config)# exit * An illustrative example can be found in the chapter "Unicast Route".
Error Messages	% 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
	vlan id does not exist!!
	^Parse error
	^Incomplete command
Related Commands	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**

Option Description	vlan-id	Ranges from 1 to 4094.
	directed-broadcast	Enables directed broadcast feature.
	source-ip	Specifies to overwrite source IP
Defaults	Directed broadcast is disabled by default.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the non-management VLAN. • Make sure the VLAN ID is created in advance before using it. • This feature supports directed broadcast for UDP packets only; ICMP is not included.	
Examples	Enable directed broadcast. router# configure router(config)# interface vlan 10 router(config-vif)# ip directed-broadcast router(config-vif)# exit	
Error Messages	^Parse error	
	vlan id does not exist!!	
	^Incomplete command	
Related Commands	show ip directed-broadcast	

interface vlan ip ospf passive-interface

To enable passive interface, use **interface vlan ip ospf passive-interface** command.

Synopsis

(config)# **interface vlan**

(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>} **passive-interface** <STRING:name>|

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

Option Description	passive-interface	Enable passive-interface
Defaults	Directed broadcast is disabled by default.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the management VLAN. • This feature supports directed broadcast for UDP packets only; ICMP is not included.	
Examples	Enable directed broadcast. `router# configure` `router(config)# interface vlan` `router(config-vif)# ip ospf passive-interface` `router(config-if)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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 proy-arp** <vlan-id>

Option Description	vlan-id	Ranges from 1 to 4094.
Defaults	Proxy ARP is disabled by default.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the non-management VLAN. • Make sure the VLAN ID is created in advance before using it.	
Examples	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`	
Error Messages	^Parse error	
	vlan id does not exist!!	
	^Incomplete command	
Related Commands	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}

Option Description	vlan-id	Ranges from 1 to 4094.
	mac-addr	The virtual MAC address.
	default	Return to default value 00:00:00:00:00:00
Defaults	00:00:00:00:00:00	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the non-management VLAN. • Make sure the VLAN ID is created in advance before using it.	
Examples	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`	
Error Messages	vlan id does not exist!!	
	^Parse error	
	^Incomplete command	
Related Commands	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>]

Option Description	vlan-id	Specifies a specific VLAN ID
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	Make sure the VLAN ID is created in advance before using it.	
Examples	`router# show interfaces vlan 2` `Interface Name : LAN2` `State : Enable` `IPv4 Connection Type : Static IP` `IPv4 Address : 192.168.2.254` `Subnet Mask : 255.255.255.0` `VLAN ID : 2`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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>**

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

Option Description	interface	Interface setting
	lan	LAN setting
	ip address static	Settings for IP address, mask and gateway
Defaults	IP: 192.168.127.254 Mask: 255.255.255.0 Gateway: 0.0.0.0	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	`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)`	

	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
Error Messages	% Configured IP Address is in the subnet of interface MGMT
	% Invalid parameter!
	^Incomplete command
	^Parse error
Related Commands	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>]]**

Option Description	ipaddr1	IP address
	ipaddr2	IP address
	ipaddr3	IP address
Defaults	0.0.0.0	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	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	
Error Messages	% Invalid parameters!	
	^Parse error	
	% Incomplete command	
Related Commands	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**

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

Usage Guidelines	N/A
Examples	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
Error Messages	N/A
Related Commands	show interface lan

show interface lan

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

Synopsis

show interface lan

Option Description	N/A
Defaults	N/A
Command Modes	Global configuration, sub-level configuration
Usage Guidelines	N/A
Examples	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
Error Messages	^Incomplete command
	^Parse error
Related Commands	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**

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

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

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	% 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	
Related Commands	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**]

Option Description	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
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	% is over length. It must be 1 - 30.	
	^Parse error	
	^Incomplete command	
Related Commands	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>]]

Option Description	dns1	1st The DNS IP address
	dns2	2nd The DNS IP address
	dns3	3rd The DNS IP address
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	The priority of a manually configured DNS will be higher than the DNS from the PPPoE or DHCP server. Note: Duplicate DNS entries are blocked on TN-4900 series products. While other models will show a warning suggesting the use of distinct IP addresses.	
Examples	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`	
Error Messages	^Parse error	
	^Incomplete command	
	Invalid DNS Configuration. Primary, secondary and tertiary DNS server IP addresses must be unique.	
	Use distinct IP addresses for primary, secondary, and tertiary DNS servers to ensure network stability.	
Related Commands	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}]

Option Description	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
Defaults	• metric : 1 • h-interval : 10 • d-interval : 40 • pri-number : 1	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	• Specify Auth type to "none". `router# configure` `router(config)# interface wan` `router(config-if)# no ip ospf auth` `router(config-if)# exit` `router(config)# exit` • Delete OSPF WAN interface. `router# configure` `router(config)# interface wan` `router(config-if)# no ip ospf` `router(config-if)# exit` `router(config)# exit` • Return hello interval to default. `router# configure` `router(config)# interface wan` `router(config-if)# no ip ospf hello-interval` `router(config-if)# exit` `router(config)# exit` * An illustrative example can be found in the chapter "Unicast Route".	
Error Messages	% 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	
Related Commands	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**

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

interface wan ip ospf passive-interface

To enable passive interface, use **interface wan ip ospf passive-interface** 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>} **passive-interface** <STRING:name>|

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

Option Description	passive-interface	Enable passive-interface
Defaults	Directed broadcast is disabled by default.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• This command only applies to LAN interface using the management VLAN. • This feature supports directed broadcast for UDP packets only; ICMP is not included.	
Examples	Enable directed broadcast. `router# configure` `router(config)# interface wan` `router(config-if)# ip ospf passive-interface` `router(config-if)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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**

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

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

Option Description	mac-addr	The virtual MAC address.
	default	Return to default value 00:00:00:00:00:00
Defaults	00:00:00:00:00:00	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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>]

Option Description	status	Specifies to display WAN interface information
	wan-id	Integer value starting from 1. This option is only valid for the product which supports multi-WAN interfaces.
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	• If the connection type is "Static IP", suggest use #show interfaces wan to display the settings. • If the connection type is "Dynamic IP" or "PPPoE", suggest use #show interfaces wan status to display the status.	
Examples	• When the connection type is Static IP, display current settings. router# show interfaces wan WAN Alias : Vlan ID : 200 Connect Mode : Enable IPv4 Connection Type : Static IPv4 Address : 10.0.0.1 Netmask : 255.255.255.0 IPv4 Gateway : 0.0.0.0 PPTP Connection : Disable PPTP IPv4 Address : 0.0.0.0 PPTP User Name : PPTP Password : ******** PPTP MPPE Encryption : Disable IPv4 DNS Server : 0.0.0.0 0.0.0.0 0.0.0.0 • When the connection type is Dynamic IP, display current status. router# show interfaces wan status WAN IPv4 Connection Type : DHCP IPv4 Address : 10.123.24.12 Netmask : 255.255.252.0 IPv4 Gateway : 10.123.24.1 DNS Server : 10.123.200.11 10.123.200.12 0.0.0.0	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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**

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

DNS Forwarding (TN-4900 Models only)

show ip dns-server dns-forwarding

To show DNS forwarding information use, use the **show ip dns-server dns-forwarding** global configuration command.

Synopsis

(config)# **show ip dns-server dns-forwarding**

Option Description	**show**	Display configuration/status information
	ip	Display IP information
	dns-server	DNS server configuration
	dns-forwarding	DNS forwarding configuration
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000# show ip dns-server dns-forwarding` `DNS Forwarding: Disable` `DNS Forwarding: Enable` `Forwarders Table:` `----------` `Index  Zone  Forwarder IP Address`	

	1 a 10.0.2.3 2 b 192.168.127.16 3 k 20.23.20.12 ----------
Error Messages	N/A
Related Commands	N/A

ip dns-server dns-forwarding

To enable DNS forwarding, use the **ip dns-server dns-forwarding** global configuration command. To disable DNS forwarding, use the **no** form of the command.

Synopsis

(config)# **ip dns-server dns-forwarding**

(config)# **no ip dns-server dns-forwarding**

Option Description	**ip**	Display IP information
	dns-server	DNS server configuration
	dns-forwarding	Enable DNS Forwarding
Defaults	Disabled	
Command Modes	configuration mode	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000(config)# ip dns-server dns-forwarding`	
Error Messages	N/A	
Related Commands	no ip dns-server dns-forwarding	

ip dns-server dns-forwarding zone / ip

To configure DNS forwarding, use the **ip dns-server dns-forwarding** global configuration command. To disable DNS forwarding zones or forwarders, use the relavent **no** form of the command.

Synopsis

(config)# **ip dns-server dns-forwarding** {zone <forward_zone(63)> forwarder-ip <ip-address>}

(config)# **no ip dns-server dns-forwarding forwarder-ip <ip-address>**

(config)# **no ip dns-server dns-forwarding zone <forward_zone(63)>**

(config)# **no ip dns-server dns-forwarding zone all**

Option Description	**Ip**	Configure IP parameters
	dns-server	DNS server configuration
	dns-forwarding	DNS Forwarding configuration
	zone	Zone for DNS Forwarding entry
	<forward_zone(63)>	Specify forwarder zone. Allowed characters: • a to z • A to Z • 0 to 9 • . • - Maximum 63 characters. Cannot begin or end with '.' or '-'.
	forwarder-ip	IP address for DNS Forwarding entry
	<ip-address>	Unicast IP address
Defaults	N/A	
Command Modes	configuration mode	
Usage Guidelines	This command serves two functions. It can both create a new forwarder info or edit an existing zone's information.	

Examples	`Firewall/VPN Router 00000(config)# ip dns-server dns-forwarding zone local forwarder-ip 10.0.2.3` `Firewall/VPN Router 00000(config)# no ip dns-server dns-forwarding zone local` `Firewall/VPN Router 00000(config)# no ip dns-server dns-forwarding forwarder-ip 10.0.2.3`
Error Messages	% Invalid: The given Domain Name does not represent a valid Domain Name.
	% Invalid Unicast IP
	% Invalid: This domain is already used by a DNS local zone. Use a different domain, or a more specific sub-domain.
	% Invalid: <FQDN> is also used by a DNS local zone host record.
Related Commands	no ip dns-server dns-forwarding zone <forward_zone(63)> no ip dns-server dns-forwarding forwarder-ip <ip-address> no ip dns-server dns-forwarding zone all

Application Layer Gateway (ALG) for SIP (TN-4900 Models only)

ip nat alg

To enable ALG SIP configuration, use the **ip nat alg sip** global configuration command. To return to default settings, use the **no** form of this command.

Synopsis

(config)# **ip nat alg sip**

(config)# **no ip nat alg sip**

Option Description	**ip nat alg sip**	Enables ALG SIP
Defaults	Disabled.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000r# configure` `Firewall/VPN Router 00000(config)# ip nat alg sip`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	no ip nat alg sip	

show ip nat alg

To show information about ALG SIP configuration, use the **show ip nat alg** command.

Synopsis

(config)# **show ip nat alg**

Option Description	N/A
Defaults	N/A
Command Modes	Privileged EXEC / User EXEC
Usage Guidelines	N/A
Examples	`Firewall/VPN Router 00000r# show ip nat alg` `SIP ALG : Enable` `SIP ALG : Disable`
Error Messages	^Parse error
	^Incomplete command
Related Commands	ip nat alg sip no ip nat alg sip

Application Layer Gateway (ALG) for SIP (TN-4900 Models only)

ip nat alg

To enable ALG SIP configuration, use the **ip nat alg sip** global configuration command. To return to default settings, use the **no** form of this command.

Synopsis

(config)# **ip nat alg sip**

(config)# **no ip nat alg sip**

Option Description	**ip nat alg sip**	Enables ALG SIP
Defaults	Disabled.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000r# configure` `Firewall/VPN Router 00000(config)# ip nat alg sip`	

Error Messages	^Parse error
	^Incomplete command
Related Commands	no ip nat alg sip

show ip nat alg

To show information about ALG SIP configuration, use the **show ip nat alg** command.

Synopsis

(config)# **show ip nat alg**

Option Description	N/A
Defaults	N/A
Command Modes	Privileged EXEC / User EXEC
Usage Guidelines	N/A
Examples	`Firewall/VPN Router 00000r# show ip nat alg` `SIP ALG : Enable` `SIP ALG : Disable`
Error Messages	^Parse error
	^Incomplete command
Related Commands	ip nat alg sip no ip nat alg sip

Profinet DCP forward (NAT-102/NAT-108 Models only)

pn-forward

To enable Profinet DCP forwarding, use the **pn-forward** global configuration command. To return to default settings, use the **no** form of this command.

Synopsis

(config)# **pn-forward**

(config)# **no pn-forward**

Option Description	**pn-forward**	Enable Profinet DCP forwarding.
Defaults	Default Profinet forward is disabled.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000r# configure` `Firewall/VPN Router 00000(config)# pn-forward`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	no pn-forward	

show pn-forward

To show Profinet DCP forwarding configuration, use the **show pn-forward** command.

Synopsis

(config)# **show pn-forward**

Option Description	**show pn-forward**	Shows Profinet DCP forwarding configuration.
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000r# show pn-forward` `Status:                    : Enable` `Forward interface list:` `Index Incoming Interface Outgoing Interface2` `----- ------------------ -------------------` `  1           LAN1                LAN2` `Translated IP list:` `Index Original IP Translated IP` `----- ----------- -------------` `  1    10.0.0.1   192.168.127.1` `  2    10.0.2.3   192.168.126.3`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands		

WAN2/DMZ

interface wan dmz

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

Synopsis

(config-if)# **dmz**

Option Description	N/A	
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	• There is only one WAN interface supporting DMZ: the WAN2 on the EDR-G9004 models.	
Examples	• `router(config)# interface wan 2` • `router(config-if)# dmz` • `router(config-if)# exit` •	
Error Messages	% 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.	
Related Commands	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**

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

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

show mtu

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

Synopsis

show mtu

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

Multi-WAN

This section describes the commands used to set up multi-wan interface in specific devices.

interface wan <wanid>

To enter the specific WAN interface sub mode, use **interface wan** command.

Synopsis

(config)# **interface wan <wanid>**

Option Description	wanid	The WAN ID, ranging from 1 to the maximum number of supported WAN
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	For the models that support multiple WAN, the additional WAN ID is required to enter its submode. For the models that only support one WAN interface, the WAN ID is not necessary.	
Examples	`router# configure` `router(config)# interface wan 1` `router(config-if)# exit` `router(config)# exit`	
Error Messages	% Not Support Multi-WAN Feature.	
	% Invalid WAN ID. It must be 1 - <Number of WAN>	
Related Commands	N/A	

no interface wan <wanid>

To delete the specific WAN interface, use **no interface wan** command.

Synopsis

(config)# **no interface wan <wanid>**

Option Description	wanid	The WAN ID, ranging from 1 to the maximum number of supported WAN
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	The WAN ID is required to delete the specific WAN interface	
Examples	`router# configure` `router(config)# no interface wan 1` `router(config-if)# exit` `router(config)# exit`	
Error Messages	% Not Support Multi-WAN Feature.	
	% Invalid WAN ID. It must be 1 - <Number of WAN>	
	% This interface is fixed, and deletion is not permitted.	
Related Commands	N/A	

interface wan alias

To set the alias of the specific WAN interface, use **interface wan alias** command.

Synopsis

(config-if)# **alias <alias>**

Option Description	alias	The alias of the WAN interface, length ranges from 1 to 32.
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface wan 1` `router(config-if)# alias WAN_PPPoE` `router(config)# exit`	
Error Messages	% <alias> is an invalid system symbol.	
	% <alias> is over length. It must be 1 - 31.	
Related Commands	N/A	

show interface wan <wanid>

To display the configuration of the specific WAN interface, use **show interface wan** command.

Synopsis

(config)# **show interface wan <wanid>**

Option Description	wanid	The WAN ID, ranging from 1 to the maximum number of supported WAN
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	For models supporting multiple WAN, the additional **<wanid>** must be specified. For single-WAN models, the **<wanid>** is not necessary.	
Examples	`router# show interface wan 1` `WAN1` `Connect Mode : Enable` `Connect Type : DHCP` `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`	
Error Messages	% Not Support Multi-WAN Feature.	
	% Invalid WAN ID. It must be 1 - <Number of WAN>	
	% WAN ID <WAN_ID> is not exist	
Related Commands	N/A	

show interface wan status

To display the status of the specific WAN interface, use **show interface wan status** command.

Synopsis

(config)# **show interface wan status <wanid>**

Option Description	wanid	The WAN ID, ranging from 1 to the maximum number of supported WAN
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	For models supporting multiple WAN, the additional **<wanid>** must be specified. For single-WAN models, the **<wanid>** is not necessary.	
Examples	router# show interfaces wan status 1 WAN1 Alias : Vlan ID : 21 Connect Mode : Enable Connect Type : DHCP 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	
Error Messages	% Not Support Multi-WAN Feature.	
	% Invalid WAN ID. It must be 1 - <Number of WAN>	
	% WAN ID <WAN_ID> is not exist	
Related Commands	N/A	

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**

Option Description	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.
Defaults	Disabled.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Bridge member ports can be configured via **interface ethernet** and its sub-level **bridge group** commands. • Maximum number of bridge interface is one which means either a port-based bridge or a zone-based bridge interface can be configured. • Enabling the '**no shutdown**' command when the zone-based bridge is already active will switch to port-based bridge mode while disabling the zone-based bridge simultaneously.	
Examples	• Specify PORT5, PORT6, PORT7 as port-based bridge members. `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)#` • Specify the IP address and netmask of the port-based bridge interface. `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)#` • Specify the name of the port-based bridge interface. `router# configure` `router(config)# interface bridge` `router(config-brg)# name BRG_LAN`	

	router(config-brg)# exit router(config)# • Enable the port-based bridge interface. router# configure router(config)# interface bridge router(config-brg)# no shutdown router(config-brg)# exit router(config)#
Error Messages	% is over length. It must be 1 - 12.
	^Parse error
	^Incomplete command
Related Commands	show interfaces bridge interface ethernet bridge

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**

Option Description	mod-port	Port ID (consists of module/port-number) or list. E.g. 1/1,2,3,2/1-3,5,...
	bridge group	Adds/removes the Ethernet interface to/from bridge member ports
Defaults	Unselected.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• If bridge member is empty, remember to disable the bridge interface by using **interface bridge** and **shutdown** command. • Once all member ports have been specified, use **interface bridge** and **no shutdown** command to let settings take effect. • When the sub-level command '**bridge group**' is specified, an additional VLAN ID will be created automatically. • 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. • At least two member ports are selected before using this bridge interface. • Maximum number of bridge member of TN-4908 series is 8. • Maximum number of bridge member of TN-4916 series is 16.	
Examples	Specify PORT5, PORT6, PORT7 as port-based bridge members. (A comprehensive example can be found in the command "**interface bridge**") `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`	
Error Messages	% Illegal parameter.	
	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	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.
Defaults	Disabled	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Bridge member ports can be configured via **interface vlan zone-base-bridge** commands. • Maximum number of bridge interface is one which means either a port-based bridge or a zone-based bridge interface can be configured. • 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. • Ensure to designate the PVID for the ports allocated to the zone-based bridge interface.	
Examples	• Assign VLAN(5) to PORT5 and PORT6 and VLAN(8) to PORT7 and PORT8. Specify VLAN(5), VLAN(8) as zone-based bridge members. `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` • Specify the IP address and netmask of the zone-based bridge interface. `router# configure` `router(config)# interface zone-base-bridge` `router(config-brg)# ip address 192.168.58.254 255.255.255.0`	

	router(config-brg)# exit • Specify the name of the zone-based bridge interface. router# configure router(config)# interface zone-base-bridge router(config-brg)# name BRG_LAN router(config-brg)# exit • Enable the zone-based bridge interface. router# configure router(config)# interface zone-base-bridge router(config-brg)# no shutdown router(config-brg)# exit
Error Messages	% is over length. It must be 1 - 12.
	^Parse error
	^Incomplete command
Related Commands	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>

Option Description	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.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• This command only applies to LAN interface using the non-management VLAN. • Once all member ports have been specified, use **interface zone-base-bridge** and **no shutdown** command to let settings take effect. • At least two member ports are selected before using this bridge interface. • Only one VLAN segment (VID) is allowed in each zone. • Eligible VIDs should be configured before selecting the bridge member. • Maximum number of bridge member of TN-4900 series is 4.	
Examples	Specify VLAN(5), VLAN(8) as zone-based bridge members. (A comprehensive example can be found in the command "**interface zone-base-bridge**") 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	
Error Messages	% is over length. It must be 1 - 12.	
	vlan id does not exist!!	
	^Parse error	
	^Incomplete command	
Related Commands	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

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

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

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

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

show bypass

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

Synopsis

show bypass

Option Description	show	Show configuration
	bypass	Display LAN bypass configuration
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`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)`	
Error Messages	^Incomplete command	
	^Parse error	
Related Commands	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**

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

Virtual Interface (Loopback Interface)

interface lookback

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

Synopsis

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

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

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

Option Description	ip	Loopback interface IP address
	mask	Loopback interface IP mask
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	`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`	
Error Messages	N/A	
Related Commands	show interface loopback	

shutdown/no shutdown

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

Synopsis

Option Description	shutdown	Enable loopback interface
	no shutdown	Disable loopback interface
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	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	
Error Messages	N/A	
Related Commands	show interface loopback	

GRE Interface

This section describes the commands used in the **Generic Routing Encapsulation** (GRE) interface.

interface gre

To create a new GRE tunnel, use **interface gre** command.

Synopsis

(config)# **interface gre {<STRING:name>}**

Option Description	gre	Create a new GRE tunnel
	name	GRE tunnel name
Defaults	N/A	
Command Modes	Global configuration/GRE submode	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gre test` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

ip address

To set the GRE tunnel IP address, use **ip address** command.

Synopsis

(config-gre)# **ip address {IPV4ADDR:ipaddr} {IPV4ADDR:netmask}**

Option Description	ipaddr	Set the GRE tunnel IP address
	netmask	Set the GRE tunnel netmask
Defaults	N/A	
Command Modes	GRE mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gre test` `router(config-gre)# ip address 10.10.10.10 255.255.255.0` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

tunnel source

To set the GRE tunnel source, use **tunnel source** command.

Synopsis

(config-gre)# **tunnel source {ip address}**

Option Description	tunnel source	Set the GRE tunnel source
	ip address	Set the GRE tunnel source IP address
Defaults	N/A	
Command Modes	GRE mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gre test` `router(config-gre)# tunnel source 77.77.77.77` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

tunnel destination

To set the GRE tunnel destination, use **tunnel destination** command.

Synopsis

(config-gre)# **tunnel source {ip address}**

Option Description	tunnel destination	Set the GRE tunnel destination
	ip address	Set the GRE tunnel destination IP address
Defaults	N/A	
Command Modes	GRE mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gre test` `router(config-gre)# tunnel destination 77.77.77.77` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

shutdown

To disable the selected GRE interface, use **shutdown** command.

Synopsis

(config-gre)# **shutdown**

Option Description	shutdown	Disable the selected GRE interface
Defaults	N/A	
Command Modes	GRE mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gre test` `router(config-gre)# shutdown` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

no shutdown

To reset or disable the GRE configuration, use **no shutdown** command.

Synopsis

(config-gre)# **shutdown**

Option Description	no	Reset or disable configurations
	shutdown	Disable the selected GRE interface
Defaults	N/A	
Command Modes	GRE mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gre test` `router(config-gre)# no shutdown` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

exit

To exit the GRE tunnel sub mode, use **exit** command.

Synopsis

(config-gre)# **exit**

Option Description	exit	Exit the GRE tunnel sub mode
Defaults	N/A	
Command Modes	GRE mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gre test` `router(config-gre)# exit` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

no interface gre

To delete or disable the GRE configuration, use **no interface gre** command.

Synopsis

(config)# **no interface gre {<STRING:name>}**

Option Description	no	Delete or disable the configuration
	gre	GRE tunnel
	name	GRE tunnel name
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# no gre test` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

show interface gre

To show the GRE tunnel information, use **show interface gre** command.

Synopsis

(config)# **show interface gre {<STRING:name>}**

Option Description	gre	GRE tunnel
	name	GRE tunnel name
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# show interface gre gre_1`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

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>

Option Description	ip	Interface IP address
	mask	Mask IP address
Defaults	IP: 192.168.1.1 Mask: 255.255.255.0	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	`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`	
Error Messages	% Configured IP Address is in the subnet of interface BRG_LAN	
	% Invalid parameter!	
	^Incomplete command	
	^Parse error	
Related Commands	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**

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

Related Commands	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

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

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

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

Option Description	N/A
Defaults	N/A
Command Modes	Global configuration
Usage Guidelines	N/A
Examples	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
Error Messages	^Incomplete command
	^Parse error
Related Commands	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 **interfce lfp** command.

Synopsis

(config)# **interface lfp**

(config)# **no interface lfp**

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

Option Description	port1	The name of the first LFP port
	port2	The name of the second LFP port
Defaults	N/A	
Command Modes	By product: the default LFP ports for EDR-G9004 are 1/3 & 1/4 and not configurable.	
Usage Guidelines	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.	
Examples	Configure ethernet port 1/3 & 1/4 as LFP ports `router# configure` `router(config)# interface lfp port 1/3 1/4` `router(config)# exit`	
Error Messages	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	
Related Commands	show interface lfp	

show interfaces lfp

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

Synopsis

show interfaces lfp

Option Description	N/A
Defaults	N/A
Command Modes	Global configuration
Usage Guidelines	N/A
Examples	`# show interfaces lfp` `Link Fault Passthrough Setting` `State : Disable` `Ports : 1/3, 1/4`
Error Messages	N/A
Related Commands	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 }**

Option Description	0	Moxa default/System default alarm
	1	Advanced/Configuration change alarm
Defaults	0	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`Specify/modify Fault LED behavior with 0.` `router# configure` `router(config)# led mode 0` `router(config)# exit`	
Error Messages	% Mode must be 0 or 1.	
	^Parse error	
	^Incomplete command	
Related Commands	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>	

VXLAN

interface vxlan

To configure VXLan interface, use the interface **vxlan** global configuration command.

Synopsis

(config)# **interface vxlan** <name>

Option Description	vxlan	Create new VXLAN interface.
	name	Specify a VXLAN interface name.
Defaults	#	
Command Modes	Global configuration + enter vxlan sub mode	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# vxlan vxlan_test` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

vxlan id

To configure VXLAN ID, use the **id** VXLAN configuration command.

Synopsis:

(config-vxlan)# **id** <vxlan_id>

Option Description	vxlan_id	Set vxlan interface id (1 to 16777215).
Defaults	N/A	
Command Modes	vxlan mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# vxlan vxlan_test` `router(config-vxlan)# id 10` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

vxlan local-ip

To configure VXLAN local IP address, use the **vxlan local-ip** VXLAN configuration command.

Synopsis:

vxlan local-ip

(config-vxlan)# **local-ip** <ipaddr>

Option Description	local-ip	Set VXLAN interface local IP address.
	ipaddr	Specify a VXLAN tunnel local IP address (IPv4 address) in 4 octets (123.123.123.123).
Defaults	#	
Command Modes	vxlan mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# vxlan vxlan_test` `router(config-vxlan)# local-ip 77.77.77.77` `router(config)# exit`	

Error Messages	^Parse error
	^Incomplete command
Related Commands	N/A

vxlan remote-ip

To configure VXLAN remote IP address, use the **vxlan remote-ip** VXLAN configuration command.

Synopsis:

(config-vxlan)# **remote-ip** <ipaddr>

Option Description	remote-ip	Set VXLAN interface remote IP address.
	ipaddr	Specify a VXLAN tunnel remote IP address (IPv4 address) in 4 octets (123.123.123.123).
Defaults	#	
Command Modes	vxlan mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# vxlan vxlan_test` `router(config-vxlan)# remote-ip 77.77.77.88` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

vxlan remote-ip

To configure VXLAN remote IP address, use the **vxlan remote-ip** VXLAN configuration command.

Synopsis:

(config-vxlan)# **dstport** <port_number>

Option Description	dstport	Set VXLAN interface dstport
	port_number	Specify VXLAN interface dstport number (1024 to 65535)
Defaults	4789	
Command Modes	vxlan mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# vxlan vxlan_test` `router(config-vxlan)# dstport 4789` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

vxlan id enable/disable

To toggle VXLAN interface, use the **status** VXLAN configuration command.

Synopsis:

(config-vxlan)# **status** {enable | disable}

Option Description	enable	Set VXLAN interface to enabled.
	disable	Set VXLAN interface to disabled.
Defaults	Enable	
Command Modes	vxlan mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# vxlan vxlan_test` `router(config-vxlan)# status disable` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

vxlan exit

To exit VXLAN configuration submode, use the **exit** VXLAN configuration command.

Synopsis:

(config-vxlan)# **exit**

Option Description	exit	Leave VXLAN submode.
Defaults	#	
Command Modes	vxlan mode configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# vxlan test` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

no interface vxlan

To delete a VXLAN interface, use the **no interface vxlan** global configuration command.

Synopsis:

(config)# **no interface vxlan** <name>

Option Description	no	Delete
	vxlan	Configure VXLAN interface.
	name	Specify VXLAN interface name.
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# no vxlan vxlan_test` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

no interface vxlan zone-base-bridge

To delete a VXLAN zone base, use the **no interface vxlan zone-base-bridge** global configuration command.

Synopsis:

(config)# **no interface vxlan** <name> **zone-base-bridge**

Option Description	no	delete
	vxlan	vxlan interface
	name	vxlan interface name
	zone-base-bridge	remove zone-base which id as same as vxlan interface name
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# no interface vxlan vxlan_test zone-base-bridge` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

interface vxlan zone-base-bridge

To configure a VXLAN zone base, use the **interface vxlan zone-base-bridge** global configuration command.

Synopsis:

(config)# **interface vxlan** <name> **zone-base-bridge** <Zone_Index> <Zone_Name>

Option Description	**vxlan**	VXLAN interface.
	name	VXLAN interface name.
	zone-base-bridge	Configure zone-base-bridge.
	Zone_Index	Specify zone-base-bridge index as an integer (EDR: 9010 ex : 1 to 4)
	Zone_Name	Specifies the identifier for this interface within the zone-base bridge.
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface vxlan vxlan_test zone-base-bridge 1 vxlan_test` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

interface vxlan zone-base-bridge bridge_index

To join a VXLAN zone base bidge index, use the **interface vxlan zone-base-bridge** global configuration command and specify a Bridge_Index.

Synopsis:

(config)# **interface vxlan** <name> **zone-base-bridge** <Zone_Index> <Zone_Name> < Bridge_Index>

Option Description	**vxlan**	vxlan interface
	name	vxlan interface name
	zone-base-bridge	Configures zone-base-bridge
	Zone_Index	Specify zone-base-bridge index as an integer (EDR-9010 ex: 1 to 4)
	Zone_Name	Specifies the identifier for this interface within the zone-base bridge.
	Bridge_Index	Zone-base-bridge to join as an integer (EDR-9010 ex: 1 to 8)
Defaults	Bridge_Index default 1	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface vxlan vxlan_test zone-base-bridge 1 vxlan_test 1` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

show interfaces vxlan

To show VXLAN interface information, use the **show interfaces vxlan** global configuration command.

Synopsis:

show interfaces vxlan

Option Description	**vxlan**	display all vxlan interface information
Defaults	#	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router#show interfaces vxlan`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

Routing

Unicast Route

ip route static

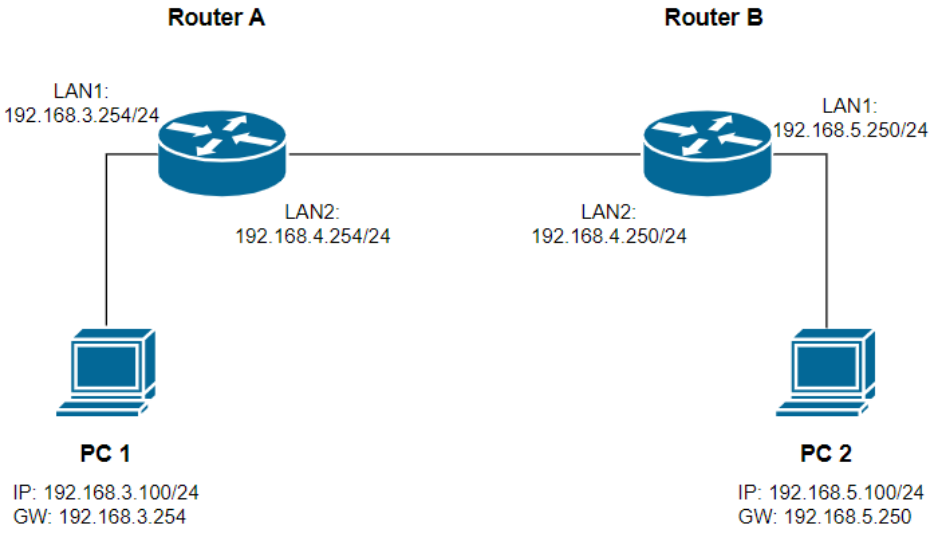
To create a static route entry, use the **ip route static** global configuration command. To delete the static route entry, use the **no** form of this command.

Synopsis

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

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

Option Description	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
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• Maximum number of static multicast route entries is 512 • Network interfaces related to this routing feature must be created in advance.	
Examples	Static route function: Prerequisites: • TN router A: - LAN1: 192.168.3.254/24, VLAN ID=3 - LAN2: 192.168.4.254/24, VLAN ID=4 • 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: a) When the network topology is fixed, no router is expected to be removed or added, configuring static route on each router is considered. b) PC1 can communicate with PC2 via its gateway: 192.168.3.254. c) 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`
Error Messages	% is existed in Static Route list
	% is over length. It must be 1 - 10.
	Invalid Metric. It must be 1 - 255
	^Parse error
	^Incomplete command
Related Commands	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>

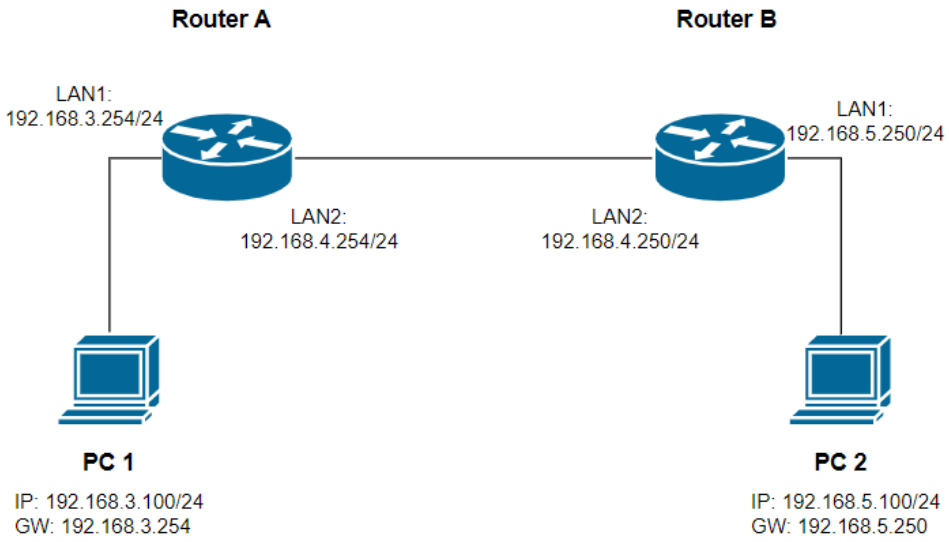
Set version of RIP
(config-rip)# **version** {**1** | **2**}

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**

Option Description	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.
Defaults	Disabled	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	Network interfaces related to this routing feature must be created in advance.	
Examples	RIP function: Prerequisites: • TN router A: - LAN1: 192.168.3.254/24, VLAN ID=3 - LAN2: 192.168.4.254/24, VLAN ID=4 • 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: a) 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. b) This example takes advantage of RIP to generate a routing table on each router automatically. c) PC1 can communicate with PC2 via its gateway: 192.168.3.254. d) 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>

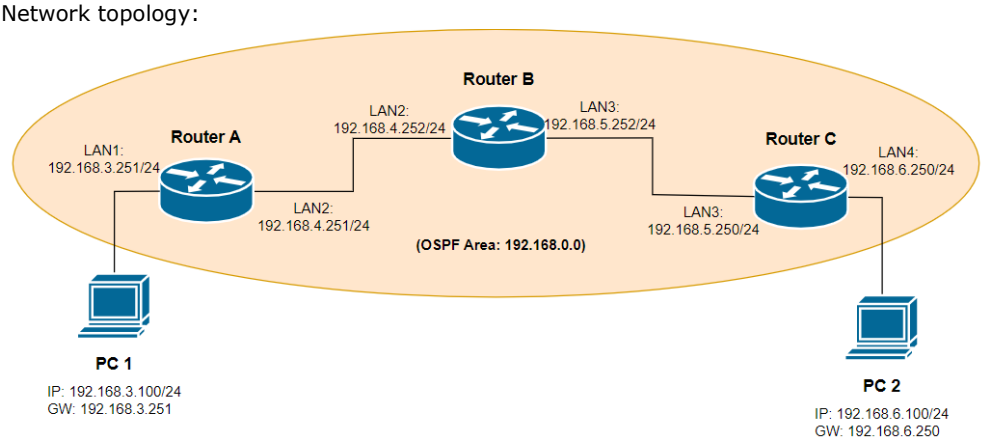
Set Area ID with Stub/NSSA Area Type
(config-ospf)# **area** <area-id> [{**stub metric** <number> |
nssa metric <number>}]

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
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	Network interfaces related to this routing feature must be created in advance.	
Examples	OSPF function: Prerequisites: • TN router A: - LAN1: 192.168.3.251/24, VLAN ID=3 - LAN2: 192.168.4.251/24, VLAN ID=4 • TN router B: - LAN2: 192.168.4.252/24, VLAN ID=4 - LAN3: 192.168.5.252/24, VLAN ID=5 • TN router C: - LAN3: 192.168.5.250/24, VLAN ID=5 - LAN4: 192.168.6.250/24, VLAN ID=6 • PC (1): - IP: 192.168.3.100/24 - Gateway: 192.168.3.251 • PC (2): - IP: 192.168.6.100/24 - Gateway: 192.168.6.250 Network topology:  Scenario: a) 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. b) This example takes advantage of OSPF to generate a routing table on each router automatically. c) PC1 can communicate with PC2 via its gateway: 192.168.3.251. d) PC2 can communicate with PC1 via its gateway: 192.168.6.250. Commands: [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`	

	[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`
Error Messages	% 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
Related Commands	show ip ospf show ip route ip ospf

show ip route

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

Synopsis

show ip route [{**static** | **kernel**}]

Option Description	static	Specifies to display the static routing entries
	kernel	Specifies to display the kernel routing table
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ip route	

show ip rip

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

Synopsis

show ip rip

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	router# show ip rip RIP Protocol : Disable RIP Version : v2 Distribution Connetced : Disable Statis : 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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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}]

Option Description	database	Specifies to display OSPF database
	instance	Specifies to display OSPF routing interface
	neighbor	Specifies to display OSPF neighbor information
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	router # show ip ospf OSPF Golbal 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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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**

Option Description	N/A	
Defaults	Disabled.	
Command Modes	Global configuration	
Usage Guidelines	• In order to let all static multicast route entries take effect, Static Multicast Route mode needs to be enabled. • Network interfaces related to this routing feature must be created in advance.	
Examples	* An illustrative example can be found in the command "**ip mroute group**".	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ip mroute group show ip mroute	

ip mroute group

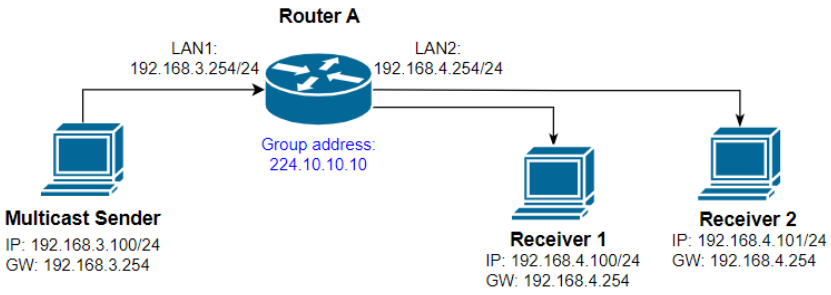
To create a static multicast route entry, use the **ip mroute group** global configuration command. To delete the static multicast route entry, use the **no** form of this command.

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>

Option Description	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 **any** for any IP address.
	in	Specifies inbound interface
	in-if	The inbound interface name of the multicast stream. Must be a LAN or WAN interface.
	out	Specifies outbound interface
	out-ifs	The outbound interface names of the multicast stream. Comma separated for more than one outbound interface. Must be a LAN or WAN interface.
	enable	Enables this static multicast route entry
	disable	Disables this static multicast route entry
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• In order to let all static multicast route entries take effect, Static Multicast Route mode needs to be enabled. • Network interfaces related to this routing feature must be created in advance.	
Examples	Static multicast route function: Prerequisites:	

	• TN router A: - LAN1: 192.168.3.254/24, VLAN ID=3 - LAN2: 192.168.4.254/24, VLAN ID=4 • 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: a) 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. b) This example takes advantage of RIP to generate a routing table on each router automatically. c) PC1 can communicate with PC2 via its gateway: 192.168.3.254. d) 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`
Error Messages	% is not existed
	% Inbound interface is unacceptable
	% Outbound interface is unacceptable
	^Parse error
	^Incomplete command
Related Commands	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**}

Option Description	kernel	Specifies to display multicast forwarding table
	static	Specifies to display static multicast route configuration settings
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ip multicast-routing static ip mroute group	

Delete Rule Function

Set multiple "Static Multicast Route" rules for the same group but with different inbound interfaces through the CLI.

Synopsis

(config)# **no ip mroute group** <mcast_addr> **src** <mcast_addr | ANY> { in <STRING:inbifname> }

Option Description	no	Delete the entry / reset to default value
	ip	Configure IP parameters
	mroute	Configure static multicast route
	group	Multicast group
	src	Multicast source
	<mcast_addr>	Multicast stream IP address
	ANY	ANY source group
	in	Inbound interface
	<inbound_interface>	Inbound interface name
Defaults	N/A	
Command Modes	Global Configuration Mode	
Usage Guidelines	N/A	
Examples	1. Delete the rule corresponding to a specific inbound interface for a particular multicast group. Firewall/VPN Router 00000(config)# no ip mroute 239.0.0.1 src ANY in LAN 2. Delete the rule corresponding to all inbound interface for a particular multicast group. (Compatible with previous command.) Firewall/VPN Router 00000(config)# no ip mroute 239.0.0.1 src ANY	
Error Messages	% No such static multicast route	
Related Commands	ip multicast-routing static ip mroute group	

Enable/Disable Rule Function

Synopsis

(config)# **ip mroute group** <mcast_addr> **src** <mcast_addr | ANY> { in <STRING:inbifname> } enable/disable

Option Description	no	Delete the entry / reset to default value
	ip	Configure IP parameters
	mroute	Configure static multicast route
	group	Multicast group
	src	Multicast source
	<mcast_addr>	Multicast stream IP address
	ANY	ANY source group
	in	Inbound interface
	<inbound_interface>	Inbound interface name
	enable/disable	Enable or disable target rule
Defaults	The previous rule status	
Command Modes	Global Configuration Mode	
Usage Guidelines	N/A	

Examples	1. Enable the rule corresponding to a specific inbound interface for a particular multicast group. Firewall/VPN Router 00000(config)# ip mroute 239.0.0.1 src ANY in LAN enable 2. Enable the rule corresponding to all inbound interface for a particular multicast group. (Compatible with previous command.) Firewall/VPN Router 00000(config)# ip mroute 239.0.0.1 src ANY enable 3. Disable the rule corresponding to a specific inbound interface for a particular multicast group. Firewall/VPN Router 00000(config)# ip mroute 239.0.0.1 src ANY in LAN disable 4. Disable the rule corresponding to all inbound interface for a particular multicast group. (Compatible with previous command.) Firewall/VPN Router 00000(config)# ip mroute 239.0.0.1 src ANY disable
Error Messages	% No such static multicast route
Related Commands	ip multicast-routing static ip mroute group

vrrp-master-only

To enable or disable the VRRP-Master Only function, use the **vrrp-master-only** command.

Synopsis

(config)# **ip mroute vrrp-master-only**

(config)# **no ip mroute vrrp-master-only**

Option Description	ip	Global IP Configuration Subcommands
	mroute	Configure static multicast route
	vrrp-master-only	Enable/disable VRRP Master Only.
	no	Delete entry / reset to default value
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Enable VRRP Master Only. Firewall/VPN Router 00000# configure Firewall/VPN Router 77777(config)# ip mroute vrrp-master-only Disable VRRP Master Only. Firewall/VPN Router 00000# configure Firewall/VPN Router 77777(config)# no ip mroute vrrp-master-only	
Error Messages	N/A	
Related Commands	show redundancy mode show redundancy turbo-chain	

VRRP checksum

To configure the checksum calculation method for VRRPv3 packets, use the **checksum** command. To restore defaults, us the **no** form of the command.

Synopsis

(config-vrrp)# **checksum** {rfc5798 | rfc9568}
(config-vrrp)# **no checksum**

(config-vif-vrrp)# **checksum** {rfc5798 | rfc9568}
(config-vif-vrrp)# **no checksum**

Option Description	checksum	Configure checksum calculation method
	rfc5798	Specify calculation of the checksum by including the IPv6 pseudo-header. This maintains backward compatibility with the legacy behavior defined in RFC 5798.
	rfc9568	Calculates the checksum by excluding the IPv6 pseudo-header, complying with the updated standard defined in RFC 9568.
	No	Set to default value.
Defaults	rfc5798	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	**Standards Compliance**: Use the rfc9568 option to comply with the latest RFC 9568 standard, which removes the pseudo-header requirement for IPv6 VRRPv3 checksums. **Legacy Compatibility**: The default rfc5798 option is highly recommended when operating with legacy hardware routers that strictly follow RFC 5798 checksum rules. **Interoperability**: It is critical that all routers participating in the same VRRP group use identical checksum calculation methods. A mismatch will cause checksum validation failures and lead to a split-brain scenario.	
Examples	Configure checksum calculation to comply with RFC 9568 via VRRP entry `router# configure` `router(config)# vrrp 1` `router(config-vrrp)# checksum rfc9568` `router(config)# exit` `Restore default checksum calculation (RFC 5798)  via VRRP entry` `router# configure` `router(config)# vrrp 1` `router(config-vrrp)# no checksum` `router(config)# exit` Configure checksum calculation to comply with RFC 9568 via Interface LAN `router# configure` `router(config)# interface lan` `router(config-if)# vrrp 1 vrip 1.1.1.1` `router(config-vif-vrrp)# checksum rfc5798` `router(config-if)# exit` `router(config)# exit` Restore default checksum calculation (RFC 5798) via Interface LAN `router# configure` `router(config)# interface lan` `router(config-if)# vrrp 1 vrip 1.1.1.1` `router(config-vif-vrrp)# no checksum` `router(config-if)# exit` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
	% Checksum configuration is only supported in VRRPv3.	
Related Commands	vrrp <UINT:version> vrrp <UINT:index> interface <STRING:ifname>	

Broadcast Forward

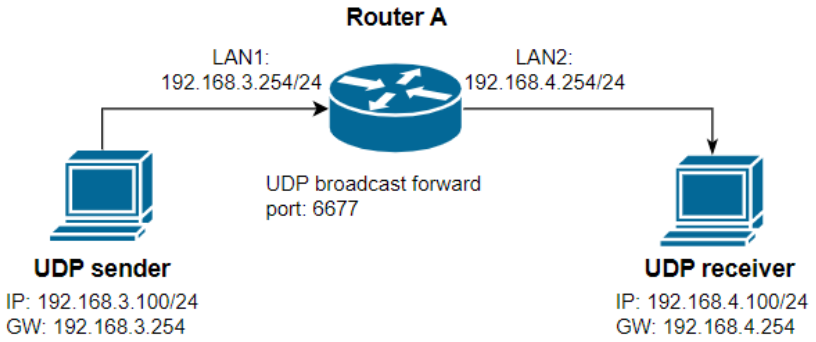
ip broadcast-forward

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>

Option Description	in	Specifies inbound interface
	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
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	• Inbound and outbound network interfaces must be configured in advance. • Multiple UDP ports can be configured in a comma separated port list.	
Examples	UDP broadcast forwarding function: Prerequisites: • TN router A: - LAN1: 192.168.3.254/24, VLAN ID=3 - LAN2: 192.168.4.254/24, VLAN ID=4 • UDP sender: - IP: 192.168.3.100/24 - Gateway: 192.168.3.254 • UDP receiver: - IP: 192.168.4.100/24 - Gateway: 192.168.4.254 Network topology:  Scenario: a) The UDP sender broadcasts packets to the destination port 6677. b) The UDP receiver in a different subnet can receive the broadcast packets.	

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

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

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

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

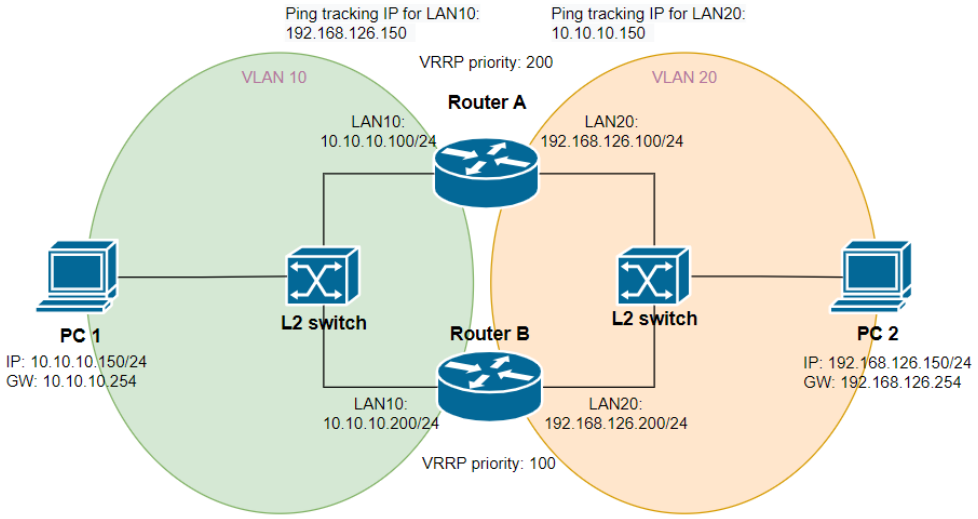
Set VRRP interface entry configuration
(config-vrrp)# {**vrrp** |
accept |
vrid <vid> |
virtual-ip <v-ip> |
priority <prio> |
preempt [**delay** <preemp-delay>] |
interface <ifs> |
adver-interval {**v2** | **v3**} <adv-interval>}

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 Description		
	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
Defaults	Disabled.	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• In order to maintain the network availability between two different networks, enabling ping tracking is highly recommended. An illustrative example can be found below. • Maximum number of VRRP interfaces is 16. • Network interfaces related to this routing feature must be created in advance.	
Examples	VRRP with ping tracking: Prerequisites: • TN router A: - LAN10: 10.10.10.100/24, VLAN ID=10 - LAN20: 192.168.126.100/24, VLAN ID=20 • TN router B: - LAN10: 10.10.10.200/24, VLAN ID=10 - LAN20: 192.168.126.200/24, VLAN ID=20 • PC 1: - IP: 10.10.10.150/24 - Gateway: 10.10.10.254 • PC 2: - IP: 192.168.126.150/24 - Gateway: 192.168.126.254 Network topology:  Scenario: a) Router A enables VRRP v3 and acts as the VRRP master with a higher priority (200). b) Router B enables VRRP v3 and acts as the VRRP backup with a lower priority (100). c) Virtual IP for VLAN10 is 10.10.10.254; virtual IP for VLAN 20 is 192.168.126.254	

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
```

	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
Error Messages	% 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
Related Commands	router vrrp vrrp version show vrrp

show vrrp

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

Synopsis

show vrrp [**detail**]

Option Description	detail	Specifies to display VRRP detailed settings
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	

	Preempt Delay (sec): 10 Native Interface Tracking: -- Object Ping Tracking: Target IP: 192.168.126.150 Intervel (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 Intervel (sec): 1 Timeout (sec): 3 Success Count: 3 Failure Count: 3
Error Messages	^Parse error
	^Incomplete command
Related Commands	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>}**

Option Description	di	Delete DI on/off
	link	Detect Port Link on/off
	port	Device port
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	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	
Error Messages	Port id must be %d - %d.	
	^Parse error	
	^Incomplete command	
Related Commands	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>|**

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

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

no wan_redundancy

To disable WAN redundancy, use the **no wan_redundancy** command.

Synopsis

(config)# **no wan_redundancy**

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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	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 ---	
Error Messages	N/A	
Related Commands	wan_redundancy mode no wan_redundancy	

WAN Backup

wan_backup interface

To run the WAN backup to the remote host, use the following command.

Synopsis

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

Option Description	name	The WAN interface name
	remoteaddr	The remote host address for ping check of the specific interface. IP address and domain name are both acceptable.
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	The "interface remotehostip" command has been deprecated and is replaced by this command.	
Examples	`router# configure` `router(config)# wan_backup` `router(config-wan-backup)# interface WAN2 remotehost 8.8.8.8` `router(config-wan-backup)# interface WAN3 remotehost www.google.com` `router(config)# exit`	
Error Messages	% Invalid WAN Interface Name.	
Related Commands	show wan_redundancy no interface remotehost	

wan_backup no interface

To disable the WAN backup to the remote host, use the following command.

Synopsis

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

Option Description	name	The WAN interface name
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	The "no interface remotehostip" command has been deprecated and is replaced by this command.	
Examples	`router# configure` `router(config)# wan_backup` `router(config-wan-backup)# no interface WAN2 remotehost` `router(config)# exit`	
Error Messages	% Invalid WAN Interface Name.	
Related Commands	show wan_redundancy no interface remotehost	

wan_backup switchmode

To configure switch mode of WAN Backup, use the **wan_backup switchmode** command.

Synopsis

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

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

wan_backup ping_check

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

Synopsis

(config-wan-backup)# **ping_check**

Option Description	N/A	
Defaults	Disabled	
Command Modes	Sub-level configuration	
Usage Guidelines	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.	
Examples	`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`	
Error Messages	% This option is not configurable.	
	% Remote host IP address should be configured on the enabled interface first.	
Related Commands	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**

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

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

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

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

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

Option Description	name	The WAN interface name.
	priority	The priority value of the specific interface. Ranges from 1 to the number of total WAN interfaces.
Defaults	In general, the default priority of the first WAN interface is 1, the second is 2, and so on.	
Command Modes	Sub-level configuration	
Usage Guidelines	For some models, the priority value of some interface may be fixed and not configurable.	
Examples	`router# configure` `router(config)# wan_backup` `router(config-wan-backup)# interface WAN2 priority 2` `router(config-wan-backup)# exit` `router(config)# exit`	
Error Messages	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN).	
	% Invalid priority range. (1 -> nums of wan interface)	
	% Priority is not configurable	
Related Commands	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>**

Option Description	name	The WAN interface name.
	ipaddr	The remote IP address for ping check of the specific interface. Non-unicast IP address and 0.0.0.0 is no acceptable.
Defaults	0.0.0.0	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	`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`	
Error Messages	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN).	
	% Invalid IP Address.	
Related Commands	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**

Option Description	name	The WAN interface name.
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	Before clearing the remote IP address, ping checks should be disabled.	
Examples	`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`	
Error Messages	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN).	
	% Invalid IP Address.	
	% when Ping Check is enabled, remote host IP could not be cleared.	
Related Commands	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**

Option Description	name	The WAN interface name.
Defaults	Disabled. But for some models, some interfaces may be non-configurable and enabled by default.	
Command Modes	Sub-level configuration	
Usage Guidelines	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.	
Examples	`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`	
Error Messages	% 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.	
Related Commands	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**

Option Description	name	The WAN interface name.
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	`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`	
	% Invalid WAN Interface ex(WAN, CELLULAR_WAN, WIFI_WAN).	

Error Messages	% This option is not configurable.
Related Commands	show wan_redundancy wan_backup no interface enable

Ping Response

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**

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

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**

Option Description	ip	Configure IP Parameter
	ping-response	Enable Ping Response/Disable Ping Response
	no	Negate Command
Defaults	Disabled on all WAN interfaces, otherwise, enabled.	

Command Modes	WAN Interface Configuration LAN Interface Configuration VLAN Interface Configuration Port-based Bridge Interface Configuration Zone-based Bridge Interface Configuration Cellular Interface Configuration
Usage Guidelines	N/A
Examples	`Enable ping response on the LAN interface.` `router# configure` `router(config)# interface lan` `router(config-if)# ip ping-response`
Error Messages	^Parse error
	^Incomplete command
Related Commands	N/A

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**

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

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**

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

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**

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

Synopsis

Enable / Disable ping response interface

(config)# **interface ping-response**

(config)# **no interface ping-response**

Enable / Disable ping response to a network interface

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

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

Set / Disable ping response log severity or destination

(config)# **logging ping-response** { severity <severity-level> flash | syslog | trap }

(config)# **no logging ping-response** { flash | syslog | trap }

Enable / Disable ping response log

(config)# **logging ping-response**

(config)# **no logging ping-response**

Enable / Disable / Remove ping response policy

(config)# **ip ping-response** <index> enable

(config)# **ip ping-response** <index> disable

(config)# **no ip ping-response** <index>

Insert ping response policy

(config)# **ip ping-response** <index>

(config-ping-res)# **interface** <incoming-interface-name>

(config-ping-res)# **src-ip** <src_ip>

(config-ping-res)# **action** { allow | deny }

(config-ping-res)# **exit**

Display ping response setting

show **ip ping-response**

show ip ping-response

To show ip ping response, use **show ip ping-response** command.

Option Description	show	Configure IP Parameter
	ip	Internet Protocol
	ping-response	Ping response information
Defaults	Disabled on all WAN interfaces, otherwise, enabled.	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	`Show ping response setting` `router# show ip ping response`	
Error Messages	N/A	
Related Commands	N/A	

show logging event-log ping-response

To show logging event log ping response severity and range, use **show logging event-log ping-response** command.

Synopsis

show logging event-log ping-response { severity <range>}

Option Description	show	Show Configurations or Status
	ip	Internet Protocol
	ping-response	Ping Response
	logging	Log
	event-log	Event Log
	severity	Severity
Defaults	Disabled on all WAN interfaces, otherwise, enabled.	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	Show ping response setting `router# show logging event-log ping-response` `0 message lines logged`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

Option Description	ip	IP Configurations
	ping-response	Ping Response Configurations
	interface	Network Interface Configurations
	logging	Logging Configurations
	severity	Log Severity Setting
	severity-level	Log Severity
	flash	Log to Local Storage
	syslog	Log to Syslog Server
	trap	Log to SNMP Trap Server
	enable	Enable the policy/setting
	disable	Disable the policy/setting
	index	Policy Index
Defaults	• Ping Response Policy is enabled. • Ping Response Policy interface is any. • Ping Response Policy source IP is any. • Ping Response Policy action is allowed.	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`Enable ping response interface` `router(config)# interface ping-response`	
Error Messages	N/A	
Related Commands	show ip ping-response	

Option Description	interface	Packet's incoming interface
	src-ip	Packet's source IP or subnet
	action	Action to matched packets.
	allow	Accept the matched packets.
	deny	Drop the matched packets.
Defaults	• Ping Response Policy is enabled. • Ping Response Policy interface is any. • Ping Response Policy source IP is any. • Ping Response Policy action is allowed.	
Command Modes	Ping-Response Policy Configuration	
Usage Guidelines	N/A	
Examples	`Allow ping response from 140.113.0.0/16` `router(config)# ip ping-response 1` `router(config-ping-res)# src-ip 140.113.0.0/16` `router(config-ping-res)# action allow` `router(config-ping-res)# exit`	
Error Messages	N/A	
Related Commands	show ip ping-response	

4. NAT, VPN and Firewall Functions

This chapter describes the commands for the NAT, VPN, and firewall 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 **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information. • Enter configuration mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	(config)#	To exit to privileged EXEC mode, enter **exit**.	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example **l3l7-policy <firewall-index>** command and press enter	(config-l3l7-policy)#	To exit to global configuration mode, enter **exit**.	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-ifname> **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-ifname> **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**

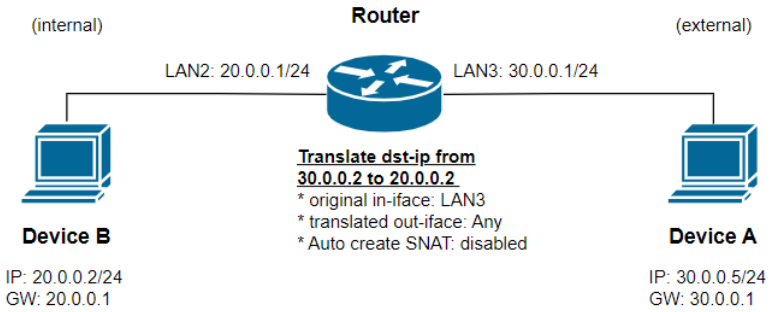
Set / Clear Double NAT (For mode 1-1, PAT only).
(config-nat)# **double-nat**
(config-nat)# **no double-nat**

Show NAT configuration
(config-nat)# **show**

Abort NAT configuration
(config-nat)# **abort**

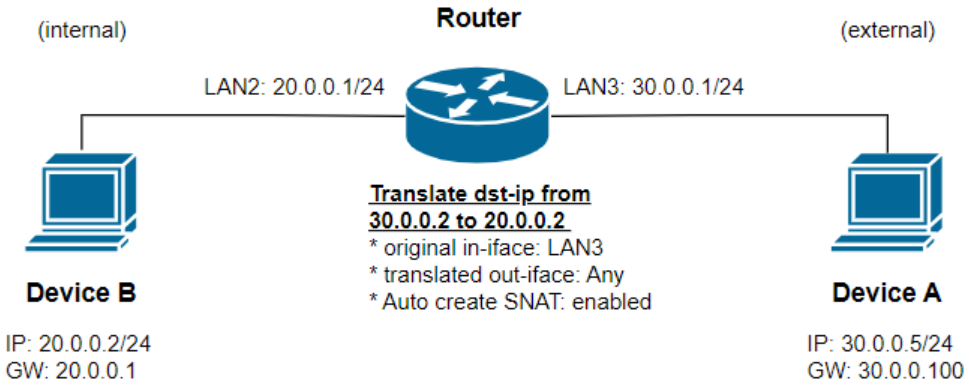
Save and Exit NAT configuration.
(config-nat)# **exit**

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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• No modification function is provided. In case modification on a specific index is required, remove it first and then add a new rule. • Types a valid index to enter sub-level configuration mode. • Maximum number of rules is 512. • Exits the sub-level configuration mode to let settings take effect. • Prior to confirming new NAT settings, utilize the "settingcheck" command to prevent the router from implementing incorrect configurations.	
Examples	**1-to-1 NAT with Auto-create Source NAT disabled:** 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 Network topology:  Scenario: 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). 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 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` **1-to-1 NAT with Auto-create Source NAT enabled:** 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: 30.0.0.100
- Device(B) on the external network:
  - IP: 20.0.0.2/24
  - Gateway: 20.0.0.1

Network topology:



Scenario:
a) On the router, the source IP address 20.0.0.2 of the packet originating from Device (B) will be transformed to 30.0.0.2 before being transmitted to Device (A).
b) 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).

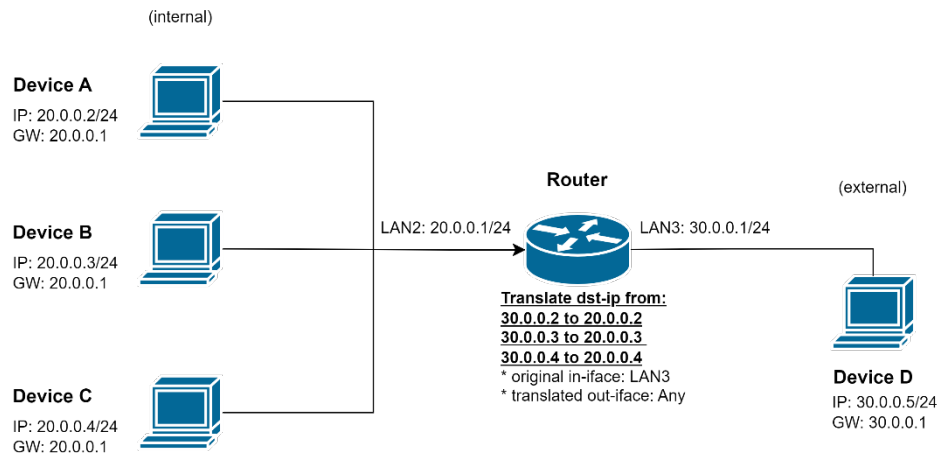
Commands:

```
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 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_wSNAT
router(config-nat)# source-nat
router(config-nat)# exit
```

1-to-1 NAT with range setting and Auto-create Source NAT enabled:

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: 20.0.0.2/24
  - Gateway: 20.0.0.1
- Device(B) on the internal network:
  - IP: 20.0.0.3/24
  - Gateway: 20.0.0.1
- Device(C) on the internal network:
  - IP: 20.0.0.4/24
  - Gateway: 20.0.0.1
- Device(D) on the external network:
  - IP: 30.0.0.5/24
  - Gateway: 30.0.0.1

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:

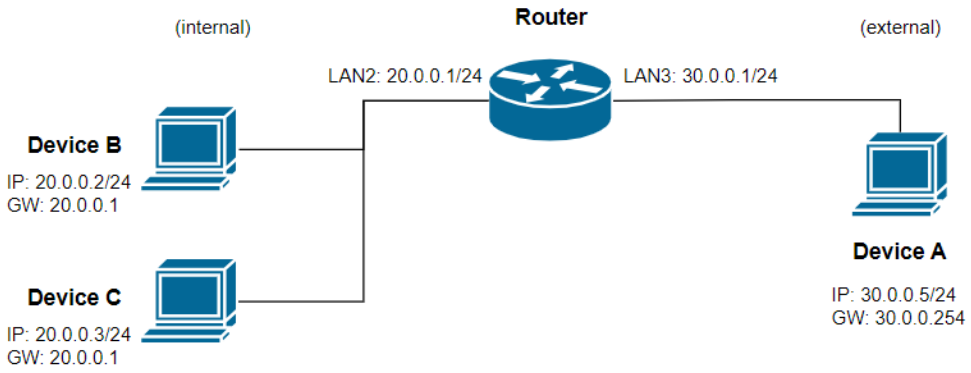
```
router# configure
router(config)# ip nat
router(config-nat)# mode 1-1
router(config-nat)# original in-iface LAN3 src-ip any src-port any
dst-ip 30.0.0.2-30.0.0.4 dst-port any
router(config-nat)# translated out-iface any src-ip any src-port any
dst-ip 20.0.0.2-20.0.0.4 dst-port any
router(config-nat)# 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:

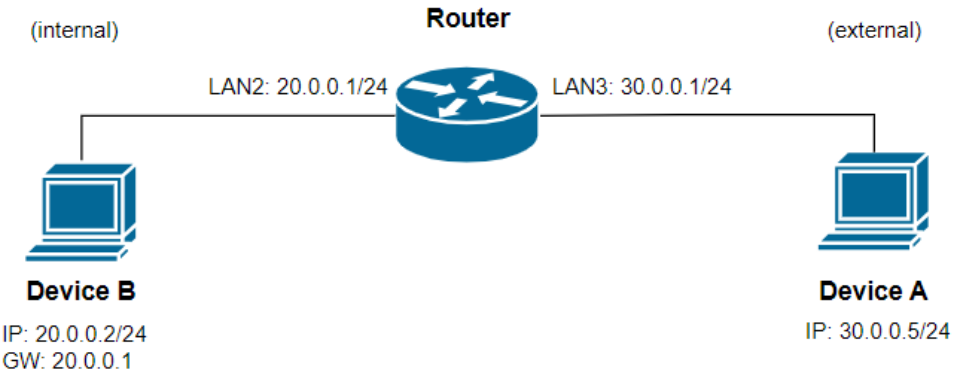
```
router# configure
router(config)# ip nat
router(config-nat)# mode n-1
router(config-nat)# original in-iface any src-ip 20.0.0.2-20.0.0.4
src-port any dst-ip any dst-port any
router(config-nat)# translated out-iface LAN3 src-ip any src-port any
dst-ip any dst-port any
router(config-nat)# desc n-1_example
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.

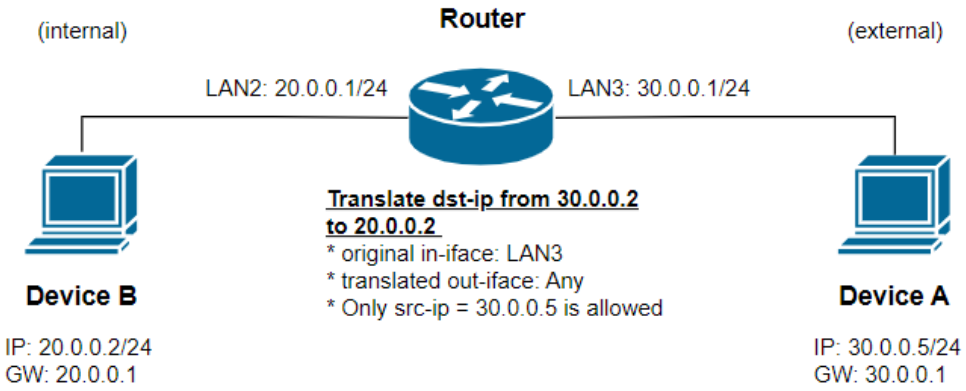
```
Commands:
router# configure
router(config)# ip nat
router(config-nat)# mode pat
router(config-nat)# original in-iface LAN3 src-ip any src-port any
dst-ip any dst-port 2222
router(config-nat)# translated out-iface any src-ip any src-port any
dst-ip 20.0.0.2 dst-port 22
router(config-nat)# protocol 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
```

	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 Apart from the aforementioned command, it is also necessary to manually create a secondary IP address (30.0.0.2) on LAN3: router(config)# interface vlan 3 router(config-vif)# ip address 30.0.0.2 255.255.255.0 secondary router(config-vif)# exit
Error Messages	- Ranged Translated Destination IP (), Original Destination IP () mismatch is forbidden
	% Invalid in-iface Interface Name.
	% Invalid format
	% Invalid Protocol. It must be tcp, udp or select multiple protocol with ",".
	% is over length. It must be 1 - 128.
	% is not a valid mode.
	^Parse error
	^Incomplete command
Related Commands	no ip nat show ip nat settingcheck

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>

Option Description	nat-index	Index of existing NAT rule
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Delete an existing NAT rule: Prerequisites: • TN router: - There exists 4 NAT rules before deletion. Scenario: The 3rd NAT rule is outdated and needs to be removed. Commands: router# configure router(config)# no ip nat 3 router(config)# exit	
Error Messages	% Invalid Index. It must be 1 - .	
	^Parse error	
	^Incomplete command	
Related Commands	ip nat show ip nat	

show ip nat

To check the NAT settings on the router, use the **show ip nat** command.

Synopsis

show ip nat

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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 : -- ----------	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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>
(config-obj-addr)# **no name**

Remove object of IP address and subnet type
(config)# **no object** <name>

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**

Option Description	name	Specifies the object's name
	name	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• No modification function is provided. In case modification is required, remove it first and then add a new object. • Exits the sub-level configuration mode to let settings take effect. • "uuid" option in this command is reserved for Moxa use only.	
Examples	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`	
Error Messages	% 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	

Related Commands	show object

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>
(config-obj-serv)# **no name**

Remove object of user-defined service type
(config)# **no object** <name>

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>
(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**

Option Description		
	tcp	Specifies TCP protocol
	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	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• No modification function is provided. In case modification is required, remove it first and then add a new object. • Exits the sub-level configuration mode to let settings take effect.	
Examples	Create an object of user-defined service type for Layer 3-7 policy: `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`	
Error Messages	% 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	
Related Commands	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>
(config-obj-net-serv)# **no name**

Remove object of network service type
(config)# no object <name>

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**

Option Description	name	Specifies the object's name
	name	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: 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 ├ Simple FTP TCP 115; UDP 115 ├ Secure-FTP TCP 22 ├ 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 └ SYSLOG-TCP TCP 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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• No modification function is provided. In case modification is required, remove it first and then add a new object. • Exits the sub-level configuration mode to let settings take effect.	
Examples	Create an object of Network-Service type for Layer 3-7 policy: `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`	
Error Messages	% 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	
Related Commands	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>
(config-obj-indust-app)# **no name**

Remove object of industrial application service type
(config-obj-indust-app)# **no object** <name>

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**

Option Description	name	Specifies the object's name
	name	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: 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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• No modification function is provided. In case modification is required, remove it first and then add a new object. • Exits the sub-level configuration mode to let settings take effect.	
Examples	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`	
Error Messages	% 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
Related Commands	show object

show object

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

Synopsis

show object

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	object address object service object network-service object industrial-application-service	

IP object group

To create an address object group.

Synopsis

Create a new object group of address and enter the sub-level mode

(config)# **object group address**

(config-obj-grp-addr)#

Set an object group name

(config-obj-grp-addr)# **name** <name>

List object names can be selected

(config-obj-grp-addr)# **select list**

Select an object name

(config-obj-grp-addr)# **select** <STRING:obj_name>

Remove the selected object name

(config-obj-grp-addr)# **no selec**t <STRING:obj_name>

Show all selected object name

(config-obj-grp-addr)# **show**

Quit the object configuration without saving

(config-obj-grp-addr)# **abort**

Save and exit the object configuration

(config-obj-grp-addr)# **exit**

Option Description	object	Object setting
	group	Object address setting
	address	IP address setting
	name	Object Name
	no	Remove
	select	Select Defined Object Name(s)
	show	Show Selected Objects.
	abort	Quit without Saving
	exit	Save and Quit
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# object group address router(config-obj-grp-addr)# name test_grp router(config-obj-grp-addr)# select list Name Detail --- obj1 1.1.1.1 obj2 2.2.2.2-3.3.3.3 router(config-obj-grp-addr)# select obj1 router(config-obj-grp-addr)# show Name Detail --- test_grp obj1 router(config-obj-grp-addr)# exit	
Error Messages	^Parse error	
	^Incomplete command	
	% No object named X was found.	
	% Incorrect Object Type.	
	% Please at least select one object.	
Related Commands	show object groups address	

Service object group

To create an object service group.

Synopsis

Create a new object group of address and enter the sub-level mode

(config)# **object group service**

(config-obj-grp-serv)#

Set an object group name

(config-obj-grp-serv)# **name** <name>

List object names can be selected

(config-obj-grp-serv)# **select list**

Select an object name

(config-obj-grp-serv)# **select** <STRING:obj_name>

Remove the selected object name

(config-obj-grp-serv)# **no select** <STRING:obj_name>

Show all selected object name

(config-obj-grp-serv)# **show**

Quit the object configuration without saving

(config-obj-grp-serv)# **abort**

Save and exit the object configuration

(config-obj-grp-serv)# **exit**

Option Description	object	Object setting
	group	Object address setting
	service	User-define service setting
	name	Object Name
	no	Remove
	select	Select Defined Object Name(s)
	show	Show Selected Objects.
	abort	Quit without Saving
	exit	Save and Quit
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# object group service router(config-obj-grp-serv)# name test_grp router(config-obj-grp-serv)# select list Name Detail --- udp1 UDP 555 tcp1 UDP 3000-4000 router(config-obj-grp-serv)# select udp1 router(config-obj-grp-serv)# show Name Detail --- test_grp udp1	

	router(config-obj-grp-serv)# exit
Error Messages	^Parse error
	^Incomplete command
	% No object named X was found.
	% Incorrect Object Type.
	% Please at least select one object.
Related Commands	show object groups service

Interface group

To create an interface group or add an interface to an interface group already existed.

Synopsis

Bind/Unbind LAN interface to an interface group

(config)# **interface lan**

(config-if)# **interface-group** <STRING:name>

(config-if)# **no interface-group** <STRING:name>

Bind/Unbind vlan interface to an interface group

(config)# **interface vlan** <UINT:vlanid>

(config-vif)# **interface-group** <STRING:name>

(config-vif)# **no interface-group** <STRING:name>

Bind/Unbind wan interface to an interface group

(config)# **interface wan** <UINT:wanid>

(config-if)# **interface-group** <STRING:name>

(config-if)# **no interface-group** <STRING:name>

Bind/Unbind port bridge interface to an interface group

(config)# **interface bridge**

(config-brg)# **interface-group** <STRING:name>

(config-brg)# **no interface-group** <STRING:name>

Bind/Unbind zone bridge interface to an interface group

(config)# **interface zone-base-bridge**

(config-brg)# **interface-group** <STRING:name>

(config-brg)# **no interface-group** <STRING:name>

Bind/Unbind bridge port to an interface group

(config)# **interface ethernet** <STRING:mod_port>

(config-if)# **interface-group** <STRING:name>

(config-if)# **no interface-group** <STRING:name>

Bind/Unbind bridge zone to an interface group

(config)# **interface vlan** <UINT:vlanid> **zone-base-bridge interface-group** <STRING:name>

(config)# **no interface vlan** <UINT:vlanid> **zone-base-bridge interface-group** <STRING:name>

Option Description	interface-group	Interface group
	name	Object name
	no	Remove
Defaults	N/A	

Command Modes	Sub-level configuration
Usage Guidelines	N/A
Examples	`router# configure` `router(config)# interface ethernet 1/4` `router(config-if)# interface-group ifsBrgGroup` `router(config-if)# exit` `router(config)# interface lan` `router(config-if)# no interface-group ifsLanGroup` `router(config-if)# exit` `router(config)# interface vlan` `router(config-if)# no interface-group ifsLanGroup` `router(config-if)# exit`
Error Messages	^Parse error
	^Incomplete command
	% Port X cannot be added to interface group since it is not a bridge member.
	% X is an invalid system symbol.
	% X is over length. It must be 1 - 32.
	% Interface Group member is full!
	% This Object Group type is not for Interface Member!
	% This Object Group type is not for Port Bridge Member!
	% This Object Group type is not for Zone Bridge Member!
	% Bind interface to vlan before setting interface group!
	% Interface Group X does not exist!
Related Commands	show interfaces group

Show group

To show group members, use this command.

Synopsis

show object groups address

Option Description	show	Show System Information
	object	Show All User-defined Objects
	groups	Show Object Groups
	address	Show Address Object Groups
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# show object groups address Name Detail --- ipGroupA ip1, ip2	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	object group address	

show object groups service

Option Description	show	Show System Information
	object	Show All User-defined Objects
	groups	Show Object Groups
	service	Show Service Object Groups
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# show object groups service Name Detail --- groupA icmpAll, udpObj1, udpObj2 icmpA icmpAll	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	object group service	

show interfaces group

Option Description	show	Show System Information
	interfaces	Interface status and configuration
	group	Show Interface Group
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# show interfaces group Name Type Detail ---	

	bridgePort: Port Bridge Member 1/3, 1/4 ifsGroup: Interface Member LAN, lan2	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	interface-group	

Firewall

Layer 2 Policy

l2-policy

To create a firewall layer 2 policy rule, use the **l2-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)# **l2-policy** <l2-index>
(config)# **no l2-policy** <l2-index>

Enable / Disable Layer 2 policy.
(config)# **l2-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**

Option Description	no	Remove or set to default
	l2-policy	Configure Layer 2 Policy
	l2-index	One of the following: 1. Index of existing **Layer 2 policy**: New **Layer 2 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.
	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
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• No modification function is provided. In case modification on a specific index is required, remove it first and then add a new policy. • Command # **protocol manual** is required when configuring a specific ether-type. • Types a valid index to enter sub-level configuration mode. • Exits the sub-level configuration mode to let settings take effect. • Network interfaces related to this firewall feature must be created in advance. • Layer 2 policy priority is higher than the Layer 3 policy. • Trap only works when logging is enabled, SNMP is enabled and SNMP trap is well configured.	
Examples	Drop ARP packets from a port-based bridge interface member port PORT7 to PORT8:	

	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
Error Messages	% 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
	^Parse error
	^Incomplete command
Related Commands	show l2-policy show logging event-log 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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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 : <4> Warning Local Storage: Disable Syslog Server: Disable Trap Server : Disable	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	l2-policy show logging event-log l2-policy show logging event-log l2-policy severity <range>	

Layer 3 - 7 Policy

l3l7-policy

To create a Layer 3-7 firewall policy, use the **l3l7-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)# **l3l7-policy** [<firewall-index>]
(config)# **no l3l7-policy** <firewall-index>

Enable / Disable Layer 3-7 policy globally or set default action.
(config)# **l3l7-policy** {**enable** |
disable |
default-action {**allow** | **deny**}}

Set Layer 3-7 policy enabled / disabled in sub-level configuration mode
(config-l3l7-policy)# **enable**
(config-l3l7-policy)# **no enable**

Set / Clear Layer 3-7 policy name in sub-level configuration mode
(config-l3l7-policy)# **name** <name>
(config-l3l7-policy)# **no name**

Set / Clear Layer 3-7 policy description in sub-level configuration mode
(config-l3l7-policy)# **description** <desc>
(config-l3l7-policy)# **no description**

Set Layer 3-7 policy logging enabled / disabled in sub-level configuration mode
(config-l3l7-policy)# **logging**
(config-l3l7-policy)# **no logging**

Set / Clear Layer 3-7 policy logging in sub-level configuration mode (for multiple logging destinations, use different arguments separately)
(config-l3l7-policy)# **logging** {**severity** <severity-level>|
flash |
syslog |
trap}
(config-l3l7-policy)# **no logging** {**flash** |
syslog |
trap}

Set / Clear Layer 3-7 policy interface in sub-level configuration mode
(config-l3l7-policy)# **interface** <if-from> <if-to>
(config-l3l7-policy)# **no interface**

Set Layer 3-7 policy mode in sub-level configuration mode
(config-l3l7-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-por**t

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	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• No modification function is provided. In case modification on a specific index is required, remove it first and then add a new policy. • Types a valid index to enter sub-level configuration mode. • Exits the sub-level configuration mode to let settings take effect. • Network interfaces related to this firewall feature must be created in advance. • Layer 2 policy priority is higher than the Layer 3 policy. • Create network(service) object(s) in advance so that those object(s) can be used on this firewall policy. • Configure SNMP Trap in advance when sending event logs via SNMP trap. • Configure Syslog server in advance when sending event logs to syslog server. • "uuid" option in this command is reserved for Moxa use only.	
Examples	• Drop all packets from interface LAN10 to LAN20: • `router# configure` • `router(config)# l3l7-policy 1` • `router(config-l3l7-policy)# name dropLAN10` • `router(config-l3l7-policy)# no logging` • `router(config-l3l7-policy)# logging severity 4` • `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 LAN10 LAN20` • `router(config-l3l7-policy)# action deny` • `router(config-l3l7-policy)# mode ip` • `router(config-l3l7-policy)# enable` • `router(config-l3l7-policy)# exit` • Delete L3-7 policy index 1: • `router# configure` • `router(config)# no l3l7-policy 1` • `router(config)# exit` • Allow all packets from the end device (using pre-defined object "ED1" in this example) to LAN20: • `router# configure` • `router(config)# l3l7-policy 2`	

	• router(config-l3l7-policy)# name Allow-ED1 • router(config-l3l7-policy)# no logging • router(config-l3l7-policy)# logging severity 4 • 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 •
Error Messages	% 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
Related Commands	show l3l7-policy show logging event-log l3l7-policy snmp-server host snmp-server trap-mode logging <ip-addr> settingcheck

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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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
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
------------------------------------------------------------------------
```

Error Messages	^Parse error
	^Incomplete command
Related Commands	l3l7-policy
	show logging event-log l3l7-policy

l3l7-policy Global Settings

To create a Layer 3-7 firewall policy, use the l3l7-policy global configuration command and corresponding sub-level configuration mode commands. To remove the firewall policy, use the no form of this command.

Synopsis

Enable / Disable default action log

(config)# **l3l7-policy default-log**

(config)# **no l3l7-policy default-log**

Set / Clear default action log severity or destination

(config)# **l3l7-policy default-log** { severity <severity-level> flash | syslog | trap }

(config)# **no l3l7-policy default-log** { flash | syslog | trap }

Option Description	default-log	Redundancy configuration
Defaults	L3-L7 Policy is disabled. L3-L7 Policy log is enabled. L3-L7 Policy default action is to deny all. L3-L7 Policy default action log is disabled. L3-L7 Policy default action log severity is Warning. L3-L7 Policy default action log destination is none.	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`Enable Default Action Log` `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# l3l7-policy default-log` `Set Default Action Log Severity to Critical` `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# l3l7-policy default-log severity 2` `Set Default Action Log Severity to Flash` `Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# l3l7-policy default-log flash`	
Error Messages	N/A	
Related Commands	show l3l7-policy show logging event-log l3l7-policy snmp-server host snmp-server trap-mode logging <ip-addr> settingcheck	

To configure more details of the L3L7 Policy, user need to enter the submode of the L3L7 Policy for a specific entry by specifying an index. If no index is entered, the system will assign the default index value of 1.

Synopsis

Create and Insert / Remove specific L3L7 Policy rule

(config)# **l3l7-policy** { <index> }

(config)# **no l3l7-policy** <index>

Option Description	l3l7-policy	L3L7 Policy (Append New Policy)
	index	Insert a new policy on the specified index
Defaults	Default Index: 1	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Create and insert a L3L7 policy rule to the location of index 1 in L3L7 Policy Table. Firewall/VPN Router 00000# configure Firewall/VPN Router 00000(config)# l3l7-policy 1 Remove the second L3L7 policy rule from current L3L7 Policy Table Firewall/VPN Router 00000# configure Firewall/VPN Router 00000(config)# no l3l7-policy 2	
Error Messages	N/A	
Related Commands	show l3l7-policy	

To meet the requirements of IEC 61162-460 [10.8.4], control the lifetime of the firewall to manage the usage time of the connection. (10.8.4, IEC 61162-460)

Synopsis

Enable / Disable monitoring to lifetime

(config-l3l7-policy)# **lifetime** <lifetime_sec>

(config-l3l7-policy)# **no lifetime**

Option Description	lifetime	The maximal lifetime for the continuous working period of a rule
	<lifetime_sec>	Configure lifetime in seconds: 0 to 14400, 0 means infinite
Defaults	0	
Command Modes	Sub-level Configuration	
Usage Guidelines	N/A	
Examples	Set lifetime of 4 hours to the rule. Firewall/VPN Router 00000 (config)# l3l7-policy 1 Firewall/VPN Router 00000(l3l7-policy)# lifetime 14400 Disable lifetime to the rule Firewall/VPN Router 00000 (config)# l3l7-policy 1 Firewall/VPN Router 00000(l3l7-policy)# no lifetime	
Error Messages	% The lifetime can be set within the range of 0 to 14400 seconds, where 0 represents an infinite period.	
Related Commands	show l3l7-policy	

To meet the requirements of IEC 61162-460 [10.8.4], the ability for user to manually extend remaining lifetime is provided on a per policy rule basis. (10.8.4, IEC 61162-460)

Synopsis

Extending remaining lifetime to the configuration of lifetime

(config-l3l7-policy)# **extend**

Option Description	extend	Reset the remaining lifetime to the configured lifetime value
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	N/A	
Examples	`Reset the remaining lifetime to the configured lifetime value.` `Firewall/VPN Router 00000 (config)# l3l7-policy 1` `Firewall/VPN Router 00000(l3l7-policy)# extend`	
Error Messages	% Cannot take effect because the lifetime has not started yet.	
Related Commands	show l3l7-policy	

To meet the requirements of IEC 61162-460 [10.8.4], control the idle time of the firewall to manage the usage time of the connection. (10.8.4, IEC 61162-460)

Synopsis

Enable / Disable monitoring to idle time

(config-l3l7-policy)# **idle** <idle_sec>

(config-l3l7-policy)# **no idle**

Option Description	Idle	The maximal idle time for the current working rule
	<idle_sec>	Configure idle time in seconds: 0 to 600, 0 means infinite
Defaults	0	
Command Modes	Sub-level Configuration	
Usage Guidelines	N/A	
Examples	`Set idle time of 10 minutes to the rule.` `Firewall/VPN Router 00000 (config)# l3l7-policy 1` `Firewall/VPN Router 00000(l3l7-policy)# idle 600` `Disable idle time to the rule` `Firewall/VPN Router 00000 (config)# l3l7-policy 1` `Firewall/VPN Router 00000(l3l7-policy)# no idle`	
Error Messages	% The lifetime can be set within the range of 0 to 14400 seconds, where 0 represents an infinite period.	
Related Commands	show l3l7-policy	

Firewall -L3 Policy



NOTE

The commands in this section are only used for the NAT Series devices.

show firewall

To show the firewall information for L3 filter policy, use **show firewall** command.

Synopsis

show firewall

Option Description	show	Display information
	firewall	Firewall information
Defaults	0	
Command Modes	Privileged EXEC/User EXEC	
Usage Guidelines	N/A	
Examples	router# show firewall Global Setting Status : Enabled //Reserved item Default Action : Accept //Reserved item Log : Disabled Policy Setting Index :1 State :Enable Action :ACCEPT Interface :from any to any Protocol :All Mode :IP Address Filter Src IP :ALL Src Port :ALL Dst IP :ALL Dst Port :ALL Severity :<0> Emergency Flash :Disable Syslog :Disable Trap :Disable ---------- Index :2 State :Enable Action :ACCEPT Interface :from any to any Protocol :All Mode :IP Address Filter Src IP :ALL Src Port :ALL Dst IP :ALL Dst Port :ALL Severity :<0> Emergency Flash :Disable Syslog :Disable Trap :Disable ----------	

Error Messages	^Parse error
Related Commands	firewall <UINT:index> no firewall <UINT:index> firewall <UINT:index> enable firewall <UINT:index> disable

firewall

To create a Layer 3 filter policy, use the firewall configuration command and corresponding sub-level configuration mode commands. To remove the firewall policy, use no form of this command.

Synopsis

Enable/Disable Firewall Layer 3 Policy

(config)# **firewall** <UINT:index>

(config)# **no firewall** <UINT:index>

Delete Firewall Layer 3 Policy

(config)# **no firewall** <UINT:index>

Add Firewall Layer 3 Policy

(config)# **firewall** <UINT:index>

Set Policy Action

(config-firewall)# **action** {accept | drop }

Set Policy Filter Mode

(config-firewall)# **mode** {ip | mac}

Set Policy Filter Protocol

(config-firewall)# **protocol** {all | tcp | udp | icmp }

Set Policy Source IP Address

(config-firewall)# **src-ip** {all | single | range}

Set Policy Destination IP Address

(config-firewall)# **dst-ip** {all | single | range}

Set Policy Source Port

(config-firewall)# **src-port** {all | single | range}

Set Policy Destination Port

(config-firewall)# **dst-port** {all | single | range}

Set Policy Source MAC Address

(config-firewall)# **src-mac** {MACADDR:macaddr}

Set Policy Interface

(config-firewall)# **interface** {STRING:if_from} {STRING:if_to}

Set Firewall Policy Log for Rule

(config-firewall)# **logging** {severity | flash | syslog | trap}

Disable Firewall Policy Log for Rule

(config-firewall)# **no** {logging}

Name a Firewall Rule

(config-firewall)# **name** {STRING:name}

Exit Policy Configuration Mode

(config-firewall)# **exit**

Option Description	firewall	Configure Layer 3 filter policy
	firewall <index>	Could be one of the cases below: Index of existing Layer 3 filter policy: New Layer 3 Policy will be created at this position and original index after this value will be incremented by 1. A new index: New index value should be the last existing index value plus 1
	no firewall <index>	Delete Layer 3 filter policy
	firewall <index> enable	Set Policy Enable
	firewall <index> disable	Set Policy Disable
	action	Set Policy Action
	mode	Set Policy Filter Mode
	protocol	Set Policy Filter Protocol Use one of the below options: {all | tcp | udp | icmp | list}
	src-ip	Set Policy Source IP Address, default all {all | single | range} src-ip single <IPV4ADDR:ipaddr> src-ip range <IPV4ADDR:ipaddr1> <IPV4ADDR:ipaddr2>
	dst-ip	Set Policy Destination IP Address, default all {all | single | range} dst-ip single <IPV4ADDR:ipaddr> dst-ip range <IPV4ADDR:ipaddr1> <IPV4ADDR:ipaddr2>
	src-port	Set Policy Source Port
	dst-port	Set Policy Destination Port

	src-mac	Set Policy Source MAC Address
	interface	Set Policy Interface
	logging	Set firewall policy log for rule
	no	Disable firewall policy log for rule
	name	Naming a firewall rule.
	exit	Exit Policy Configuration Mode
Defaults	N/A	
Command Modes	Global Configuration/Sub-level Configuration	
Usage Guidelines	• No modification function is provided for layer 3 filter policy. It only supports insert method. In case modification on a specific index is required, remove it first and then add a new policy. • Types a valid index to enter sub-level configuration mode. It is start from 1 to N+1. The number N is current maximum number of rules. • Exits the sub-level configuration mode to let settings take effect. • Network interfaces related to this firewall feature must be created in advance. • Trap only work when logging is enable, SNMP is enabled and SNMP trap is well configured.	
Examples	Drop TCP packets from interface LAN to WAN: 86151# configure 86151(config)# firewall 1 86151(config-firewall)# action drop 86151(config-firewall)# mode ip 86151(config-firewall)# protocol tcp 86151(config-firewall)# interface lan wan 86151(config-firewall)# name test_item 86151(config-firewall)# exit 86151(config)# exit	
Error Messages	% Invalid Index. It must be 1 - N.	
	% firewall list is empty.	
	% Invalid Protocol. It must be invalid protocol.	
	% Invalid Input Interface Name	
	% Invalid Output Interface Name.	
	% Severity level is out of range!	
	^Parse error	
	^Incomplete command	
Related Commands	show firewall show logging event-log l3-policy show logging event-log l3-policy severity <range> show security-notification setting show security-notification status security-notification event-l3policy logging firewall no logging firewall clear logging event-log l3-policy	

logging-firewall

To enable Layer 3 filter policy firewall log. To disable the firewall log, use **no** form of this command.

Synopsis

Enable/Disable firewall log

(config)# **logging firewall**

(config)# **no logging firewall**

security-notification event-l3policy

To enable Layer 3 filter policy security notification. To disable the security notification, use **no** form of this command.

Synopsis

Enable/Disable security-notification event-l3policy

(config)# **security-notification event-l3policy**

(config)# **no security-notification event-l3policy**

show security-notification setting & status

Use the show security-notification EXEC command to display the Security Notification Configuration

Synopsis

(config)# **show security-notification setting**

(config)# **show security-notification status**

show logging event-log l3-policy

show Layer 3 Policy event log

Synopsis

(config)# **show logging event-log**

(config)# **show logging event-log l3-policy severity** <STRING:range>

Clear logging event-log l3-policy

Clear Layer 3 Filter Policy Event Logs

Synopsis

(config)# clear logging event-log l3-policy

l3-policy-event active

To turn on/off the Layer 3 event trigger, use this command.

Synopsis

(config)# **warning-notification firewall-event l3-policy-event active**

(config)# **no warning-notification firewall-event l3-policy-event active**

Option Description	warning-notification	Warning notification
	firewall-event	Firewall event setting
	l3-policy-event	Layer 3 Deny Policy Event setting
	active	Activate
Defaults	Disabled	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification firewall-event l3-policy-event active`	

	`router(config)# no warning-notification firewall-event l3-policy-event active`
Error Messages	^Parse error
Related Commands	N/A

l3-policy-event action

To set the Layer 3 event trigger action, use this command.

Synopsis

(config)# **warning-notification firewall-event l3-policy-event action** <UINT:combination>

Option Description	warning-notification	Warning notification
	firewall-event	Firewall event setting
	l3-policy-event	Layer 3 Deny Policy Event setting
	action	Enable Action setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification firewall-event l3-policy-event action 8` `router(config)# warning-notification firewall-event l3-policy-event action 0`	
Error Messages	^Parse error	
	% Invalid action value or non-support this combination action	
Related Commands	N/A	

Device Lockdown

> **NOTE**
>
> The commands in this section are only used for the NAT Series devices.

Device Lockdown is a firewall allowlist.

Use the Device lockdown EXEC command to set configuration and configure manual entries for device lockdown. To disable device-lockdown, use **no** form of this command. For more details, refer to the commands below.

Synopsis

Enable/Disable Device Lockdown

(config)# **device-lockdown**

(config)# **no device-lockdown**

Set Device Lockdown learning period

(config)# **device-lockdown {learning {period {30-86400} | start | stop}**

Set Device Lockdown mode

(config)# **device-lockdown {mode {mac | macip}}**

Enable/Disable Device Lockdown Auto Learning on Boot

(config)# **device-lockdown {onboot}**

(config)# **no device-lockdown {onboot}**

Set Device Lockdown Interface to Learn and Lockdown

(config)# **device-lockdown {interface {LAN | LAN2 | WAN| other interface in system}}**

Add Manual Device Lockdown Entry

(config)# **device-lockdown manual {src-ip} {src-mac} {interface} {action {accept | drop}} {description { "" | max length 128}}**

Modify Manual Device Lockdown Entry

(config)# **device-lockdown manual {src-ip} {src-mac} {interface} {action {accept | drop}} {description { "" | max length 128}} {index}**

Delete Manual Device Lockdown Entry

(config)# **no device-lockdown manual {index | src-mac}**

Option Description	learning	Configure Device Lockdown Auto Learning
	period	Set Device Lockdown learning period on boot up. Learning Time (second) between 30-86400
	start	Start device lockdown device learning
	stop	Stop device lockdown device learning
	mode	Address to lockdown
	mac	MAC address
	macip	MAC address and IP address
	onboot	Enable device lockdown auto learning on boot
	interface	Interface to learn and lockdown
	manual	Add manual device lockdown device
	src-ip	Specify source IP address for device
	src-mac	Specify source MAC for device
	interface	Specify connected L3 interface for device
	action	How to deal with traffic from device when lockdown

	description	Description of specified lockdown entry. Maximum length is 128. Whitespaces not allowed. To leave description unchanged when modifying an entry, specify "".
	index	The index of the lockdown entry
Defaults	Disabled	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	Maximum number of entry is 50 (including 1 default entry)	
Examples	Manually add/modify/delete a rule for device lockdown entry: Add entry: router(config)# device-lockdown manual src-ip 192.167.127.11 src-mac aa:bc:00:12:dd:01 interface LAN action accept Entry 2 added Modify entry: router(config)# device-lockdown manual src-ip 192.167.127.11 src-mac aa:bc:00:12:dd:01 interface LAN action drop description "" index 2 Entry 2 modified Delete entry by index: router(config)# no device-lockdown manual index 2 Entry 2 removed Delete entry by src-mac: router(config)# no device-lockdown manual src-mac aa:bc:00:12:dd:01 Entry 2 removed	
Error Messages	^Parse error	
	% Invalid parameter!	
	% Illegal learning period (30-86400).	
	% Invalid interface name	
	% Invalid ip address	
	% Entry is existing! MAC address as device unique key	
	% Invalid action	
	% Invalid index	
	% Can not Manually Add/Remove while Learning!	
	% Disable Local Device Lockdown before Manually Add/Remove	
	% Modify failed! Entry is existing, MAC address as device unique key	
	% Device Lockdown entry limit is 49	
Related Commands	show device-lockdown	

show device-lockdown

Use the **Show Device lockdown** EXEC command to display the setting and entries (including auto learned and manual) of device lockdown

Synopsis

show device-lockdown

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	router# show device-lockdown Local Device Lockdown : Disabled Device Lockdown State : Learning Done	

	Device Lockdown Mode : MAC Address Learning / Lockdown Interface : LAN Log : Disabled Log Destination : None Log Level : 4 Auto Learning Duration : 60 Auto Learning on Boot : Disabled ------ Entry 1 : Enable Source : Auto Learned Learned Interface : LAN Source Mac : AC:91:A1:6A:D9:6A Network Access : Allow ------ Default Entry Interface : LAN Source Mac : Any Network Access : Block Description : Lockdown Default Entry ------
Error Messages	^Parse error
Related Commands	N/A

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 the **no** form of this command.

Synopsis

(config)# **firewall malformed** [**logging** {**severity** <severity-level>|
flash |
syslog |
trap}]

(config)# **no firewall malformed** [**logging** {**flash** |
syslog |
trap}]

Option Description	logging	Enables logging function for malformed packets.
	severity	Specifies severity of logging for malformed packet function
	severity-level	Specify an integer as follows: {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
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	• Network interfaces related to this firewall feature must be created in advance. • Configure SNMP Trap in advance when sending event logs via SNMP trap. • Configure Syslog server in advance when sending event logs to syslog server.	
Examples	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`	
Error Messages	% Severity level is out of range!	
	^Parse error	
	^Incomplete command	
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	This command only displays Malformed Packets settings. If you need to check firewall policy settings, please use the command "show l3l7-policy" instead.	
Examples	router # show firewall Global Setting Log Enable:Enable ---------- Malformed Packets Severity :<0> Emergency Flash :Enable Syslog :Enable Trap :Enable ----------	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	firewall malformed show logging event-log malformed	

Advanced Protection Protocol Filter Policy

protocol-filter

To enable/disable the main protocol filter function, use **protocol-filter** command.

Synopsis

(config)# **protocol-filter** { enable | disable }

Option Description	enable	Enable the main protocol filter function
	disable	Disable the main protocol filter function
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Configure to enable main protocol filter function. router# configure router(config)# protocol-filter enable router(config)# exit	
Error Messages	N/A	
Related Commands	show protocol-filter	

protocol-filter action

To enable/disable the main protocol filter action function, use **protocol-filter action** command.

Synopsis

(config)# **protocol-filter action** { accept | monitor | reset }

Option Description	accept	Set to accept action to main protocol filter function
	monitor	Set to monitor action main protocol filter function
	reset	Set to reset action main protocol filter function
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Configure to enable main protocol filter function action monitor. router# configure router(config)# protocol-filter action monitor router(config)# exit	
Error Messages	N/A	
Related Commands	show protocol-filter	

protocol-filter modbus

To enable/disable the Modbus protocol filter function, use **protocol-filter modbus** command.

Synopsis

(config)# **protocol-filter modbus** { enable | disable }

Option Description	enable	Enable the Modbus protocol filter function
	disable	Disable the Modbus protocol filter function
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`Configure to enable the function of the Modbus protocol filter.` `router# configure` `router(config)# protocol-filter modbus enable` `router(config)# exit`	
Error Messages	N/A	
Related Commands	show protocol-filter	

protocol-filter modbus adp

To enable/disable the ADP function of the Modbus protocol filter, use the **protocol-filter modbus adp** command.

Synopsis

(config)# **protocol-filter modbus adp** { enable | disable }

Option Description	enable	Enable the ADP function of the Modbus protocol filter
	disable	Disable the ADP function of the Modbus protocol filter
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`Configure to enable the ADP function of the Modbus protocol filter.` `router# configure` `router(config)# protocol-filter modbus adp enable` `router(config)# exit`	
Error Messages	N/A	
Related Commands	show protocol-filter	

protocol-filter modbus service-port

To enable/disable the ADP function of the Modbus protocol filter, use **protocol-filter modbus service-port** command.

Synopsis

(config)# **protocol-filter modbus service-port** <port>

Option Description	port	Configure service port number(s) of the Modbus protocol filter. The range is 1 to 65535, including comma (,).
Defaults	502	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`Configure the service port numbers of the Modbus protocol filter.` `router# configure` `router(config)# protocol-filter modbus service-port 502,505` `router(config)# exit`	
Error Messages	N/A	
Related Commands	show protocol-filter	

protocol-filter trdp

To enable/disable the TRDP function of the protocol filter, use **protocol-filter trdp** command.

Synopsis

(config)# **protocol-filter trdp** { enable | disable }

Option Description	enable	Enable the TRDP function of the protocol filter
	disable	Disable the TRDP function of the protocol filter
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`Configure to enable the TRDP function of the Modbus protocol filter.` `router# configure` `router(config)# protocol-filter modbus trdp enable` `router(config)# exit`	
Error Messages	N/A	
Related Commands	show protocol-filter	

protocol-filter trdp service-port

To enable/disable the TRDP function of the protocol filter, use the **protocol-filter trdp service-port** command.

Synopsis

(config)# **protocol-filter trdp service-port** <port>

Option Description	port	Configure service port number(s) of the TRDP protocol filter. The range is 1 to 65535, including comma (,).
Defaults	17224, 17225	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Configure the service port numbers of the TRDP protocol filter. router# configure router(config)# protocol-filter trdp service-port 17224,17225 router(config)# exit	
Error Messages	% Invalid Index. It must be 1-65535.	
Related Commands	show protocol-filter	

show protocol-filter

To show the protocol filter global information, use the **show protocol-filter** command.

Synopsis

show protocol-filter

Option Description	N/A
Defaults	N/A
Command Modes	Global Configuration
Usage Guidelines	N/A
Examples	Show information of protocol filter global settings. router# show protocol-filter Global Status: Enable Default Action: Reset Modbus/TCP Firewall Status: Enable Modbus/TCP ADP Status: Enable Modbus/TCP Service Port: 502 TRDP Firewall Status: Enable TRDP Service Port: 17224, 17225
Error Messages	N/A
Related Commands	show protocol-filter

object industrial-protocol-dpi modbus

To set up the object of Modbus protocol filter, see the following examples.

Synopsis

Create a new object of protocol filter and enter the sub-level mode

(config)# **object industrial-protocol-dpi modbus**

(config-obj-dpi-modbus)#

Setting an Object Name

(config-obj-dpi-modbus)# **name** <name>

Setting a Slave ID (optional)

(config-obj-dpi-modbus)# **slave-id** <index>

Selecting an object Profile

(config-obj-dpi-modbus)# **protocol-filter-profile** { list | <profile-number> }

Setting Function Code(s) of Manual-type Protocol Filters

(config-obj-dpi-modbus)# **function-code** <code>

Setting the Enable/Disabled Status of PLC Address Base 1 On Function Codes 1-6, 15, 16, or 23

(config-obj-dpi-modbus)# **plc-addr-base1** { enable | disable }

Setting Filter Type On Function Codes 1-6, 15, 16, or 23

(config-obj-dpi-modbus)# **filter-type** { none | addr-range <start-addr> <end-addr> }

Setting Data Value Filter Type and Parameters on Function Code 1,2,5, or 15

(config-obj-dpi-modbus)# **filter-type data-value** <addr> <val>

Setting Data Value Filter Type and Parameters on Function Code 3,4,6,16, or 23

(config-obj-dpi-modbus)# **filter-type data-value range** <start-addr> <end-addr> <start-val> <end-val>

Setting Operation Control on Function Code 23

(config-obj-dpi-modbus)# **op-control** { read-only | write-only | read-write }

Setting File Number on Function Code 20 or 21 (optional)

(config-obj-dpi-modbus)# **file-number** <file-number>

Setting And-Mask on Function Code 22 (optional)

(config-obj-dpi-modbus)# **and-mask** <mask>

Setting Or-Mask on Function Code on 22 (optional)

(config-obj-dpi-modbus)# **or-mask** <mask>

Setting MEI Type on Function Code 43

(config-obj-dpi-modbus)# **mei-type** { any | 13 | 14 }

Showing Edited Object Parameters and Information

(config-obj-dpi-modbus)# **show**

Quitting Object Configuration Without Saving

(config-obj-dpi-modbus)# **abort**

Saving and Exiting Object Configuration

(config-obj-dpi-modbus)# **exit**

Option Description	name	A set of characters without white spaces. Maximum length is 32.
	index	Optionally configure Slave ID. Range: 0-255.
	profile-number	Select pre-defined profile number. Range: 1-4. (User can use "protocol-filter-profile list" to see pre-defined profile numbers.)
	code	Select pre-defined function code(s). Range: 0-255, allows commas (,).
	start-addr	Configure the start address. Range: 0-65535
	end-addr	Configure the end address. Range: 0-65535
	addr	Configure the address. Range: 0-65535
	start-val	Configure the start data value. Range: 0-65535
	end-val	Configure the end data value. Range: 0-65535
	val	Configure the data value. Range: 0-65535
	file-number	Configure a file number. Range: 0-65535
	mask	Configure a mask. Range: 0-65535
	list	List pre-defined profiles for protocol filter profile setting. List pre-defined function codes for function code(s) setting.
Defaults	Filter type is "none". Operation control is "read-only". PLC address base is disabled.	
Command Modes	Global Configuration, Sub-level Configuration	
Usage Guidelines	• No modification function is provided. In case modification is required, remove it first and then add a new object. • Exit the sub-level configuration mode to let settings take effect	
Examples	Configure to set and show a Modbus object. router# configure router(config)# object industrial-protocol-dpi modbus router(config-obj-dpi-modbus)# name test_obj router(config-obj-dpi-modbus)# protocol-filter-profile list 1:Read Only - Function Code are 1-4,7,20,24. 2:Write Only - Function Code are 5,6,15,16,21,22.	

	3:Read/Write - Function Code are 1-7,15,16,20-24. 4:Manual - Manual to Select Function Code. router(config-obj-dpi-modbus)# protocol-filter-profile 3 router(config-obj-dpi-modbus)# show Name : test_obj Slave Id : Profile : 3:Read/Write Function Code : Filter Type : None Operation Control : Read-Only PLC Address Base1 : Disabled File Number : And Mask : Or Mask : MEI Type : Any router(config-obj-dpi-modbus)# exit
Error Messages	% Please enter an object name.
	% Object name <name> is already existed.
	% <name> is not a valid system symbol.
	% <name> is over length. It must be 1-32.
	% Please select a profile type.
	% Invalid parameter!
	% Invalid Index. It must be 0 - 65535.
	% Invalid MEI type.
	% Invalid Index. It must be 0 - 1.
	% Please enter a start address of filter type.
	% Please enter a value of filter type.
	% Please enter an address range and value range of filter type.
Related Commands	show object show object industrial-protocol-dpi

object industrial-protocol-dpi trdp

To set up the object of TRDP protocol filter, see the following examples.

Synopsis

Create a new object of protocol filter and enter the sub-level mode

(config)# **object industrial-protocol-dpi trdp**

(config-obj-dpi-trdp)#

Setting an Object Name

(config-obj-dpi-trdp)# **name** <name>

Selecting a Profile for the Object

(config-obj-dpi-trdp)# **protocol-filter-profile** { list | <profile-number> }

Setting Message Type(s) with Manual Filter Profile Type

(config-obj-dpi-trdp)# **msg-type** <msg-string>

Setting Communication Identifier(s) with Protocol Filter Profile Type on Manual

(config-obj-dpi-trdp)# **com-id** <id-string>

Showing the Edited Object Parameters and Information

(config-obj-dpi-trdp)# **show**

Quitting the Object Configuration without Saving

(config-obj-dpi-trdp)# **abort**

Saving and Exiting Object Configuration

(config-obj-dpi-trdp)# **exit**

Option Description	name	A set of characters without a white space. Maximum length: 32.
	profile-number	Select pre-defined profile number. Range: 1-10. (Users can use "protocol-filter-profile list" to see the pre-defined profile number.)
	msg-type	Select pre-defined message type(s). (User can use "msg-type list" to see the pre-defined message type numbers.)
	com-id	Configure communication identifier(s). Range: 0-4294967295, Allow Comma(,). (User can use "com-id list" to see the pre-defined communication identifier(s).)
	list	List pre-defined profiles for protocol filter profile setting. List pre-defined message types for message type(s) setting. List pre-defined communication identifiers for communication identifier(s) setting.
Defaults	N/A	
Command Modes	Global Configuration, Sub-level Configuration	

Usage Guidelines	• No modification function is provided. In case modification is required, remove it first and then add a new object. • Exit the sub-level configuration mode to let settings take effect
Examples	Configure to set and show a TRDP object. router# configure router(config)# object industrial-protocol-dpi trdp router(config-obj-dpi-trdp)# name test_obj router(config-obj-dpi-trdp)# protocol-filter-profile 10 router(config-obj-dpi-trdp)# msg-type 0x5070 router(config-obj-dpi-trdp)# com-id 1,2,3,5,16,55 router(config-obj-dpi-trdp)# show Name : test_obj Profile : 10. Manual Message Type : 0x5070 Communication Identifier : 1,2,3,5,16,55 router(config-obj-dpi-trdp)# exit
Error Messages	% Please enter an object name.
	% Object name <name> is already existed.
	% <name> is not a valid system symbol.
	% <name> is over length. It must be 1-32.
	% Please select a profile type.
	% Please select a message type.
	% Please select a communication identifier.
	% The message type is not valid, please select message types in list.
	% Invalid Index. It must be 1 - 10.
	% Invalid Index. It must be 0 - 4294967295.
Related Commands	show object show object industrial-protocol-dpi

show object industrial-protocol-dpi

To show information of the industrial protocol DPI objects, use this command.

Synopsis

show object [industrial-protocol-dpi]

Option Description	N/A	
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Show brief information of all objects. router# show object Address/Service Objects Name Detail ---------- Protocol-Filter Objects Name Detail ---------- test1_trdp trdp test_mb modbus Show information of industrial protocol DPI object settings.	

	router# show object industrial-protocol-dpi Object Name : test1_trdp Category : TRDP Profile : 10. Manual Message Type : All Communication Identifier : 131,132,140 -- Object Name : test_mb Category : Modbus Profile : 4. Manual Slave Id : 100 Function Code : 4 PLC Address Base 1 : Enabled Filter Type : Data Value Address Range : 10-100 Value : 1-5
Error Messages	N/A
Related Commands	N/A

show

To show object TRDP configuration details, use this command.

Synopsis

(config-obj-dpi-trdp)# **show**

Option Description	show	Show information
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Show the DPI TRDP information. router(config-obj-dpi-trdp)# show Name : test_obj Profile : 10. Manual Message Type : 0x5070 com-id Type : 2 (Advanced) com-id 1 : 1,2,3 reply-com-id 1 : 4,5,6 com-id 2 : 123 reply-com-id 3 : 456 Reply IP : 10.10.10.10 router(config-obj-dpi-trdp)# exit	
Error Messages	N/A	
Related Commands	N/A	

protocol-filter policy

Set up protocol filter policy.

Synopsis

Create a new policy of protocol filter and enter the sub-level mode

(config)# **protocol-filter policy** <index>

(config-dpi-policy)#

Set a Policy Name

(config-dpi-policy)# **name** <name>

Set Policy Status as Enabled or Disabled

(config-dpi-policy)# **status** { enable | disable }

Set from Interface Policy

(config-dpi-policy)# **from-if** { any | list | <interface> }

Set from Interface Policy

(config-dpi-policy)# **to-if** { any | list | <interface> }

Set Source IP Policy

(config-dpi-policy)# **src-ip** { any | single <start-addr> | range <start-addr> <end-addr> | subnet <strart-addr> <netmask> }

Set Destination IP Policy

(config-dpi-policy)# **dst-ip** { any | single <start-addr> | range <start-addr> <end-addr> | subnet <strart-addr> <netmask> }

Set Protocol Type Policy

(config-dpi-policy)# **protocol** { any | udp | tcp }

Set Protocol Type Policy

(config-dpi-policy)# **cmd-type** { master-query | slave-response }

Set Action Policy

(config-dpi-policy)# **action** { accept | monitor | reset }

Set Application Protocol Policy

(config-dpi-policy)# **app-protocol** { list | <app-proto> }

Show Edited Policy Parameters and Information

(config-dpi-policy)# **show**

Quit Policy Configuration Without Saving

(config-dpi-policy)# **abort**

Save and Exit Policy Configuration

(config-dpi-policy)# **exit**

Option Description	index	Configure policy index number.
	interface	Configure the existed interface to the policy. (User can use "from-if list" or "to-if list" to see the existed interfaces.)
	start-addr	Configure a valid (source) IP address to the policy.
	end-addr	Configure a valid end IP address to the policy.
	netmask	Configure a valid net-mask to the policy.
	app-proto	Configure an existed application protocol to the policy. (User can use "app-proto list" to see the existed application protocols.)
	list	List existed interfaces for to interface or from interface setting. List existed application protocol for application protocol setting.
Defaults	Status is disabled. From interface, to interface, source IP, destination IP and protocol are "any". Command type is "master-query". Action is "accept."	
Command Modes	Global Configuration, Sub-level Configuration	
Usage Guidelines	• No modification function is provided. In case modification is required, remove it first and then add a new object. • Exit the sub-level configuration mode to let settings take effect	
Examples	Configure and show a protocol filter policy. router# configure router(config)# protocol-filter policy 100 router(config-dpi-policy)# name pol100 router(config-dpi-policy)# app-protocol list test_mb trdp_app_pro router(config-dpi-policy)# app-protocol test_mb router(config-dpi-policy)# show Name : plo100 Status : Disable From Interface : Any To Interface : Any Source IP : Any Destination IP : Any Protocol : Any Command Type : Master-Query Application Protocol : test_mb Action : Accept router(config-dpi-policy)# exit	
Error Messages	% Invalid Index. It must be 1 - 200.	
	% <name> is not a valid system symbol.	
	% <name> is over length. It must be 1-32.	

	% Please enter a policy name.
	% Please select an application protocol.
	% <app_proto> is not a valid application protocol.
	% <interface> is not exist.
	^Parse error
	% The end address should equal to or lager than start address.
Related Commands	show protocol-filter policy [<index>}]

no protocol-filter policy

To delete assigned protocol filter policy, use this command.

Synopsis

(config)# **no protocol-filter policy** <index>

Option Description	index	Configure policy index number
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`Delete a protocol filter policy with index 100` `router# configure` `router(config)# no protocol-filter policy 100` `router(config)# exit`	
Error Messages	% Invalid Index. It must be 1 - 200.	
Related Commands	show protocol-filter policy [<index>}]	

protocol-filter-policy-event active

To turn on/off the DPI event trigger, use this command.

Synopsis

(config)# **warning-notification firewall-event protocol-filter-policy-event active**

(config)# **no warning-notification firewall-event protocol-filter-policy-event active**

Option Description	warning-notification	Warning notification
	firewall-event	Firewall event setting
	protocol-filter-policy-event	DPI Reset Policy Event setting
	active	Activate
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification firewall-event protocol-filter-policy-event active` `router(config)# no warning-notification firewall-event protocol-filter-policy-event active`	
Error Messages	^Parse error	
Related Commands	N/A	

protocol-filter-policy-event action

To set the DPI event trigger action, use this command.

Synopsis

(config)# **warning-notification firewall-event protocol-filter-policy-event action** <UINT:combination>

Option Description	warning-notification	Warning notification
	firewall-event	Firewall event setting
	protocol-filter-policy-event	DPI Reset Policy Event setting
	action	Enable Action setting
	<UINT:combination>	Relay1 only(8) None(0)
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification firewall-event protocol-filter-policy-event action 8` `router(config)# warning-notification firewall-event protocol-filter-policy-event action 0`	
Error Messages	^Parse error	
	% Invalid action value or non-support this combination action	
Related Commands	N/A	

intrusion-prevention-system-policy-event active

To turn on/off the IDPS event trigger, use this command.

Synopsis

(config)# **warning-notification firewall-event intrusion-prevention-system-policy-event active**

(config)# **no warning-notification firewall-event intrusion-prevention-system-policy-event active**

Option Description	warning-notification	Warning notification
	firewall-event	Firewall event setting
	intrusion-prevention-system-policy-event	IDPS All Policy Event setting
	active	Activate
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification firewall-event intrusion-prevention-system-policy-event active` `router(config)# no warning-notification firewall-event intrusion-prevention-system-policy-event active`	
Error Messages	^Parse error	
Related Commands	N/A	

intrusion-prevention-system-policy-event action

To set the IDPS event trigger action, use this command.

Synopsis

(config)# **warning-notification firewall-event intrusion-prevention-system-policy-event action** <UINT:combination>

Option Description	warning-notification	Warning notification
	firewall-event	Firewall event setting
	intrusion-prevention-system-policy-event	IDPS All Policy Event setting
	action	Enable Action setting
	<UINT:combination>	Relay1 only(8) None(0)
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification firewall-event intrusion-prevention-system-policy-event action 8` `router(config)# warning-notification firewall-event intrusion-prevention-system-policy-event action 0`	
Error Messages	^Parse error	
	% Invalid action value or non-support this combination action	
Related Commands	N/A	

relay-warning relay-event-operation

To turn on/off the relay event operation, use this command.

Synopsis

(config)# **relay-warning relay-event-operation**

(config)# **no relay-warning relay-event-operation**

Option Description	relay-warning	Relay Warning Configuration
	relay-event-operation	Enable Relay Event Operation
Defaults	Enabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# relay-warning relay-event-operation` `router(config)# no relay-warning relay-event-operation`	
Error Messages	^Parse error	
Related Commands	show relay-warning config	

clear relay-warning l3-policy-event

To clear Layer 3 event trigger relay warning, use this command.

Synopsis

clear relay-warning l3-policy-event

Option Description	clear	Clear Information
	relay-warning	Clear Relay Warning information
	l3-policy-event	Clear Layer 3 Deny Policy Event
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# clear relay-warning I3-policy-event`	
Error Messages	^Parse error	
	% You do not have admin privilege	
	% Clear relay event failed	
Related Commands	show relay-warning triggered-relay-event-list	

clear relay-warning protocol-filter-policy-event

To clear DPI event trigger relay warning, use this command.

Synopsis

clear relay-warning protocol-filter-policy-event

Option Description	clear	Clear Information
	relay-warning	Clear Relay Warning information
	protocol-filter-policy-event	Clear DPI Reset Policy Event
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# clear relay-warning protocol-filter-policy-event`	
Error Messages	^Parse error	
	% You do not have admin privilege	
	% Clear relay event failed	
Related Commands	show relay-warning triggered-relay-event-list	

clear relay-warning intrusion-prevention-system-policy-event

To clear IDPS event trigger relay warning, use this command.

Synopsis

clear relay-warning intrusion-prevention-system-policy-event

Option Description	clear	Clear Information
	relay-warning	Clear Relay Warning information
	intrusion-prevention-system-policy-event	Clear IDPS All Policy Event
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# clear relay-warning intrusion-prevention-system-policy-event`	
Error Messages	^Parse error	
	% You do not have admin privilege	
	% Clear relay event failed	
Related Commands	show relay-warning triggered-relay-event-list	

clear relay-warning all-event

To clear all event trigger relay warnings, use this command.

Synopsis

clear relay-warning all-event

Option Description	clear	Clear Information
	relay-warning	Clear Relay Warning information
	all-event	All Events
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# clear relay-warning all-event`	
Error Messages	^Parse error	
	% You do not have admin privilege	
	% Clear relay event failed	
Related Commands	show relay-warning triggered-relay-event-list	

show relay-warning config

To show relay warning configuration, use this command.

Synopsis

show relay-warning config

Option Description	show	Show System Information
	relay-warning	Display Relay Warning Configuration
	config	Relay Warning Configuration
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# clear relay-warning config` `Relay 1 Even Operation: Disabled`	
Error Messages	^Parse error	
Related Commands	relay-warning relay-event-operation	

show relay-warning triggered-relay-event-list

To show the reason for the triggered relay, use this command.

Synopsis

show relay-warning triggered-relay-event-list

Option Description	show	Show System Information
	relay-warning	Display Relay Warning Configuration
	triggered-relay-event-list	Current Relay Warning List
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# show relay-warning triggered-relay-event-list` `Index Event Relay` `-------- ------------------------------ --------` `1 Power Input 1 On->Off Relay 1` `2 DI 1 Off Relay 1` `3 Port 1 Link On Relay 1` `4 Port 3 Link On Relay 1` `5 Port 5 Link Off Relay 1` `6 Port 9 Link Off Relay 1` `7 Port 10 Link Off Relay 1` `8 Layer 3 Policy: Deny Event Relay 1` `9 DPI Policy: Reset Event Relay 1` `10 IDPS Policy: All Event Relay 1`	
Error Messages	^Parse error	
Related Commands	clear relay-warning l3-policy-event clear relay-warning protocol-filter-policy-event clear relay-warning intrusion-prevention-system-policy-event clear relay-warning all-event	

warning-notification system-event clear-relay-warning-event active

To turn on/off the clear relay warning event trigger, use this command.

Synopsis

(config)# **warning-notification system-event clear-relay-warning-event active**

(config)# **no warning-notification system-event clear-relay-warning-event active**

Option Description	warning-notification	Warning notification
	system-event	System event setting
	clear-relay-warning-event	Relay Warning Event setting
	active	Activate
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification system-event clear-relay-warning-event active` `router(config)# no warning-notification system-event clear-relay-warning-event active`	
Error Messages	^Parse error	
Related Commands	N/A	

warning-notification system-event clear-relay-warning-event severity {UINT:type}

To set the severity of the clear relay warning event, use this command.

Synopsis

(config)# **warning-notification system-event clear-relay-warning-event severity** {UINT:type}

(config)# **no warning-notification system-event clear-relay-warning-event severity** {UINT:type}

Option Description	warning-notification	Warning notification
	system-event	System event setting
	clear-relay-warning-event	Relay Warning Event setting
	severity	- Emergency(0) Alert(1) Critical(2) Error(3) Warning(4) Notice(5) Information(6) Debug(7)
Defaults	Disabled	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# warning-notification system-event clear-relay-warning-event severity 7`	
Error Messages	^Parse error	
Related Commands	N/A	

warning-notification system-event clear-relay-warning-event action {UINT:combination}

To configure clear relay warning event action, use this command.

Synopsis

warning-notification system-event clear-relay-warning-event action {UINT:combination}

Option Description	warning-notification	Warning notification
	system-event	System event setting
	clear-relay-warning-event	Relay Warning Event setting
	action	Enable Action setting
	<combination>	None(0) SNMP Trap Server only(1) Email only(2) SNMP Trap Server+Email(3) Syslog only(4) SNMP Trap Server+Syslog Server(5) Email+Syslog Server(6) SNMP Trap Server+Email+Syslog Server(7) Relay1 only(8) SNMP Trap Server+Relay1(9) Email+Relay1(10) SNMP Trap Server+Email+Relay1(11) Syslog+Relay1(12) SNMP Trap Server+Syslog Server+Relay1(13) Email+Syslog Server+Relay1(14) SMS(32) SNMP Trap Server+SMS(33) Email+SMS(34) SNMP Trap Server+Email+SMS(35) Syslog Server+SMS(36) SNMP Trap Server+Syslog Server+SMS(37) Email+Syslog Server+SMS(38) SNMP Trap Server+Email+Syslog Server+SMS(39) Relay1+SMS(40) SNMP Trap Server+Relay1+SMS(41) Email+Relay1+SMS(42) SNMP Trap Server+Email+Relay1+SMS(43) Syslog Server+Relay1+SMS(44) SNMP Trap Server+Syslog Server+Relay1+SMS(45) Email+Syslog Server+Relay1+SMS(46)
Defaults	N/A	
Command Modes	Global Configuration	

Usage Guidelines	N/A
Examples	router# configure router(config)# warning-notification system-event clear-relay-warning-event action 1 router(config)# warning-notification system-event clear-relay-warning-event action 0
Error Messages	^Parse error
	% Invalid action value or non-support this combination action
Related Commands	N/A

show relay-warning triggered-relay-event-list

To show the event causing relay the relay trigger, use this command.

Synopsis

show relay-warning triggered-relay-event-list

Option Description	show	Show System Information
	relay-warning	Display Relay Warning Configuration
	triggered-relay-event-list	Current Relay Warning List
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	router# show relay-warning triggered-relay-event-list Index Event Relay -------- ------------------------------ -------- 1 Power Input 1 On->Off Relay 1 2 DI 1 Off Relay 1 3 Port 1 Link On Relay 1 4 Port 3 Link On Relay 1 5 Port 5 Link Off Relay 1 6 Port 9 Link Off Relay 1 7 Port 10 Link Off Relay 1 8 Layer 3 Policy: Deny Event Relay 1 9 DPI Policy: Reset Event Relay 1 10 IDPS Policy: All Event Relay 1	
Error Messages	^Parse error	
Related Commands	clear relay-warning l3-policy-event clear relay-warning protocol-filter-policy-event clear relay-warning intrusion-prevention-system-policy-event clear relay-warning all-event	

Additional TRDP DPI Filter Parameters

show protocol-filter policy

To show information of the protocol filter policy, use this command.

Synopsis

show protocol-filter policy [<index>]

Option Description	index	Configure policy index number
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	Show information of protocol filter global settings. router# show protocol-filter policy 100 Policy Index : 20 Name : test_pol Status : Disable From Interface : Any To Interface : Any Source IP : Any Destination IP : Any Protocol : Any Application Protocol : test_mb Action : Accept Command Type : Master Query	
Error Messages	N/A	
Related Commands	N/A	

Additional TRDP DPI Filter Parameters

reply-ip

To configure reply IP as a TRDP object, use the **reply-ip** global configuration command.

Synopsis

(config-obj-dpi-trdp)# **reply-ip any**

(config-obj-dpi-trdp)# **reply-ip single <IPV4ADDR:ipaddr>**

(config-obj-dpi-trdp)# **reply-ip range <IPV4ADDR:s_ip> <IPV4ADDR:e_ip>**

(config-obj-dpi-trdp)# **reply-ip subnet <IPV4ADDR:ipaddr> <IPV4ADDR:netmask>**

Option Description	**any**	Any IP address
	single	Single IP address
	<IPV4ADDR:ipaddr>	IP address
	range	IP address range
	<IPV4ADDR:s_ip>	IP address range start
	<IPV4ADDR:e_ip>	IP address range end
	subnet	Subnet
	<IPV4ADDR:netmask>	Netmask
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# object industrial-protocol-dpi trdp` `router(config-obj-dpi-trdp)# reply-ip any` `router(config-obj-dpi-trdp)# reply-ip single 1.1.1.1` `router(config-obj-dpi-trdp)# reply-ip range 1.1.1.1 2.2.2.2` `router(config-obj-dpi-trdp)# reply-ip subnet 1.1.1.1 255.255.255.0`	
Error Messages	% The end address should equal to or larger than start address.	
	^Parse error	
	^Incomplete command	
Related Commands	show object industrial-protocol-dpi	

com-id-type

To configure com-id type as a TRDP object, use the **com-id-type** global configuration command.

Synopsis

(config-obj-dpi-trdp)# **com-id-type** <UINT:type>

Option Description	**com-id-type**	com id type
	<UINT:type>	1 (Basic), 2 (Advanced)
Defaults	n/a	
Command Modes	Global configuration	
Usage Guidelines	To set com-id Type	
Examples	`router# configure` `router(config)# object industrial-protocol-dpi trdp` `router(config-obj-dpi-trdp)# com-id-type 1`	
Error Messages	% Invalid Index. It must be 1 - 2.	
	^Parse error	
	^Incomplete command	
Related Commands	show object industrial-protocol-dpi	

com-id

To set reply COM IDs and related COM IDs by index as TRDP objects, use the **com-id** global configuration command.

Synopsis

(config-obj-dpi-trdp)# **com-id all**

(config-obj-dpi-trdp)# **com-id** <STRING:id_num_str>

(config-obj-dpi-trdp)# **com-id all reply-com-id all item** <UINT:id>

(config-obj-dpi-trdp)# **com-id all reply-com-id** <STRING:reply_id_num_str> item <UINT:id>

(config-obj-dpi-trdp)# **com-id** <STRING:id_num_str> reply-com-id all item <UINT:id>

(config-obj-dpi-trdp)# **com-id** <STRING:id_num_str> **reply-com-id** <STRING:reply_id_num_str> **item** <UINT:id>

(config-obj-dpi-trdp)# **com-id list**

(config-obj-dpi-trdp)# **show**

Option Description	com-id	com id
	All	all
	<STRING:id_num_str>	com id string
	reply-com-id	reply com id
	<STRING:reply_id_num_str>	reply com id string
	Item	item id
	<UINT:id>	item id number
	Show	show current object setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# object industrial-protocol-dpi trdp router(config-obj-dpi-trdp)# com-id list 0: unspecified PDU 1: ETBCTRL telegram 2: CSTINFO notification message 3: CSTINFOCTRL notification message 10: TRDP Echo 31: TRDP - statistics request command 35: TRDP - global statistics data 36: TRDP - subscription statistics data 37: TRDP - publishing statistics data 38: TRDP - redundancy statistics data 39: TRDP - join statistics data 40: TRDP- UDP listener statistics data 41: TRDP - TCP listener statistics data 80: Conformance test- control telegram 81: Conformance test - status telegram 82: Conformance test - confirmation request telegram 83: Conformance test - confirmation reply telegram 84: Conformance test - opTrnDir request telegram 85: Conformance test - opTrnDir reply telegram 86: Conformance test - echo request telegram 87: Conformance test - echo reply telegram 88: Conformance test - echo notification telegram 100: TTDB - operational train directory status telegram 101: TTDB - operational train directory notification	

	102: TTDB - train directory information request 103: TTDB - train directory information reply 104: TTDB - consist information request 105: TTDB - consist information reply 106: TTDB - train network directory information request 107: TTDB - train network directory information reply 108: TTDB - operational train directory information request 109: TTDB - operational train directory information reply 110: TTDB - train information complete request 120: ECSP - control telegram 121: ECSP - status telegram 122: ECSP - Confirmation/Correction request 123: ECSP - Confirmation/Correction reply 130: ETBN - control request 131: ETBN - status reply 132: ETBN - train network directory request 133: ETBN - train network directory reply 140: TCN-DNS - resolving request telegram (query) 141: TCN-DNS - resolving reply telegram router(config-obj-dpi-trdp)# name test_obj router(config-obj-dpi-trdp)# protocol-filter-profile 10 router(config-obj-dpi-trdp)# msg-type 0x5070 router(config-obj-dpi-trdp)# reply-ip single 10.10.10.10 router(config-obj-dpi-trdp)# com-id-type 2 router(config-obj-dpi-trdp)# com-id 1,2,3 reply-com-id 4,5,6 item 1 router(config-obj-dpi-trdp)# com-id 123 reply-com-id 456 item 2 router(config-obj-dpi-trdp)# show Name : test_obj Profile : 10. Manual Message Type : 0x5070 com-id Type : 2 (Advanced) com-id 1 : 1,2,3 reply-com-id 1 : 4,5,6 com-id 2 : 123 reply-com-id 3 : 456 Reply IP : 10.10.10.10 router(config-obj-dpi-trdp)# exit
Error Messages	% com-id has already set because the profile is not Manual.
	^Parse error
	^Incomplete command
Related Commands	show object industrial-protocol-dpi

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>
(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	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.
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• No modification function is provided. In case modification on a specific index is required, remove it first and then add a new policy. • Types a valid index to enter sub-level configuration mode. • Exits the sub-level configuration mode to let settings take effect. • Create network(service) object(s) in advance so that those object(s) can be used on this session control policy. • Configure SNMP Trap in advance when sending event logs via SNMP trap. • Configure Syslog server in advance when sending event logs to syslog server. • "uuid" option in this command is reserved for Moxa use only.	
Examples	• Drop all packets when total TCP connections to Server1 exceeds 10: `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 • Delete session control index 1: router# configure router(config)# no session-control 1 router(config)# exit
Error Messages	% 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
Related Commands	show session-control snmp-server host snmp-server trap-mode logging <ip-addr>

show session-control

To check the session-control policy settings on the router, use the **show session-control** command.

Synopsis

show session-control

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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 : <4> Warning Local Storage : Enable Syslog Server : Disable SNMP Trap Server : Disable	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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**}

Option Description	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.
Defaults	The default settings have all features enabled, except for 'new-tcp-without-syn-scan', which is disabled by default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Enable xmas-scan port scan protection: `router# configure` `router(config)# dos xmas-scan`	
Error Messages	% Invalid DoS Attack Name.	
	% Limit bandwidth must be 1 - 4000 pkt/s.	
	^Parse error	
	^Incomplete command	
Related Commands	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 }**

Option Description	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)
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	Enable xmas-scan port scan protection: `router# configure` `router(config)# dos xmas-scan`	
Error Messages	% 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	
Related Commands	show dos	

Show DoS Configuration

show dos

To show DoS configuration, use the **show dos** command.

Synopsis

#show dos

Option Description	show	Show system information
	dos	Display DoS Defense configurations
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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 : <2> Critical Flash : Enable Syslog : Enable Trap : Enable	
Error Messages	N/A	
Related Commands	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 }**

Option Description	logging	Set logging
	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
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`Router(config)# logging dos`	
Error Messages	% Severity level is out of range!	
Related Commands	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 }

Option Description	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.
Defaults	Soft lockdown mode is disabled.	
Command Modes	Global configuration	
Usage Guidelines	• Make sure the intended interface is created before enabling this feature. • 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.	
Examples	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.	

Error Messages	% Must be 1 - 90. % Must be 1 - 50. % Must be 1 - 5. % Must be 3 - 10.
Related Commands	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

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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#	
Error Messages	^Parse error ^Incomplete command	
Related Commands	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> | <STRING:ipaddr>
                 interface <wanif-name> | <lanif-name>
                 startup-mode {start | wait | route} |
                 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>}

(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}
```

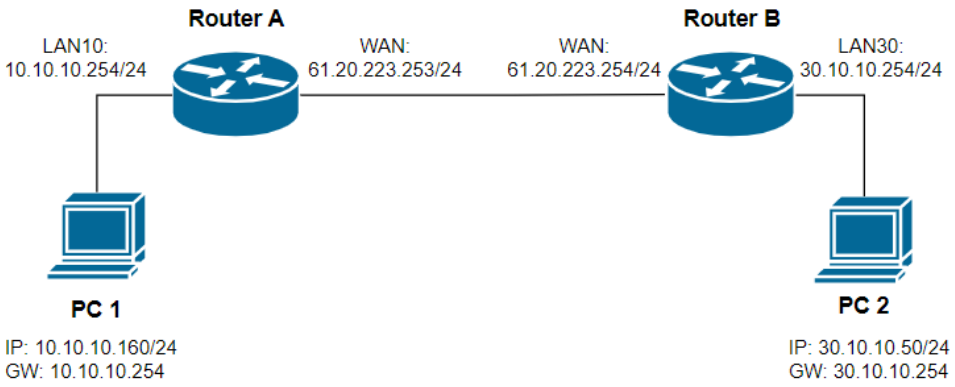
(config)# **no ipsec** {**all-connect** |
nat-t |
<ipsec-name>}

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 (IP address or Domain Name)
	interface	Specifies WAN or LAN interface
	wanif-name	WAN, wanif-name is case-sensitive
	lanif-name	LAN, lanif-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.and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # $ % & * ( ) . + = { } [ ] | : ; , ~, no space is allowed.
	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
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	• Specifies a non-existing <ipsec-name> will create a new entry of an IPsec connection. • Types a valid name of the VPN tunnel to enter sub-level configuration mode. • Exits the sub-level configuration mode to let settings take effect.	
Examples	**IPsec (Site to Site):** Prerequisites: • TN router A: - WAN: 61.20.223.253/24, VLAN ID=20, WAN interface - LAN10: 10.10.10.254/24, VLAN ID=10, interface used for internal network - L2TP server: disabled • TN router B: - WAN: 61.20.223.254/24, VLAN ID=20, WAN interface - LAN30: 30.10.10.254/24, VLAN ID=30, interface used for internal network - L2TP server: disabled • PC-1: - IP: 10.10.10.160/24 - Gateway: 10.10.10.254	

- PC-2 :
  - IP: 30.10.10.50/24
  - Gateway: 30.10.10.254

Network topology:



Scenario:
a) Router (A) and Router (B) establish an IPsec VPN site-to-site tunnel.
b) 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
```

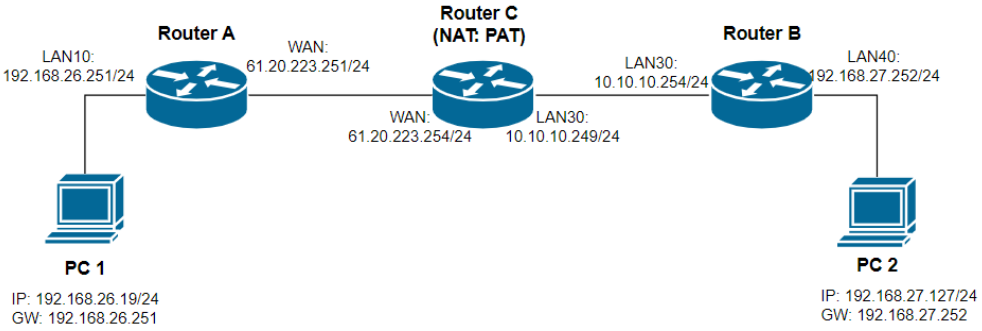
```
router(config-ipsec)# interface WAN
router(config-ipsec)# startup-mode start
router(config-ipsec)# local-multi-network 30.10.10.0/24
router(config-ipsec)# remote-multi-network 10.10.10.0/24
router(config-ipsec)# identity address
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
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:
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 [PAT 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
```

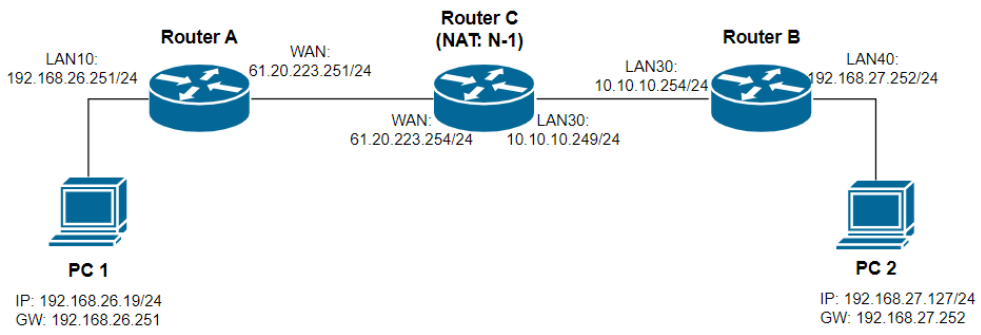
```
router(config-ipsec)# local-multi-network 192.168.27.0/24
router(config-ipsec)# remote-multi-network 192.168.26.0/24
router(config-ipsec)# identity address 192.168.27.252 192.168.26.251
router(config-ipsec)# phase1
router(config-ipsec-phase1)# ike-mode main
router(config-ipsec-phase1)# ike-version 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
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
```

	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)#
Error Messages	% is over length. It must be 1 - 64.
	% 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 - 64.
	^Parse error
	^Incomplete command
Related Commands	show ipsec show logging event-log vpn

show ipsec

To check the IPsec VPN configuration and status on the router, use the **show ipsec** command.

Synopsis

show ipsec [{**status** |
<ipsec-name>}]

Option Description	status	Specifies to display IPsec VPN connection status
	ipsec-name	Specifies to display the configuration of this IPsec VPN connection
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	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>]

Option Description	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, ...
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	`router # show logging event-log vpn` `VPN Log:  0  message lines logged,` `---` `Index  Date  Time  Severity  Event` `-----  ----  ----  --------  -----`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ipsec	

L2TP Server

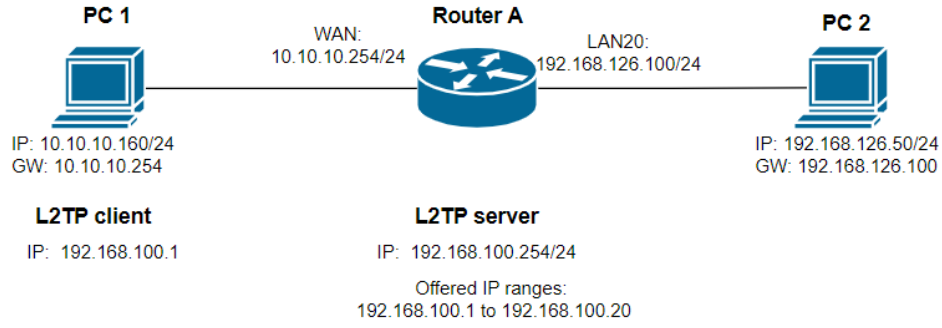
l2tp

To specify or modify L2TP server function on the router, use the **l2tp** global configuration command. To disable L2TP server mode or remove the user, use no form of this command.

Synopsis

(config)# **l2tp** {**interface WAN local-ip** <loc-ip> **offer-ip** <ip1> <ip2> |
user <username> **password** <pwd>}

(config)# **no l2tp** {**interface WAN** |
user <username>}

Option Description	interface	Specifies WAN interface
	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 64 and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # $ % & * ( ) . + = { } [ ] | : ; , ~, no space is allowed.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Configures WAN interface in advance is required to use this command.	
Examples	L2TP over IPsec (Site to Site(Any)): Prerequisites: • TN router: - WAN: 10.10.10.254/24, VLAN ID=10, WAN interface - LAN20: 192.168.126.100/24, VLAN ID=20, interface used for internal network - Layer 3 filter policy: Accept source IP addresses: from 192.168.100.1 to 192.168.100.254 • PC-1 from WAN: - IP: 10.10.10.160/24 - Gateway: 10.10.10.254 • PC-2 on the internal network: - IP: 192.168.126.50/24 - Gateway: 192.168.126.100 Network topology:  Scenario:	

	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. 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)#`
Error Messages	% is invalid WAN interface name
	% is over length. It must be 1 - 64.
	^Parse error
	^Incomplete command
Related Commands	show l2tp

show l2tp

To check the L2TP server settings on the router, use the **show l2tp** command.

Synopsis

show l2tp

Option Description	N/A	
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	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 :test Password :********	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	l2tp	

OpenVPN

ovpn

To enter OpenVPN Client configuration submode and configure OpenVPN settings.

Synopsis

(config)# **ovpn**

Option Description	vpvn	Enter OpenVPN Client configuration submode.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	The configurations set under the submode should be applied via ovpn_apply command.	
Examples	`Enter OpenVPN Client configuration submode` `(config)# ovpn`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ovpn_apply	

enable/disable

To enable / disable OpenVPN Client connection, use the enable/disable commands.

Synopsis

(config-ovpn)# { enable | disable }

Option Description	enable	Enable OpenVPN Client.
	disable	Disable OpenVPN Client.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Not applied before ovpn_apply is executed.	
Examples	`Enable OpenVPN Client` `(config-ovpn)# enable` `Disable OpenVPN Client` `(config-ovpn)# disable`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ovpn_apply	

description

To configure the description of OpenVPN Client profile use the **description** command.

Synopsis

(config-ovpn)# **description** $desc

Option Description	description	Configure the description of OpenVPN Client profile
	desc	The description of the profile.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Not applied before ovpn_apply is executed.	
Examples	`Set description of OpenVPN Client to "OVPN-profile"` `(config-ovpn)# description OVPN-profile`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ovpn_apply	

username

To set username of OpenVPN Client profile for authentication, use the **username** command.

Synopsis

(config-ovpn)# **username** $un

Option Description	username	Configure the username for authentication.
	un	The username to be set.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Not applied before ovpn_apply is executed.	
Examples	`Set username of OpenVPN Client to "OVPN-username"` `(config-ovpn)# username OVPN-username`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ovpn_apply	

password

To set the password of OpenVPN Client profile for authentication, use the **password** command.

Synopsis

(config-ovpn)# **password** $pwd

Option Description	password	Configure the password for authentication.
	pwd	The password to be set.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Not applied before ovpn_apply is executed.	
Examples	`Set password of OpenVPN Client to "OVPN-password"` `(config-ovpn)# password OVPN-password`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	ovpn_apply	

ovpn_apply

To apply modified settings of OpenVPN Client, use the **opvn_apply** command.

Synopsis

(config-ovpn)# **ovpn_apply**

Option Description	ovpn_apply	Apply the modified OpenVPN Client configuration.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`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`	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	description $desc username $un password $pwd	

show ovpn

To show the information of OpenVPN Client, use the **show ovpn** command.

Synopsis

show ovpn

Option Description	show	Display system information.
	ovpn	Display OpenVPN Client information.
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	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 ----------	
Error Messages	^Parse error	
	^Incomplete command	
Related Commands	N/A	

IPS

inline-idps

To enable or disable the inline IPS function, use the inline-idps global configuration command.

Synopsis

(config)# **intrusion-prevention-system inline-idps** [**enable** | **disable**]

Option Description	**intrusion-prevention-system**	IPS Policy Setting
	inline-idps	Inline IDPS
Defaults	disable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# intrusion-prevention-system inline-idps enable router(config)# exit	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show intrusion-prevention-system	

intrusion-prevention-system inline-idps operation-mode

Synopsis

To set IDPS operation mode, use the inline-idps global configuration command.

(config)# **intrusion-prevention-system inline-idps operation-mode** [prevention | detection]

Option Description	**intrusion-prevention-system**	IPS Policy Setting
	inline-idps	Inline IDPS
	operation-mode	Setting Operation Mode
Defaults	Prevention	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# intrusion-prevention-system inline-idps operation-mode prevention` `router(config)# exit`	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show intrusion-prevention-system	

intrusion-prevention-system log

To enable the IPS log function, use the intrusion-prevention-system log global configuration command. To disable IPS log, use the **no** form of this command.

(config)# **intrusion-prevention-system log**

(config)# **no intrusion-prevention-system log**

Option Description	**intrusion-prevention-system**	IPS Policy Setting
	log	IPS Policy Log
Defaults	Enable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# intrusion-prevention-system log` `router(config)# exit`	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	Show intrusion-prevention-system	

intrusion-prevention-system log flash

To enable the IPS local storage event, use the intrusion-prevention-system log flash global configuration command. To disable IPS local storage event, use the **no** form of this command.

(config)# **intrusion-prevention-system log flash**

(config)# **no intrusion-prevention-system log flash**

Option Description	**intrusion-prevention-system**	IPS Policy Setting
	log	IPS Policy Log
	flash	Log to Local Storage
Defaults	Enable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# intrusion-prevention-system log flash router(config)# exit	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show intrusion-prevention-system	

intrusion-prevention-system log trap

To enable the IPS trap event, use the intrusion-prevention-system log trap global configuration command. To disable the IPS trap event, use the **no** form of this command.

(config)# **intrusion-prevention-system log trap**

(config)# **no intrusion-prevention-system log trap**

Option Description	**intrusion-prevention-system**	IPS Policy Setting
	log	IPS Policy Log
	trap	Log to SNMP Trap Server
Defaults	disable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# intrusion-prevention-system log trap router(config)# exit	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show intrusion-prevention-system	

intrusion-prevention-system log syslog

To enable the IPS syslog event, use the intrusion-prevention-system log syslog global configuration command. To disable the IPS trap syslog, use the **no** form of this command.

(config)# **intrusion-prevention-system log syslog**

(config)# **no intrusion-prevention-system log syslog**

Option Description	**intrusion-prevention-system**	IPS Policy Setting
	log	IPS Policy Log
	syslog	Log to Syslog Server
Defaults	disable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# intrusion-prevention-system log syslog` `router(config)# exit`	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show intrusion-prevention-system	

intrusion-prevention-system log severity

To configure IPS log severity., use the intrusion-prevention-system log severity global configuration command.

(config)# **intrusion-prevention-system log severity** { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 }

Option Description	**intrusion-prevention-system**	IPS Policy Setting
	log	IPS Policy Log
	severity	Log Severity
	<UINT:level>	0(Emergency) - 7(Debug)
Defaults	4	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# intrusion-prevention-system log severity 1` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
	% Invalid Severity Level. (0-7)	
	% Not support this feature on this platform.	
Related Commands	show intrusion-prevention-system	

show intrusion-prevention-system

To show IPS global settings, use the show intrusion-prevention-system command.

(config)# **show intrusion-prevention-system**

Option Description	show	Show System Information
	intrusion-prevention-system	Show IPS Policy Setting
Defaults	N/A	
Command Modes	N/A	
Usage Guidelines	N/A	
Examples	router# show intrusion-prevention-system IPS Event Global Setting: Log Status: Enable Severity: <4> Warning Local Storage: Enable Syslog Server: Disable SNMP Trap Server: Disable ----------	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	N/A	

intrusion-prevention-system log syslog

To enable domain protection logs, use the domain-protect log global configuration command. To disable the domain protection logs, use the **no** form of this command.

(config)# **domain-protect log**

(config)# **no domain-protect log**

Option Description	domain-protect	Domain Protection Setting
	log	Domain Protection Log
Defaults	enable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# domain-protect log router(config)# exit	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show domain-protect	

domain-protect log flash

To enable the domain protection local storage event, use the domain-protect log flash global configuration command. To disable the domain protection local storage event, use the **no** form of this command.

(config)# **domain-protect log flash**

(config)# **no domain-protect log flash**

Option Description	**domain-protect**	Domain Protection Setting
	Log	Domain Protection Log
	Flash	Log to Local Storage
Defaults	Enable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# domain-protect log flash` `router(config)# exit`	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show domain-protect	

domain-protect log trap

To enable the domain protection local storage event, use the domain-protect log trap global configuration command. To disable the domain protection trap event, use the **no** form of this command.

(config)# **domain-protect log trap**

(config)# **no domain-protect log trap**

Option Description	**domain-protect**	Domain Protection Setting
	log	Domain Protection Log
	trap	Log to SNMP Trap Server
Defaults	disable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# domain-protect log trap` `router(config)# exit`	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show domain-protect	

domain-protect log syslog

To enable the domain protection syslog event, use the domain-protect log syslog global configuration command. To disable the domain protection syslog event, use the **no** form of this command.

(config)# **domain-protect log syslog**

(config)# **no domain-protect log syslog**

Option Description	**domain-protect**	Domain Protection Setting
	log	Domain Protection Log
	syslog	Log to Syslog Server
Defaults	disable	
Command Modes	Global configuration	
Usage Guidelines	To turn on/off domain protection syslog event.	
Examples	`router# configure` `router(config)# domain-protect log syslog` `router(config)# exit`	
Error Messages	^Parse error	
	% Not support this feature on this platform.	
Related Commands	show domain-protect	

domain-protect log severity

To configure the domain protection log severity level, use the domain-protect log severity global configuration command.

(config)# **domain-protect log severity { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 }**

Option Description	domain-protect	Domain Protection Setting
	log	Domain Protection Log
	severity	Log Severity
	<UINT:level>	0(Emergency) - 7(Debug)
Defaults	4	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)#domain-protect log severity 1` `router(config)# exit`	
Error Messages	^Parse error	
	^Incomplete command	
	% Invalid Severity Level. (0-7)	
	% Not support this feature on this platform.	
Related Commands	show domain-protect	

domain-protect log severity

To show domain protection settings information, use the **show domain-protect** global configuration command.

show domain-protect

Option Description	show	Show System Information
	domain-protect	Show Domain Protection Setting
Defaults	N/A	
Command Modes	N/A	
Usage Guidelines	N/A	
Examples	`router# show domain-protect` `Domain Protection Event Global Setting` `Log Status : Enable` `Severity : <4> Warning`	

	Local Storage : Enable Syslog Server : Disable SNMP Trap Server : Disable ----------
Error Messages	^Parse error
	% Not support this feature on this platform.
Related Commands	N/A

Connection Management

This section describes the commands used for connection management.

show conn-mgmt

To show connection management settings and current connection table, use this command.

Synopsis

show conn-mgmt

Option Description	show	Show System Information
	conn-mgmt	Show connection management settings and current connection table
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	Show connection management	
Examples	router# show conn-mgmt Connection Management ---------- Status: Enable Alive Time Setting ---------- Life time: 1000 sec Idle time: 79 sec Global Event Setting ---------- Log status: Enable Log severity: <0> Emergency Log destination Local storage: Enable Log destination Syslog: Enable Log destination SNMP Trap: Enable	
Error Messages	^Parse error	
Related Commands	N/A	

logging conn-mgmt

Synopsis

(config)# **logging conn-mgmt severity** <severity-level>

(config)# **logging conn-mgmt** { flash | syslog | trap }

(config)# **no logging conn-mgmt**

Option Description	logging	Set log
	conn-mgmt	Enable to log when a new connection is established or removed from the connection table.
	severity	Severity setting

	severity-level	Emergency(0) Alert(1) Critical(2) Error(3) Warning(4) Notice(5) Information(6) Debug(7)
	flash	Save log in Local Storage
	syslog	Send log in Syslog Server
Defaults	connection-status log: disabled. connection-status log severity: Informational. connection-status log destination: none.	
Command Modes	Global configuration	
Usage Guidelines	Enable/disable log to change connection table	
Examples	Enable change log of connection table `# configure` `(config)# logging conn-mgmt.` Set connection table change log Severity to Critical `# configure` `(config)# logging conn-mgmt severity 2` Store connection table change log into Flash `# configure` `(config)# logging conn-mgmt flash` Disable change log of connection table `# configure` `(config)# no logging conn-mgmt` Cancel syslog from log destination of connection table change `# configure` `(config)# no logging conn-mgmt syslog`	
Error Messages	^Parse error	
Related Commands	show conn-mgmt	

conn-mgmt life-time

Synopsis

(config)# **conn-mgmt life-time** <lifetime_sec>

(config)# **no conn-mgmt life-time**

Option Description	conn-mgmt	Set the alive time for connection
	life-time	The max lifetime for the continuous working period for a connection
	lifetime_sec	Lifetime in seconds. 300 to 14400, 0 means disable
Defaults	14400	
Command Modes	Sub-level configuration	
Usage Guidelines	Enable / Disable monitoring lifetime	
Examples	Set lifetime 4 hours to each the new established connection. `# configure` `(config)# conn-mgmt lifetime 14400` Disable lifetime `# configure` `(config)# no conn-mgmt lifetime`	
Error Messages	% Over length. It must be 300 - 14400 !!! <UINT:time> X	
	% Idle Time should less than Lifetime !!!	

Related Commands	show conn-mgmt

conn-mgmt idle-time

Synopsis

(config)# **conn-mgmt idle-time** <idle_sec>

(config)# **no conn-mgmt idle-time**

Option Description	conn-mgmt	Setting alive time for connection
	idle-time	The max idle time for the current working rule.
	idle_sec	Idle time in seconds. 60 to 14400. [VR] Idle time in seconds. 60 to 14400, 0 means disable.
Defaults	0	
Command Modes	Sub-level configuration	
Usage Guidelines	Enable / Disable monitoring idle time	
Examples	Set idle time of 10 minutes to each established connection. `# configure` `(config)# conn-mgmt idle 14400` Disable idle time `# configure` `(config)# no conn-mgmt idle`	
Error Messages	^Parse error	
	% Over length. It must be 60 - 14400 !!! <UINT:time> X	
	% Idle Time should less than Lifetime !!!	
Related Commands	show conn-mgmt	

conn-mgmt extend

Synopsis

(config)# **conn-mgmt extend** <conn_idx>

Option Description	conn-mgmt	Setting alive time for connection
	Extend	Reset the remaining lifetime to the configured lifetime value.
	conn_idx	The table index of the specific connection for which the remaining lifetime is to be extended.
Defaults	N/A	
Command Modes	Prvileged EXEC / User EXEC	
Usage Guidelines	Extend remaining lifetime to the configured lifetime	
Examples	Extend the remaining lifetime of the connection with index 2 to the configured lifetime value. `# conn-mgmt extend 2`	
Error Messages	^Parse error	
	% Over length. It must be 1 - 20000 !!!	
Related Commands	N/A	

conn-mgmt status

Synopsis

(config)# **conn-mgmt status enable**

(config)# **no conn-mgmt status enable**

Option Description	conn-mgmt	Setting alive time for connection

	status	Enable change logging of connection table.
	enable	Enable change logging of connection table.
Defaults	N/A	
Command Modes	Sub-level configuration	
Usage Guidelines	Extend remaining lifetime to the configured lifetime	
Examples	Enable connection alive time `# configure` `(config)# conn-mgmt enable` Disable connection alive time `# configure` `(config)# no conn-mgmt enable`	
Error Messages	^Parse error	
Related Commands	show conn-mgmt	

Directed Forwarding

This section describes the commands used for configuring the directed forwarding settings.

show directed-forwarding

Synopsis

show directed-forwarding

Option Description	show	Show System Information
	directed-forwarding	Directed Forwarding global setting and Directed Forwarding policy
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000# show directed-forwarding` `Global Enablement : Enable` `---------------------------` `Index : 1` `Status : Enable` `Incoming Interface : VLAN128` `Original Source IP : 123.1.1.1` `Original Destination IP : any` `Original UDP Destination Port : 52,53,54` `Outgoing Interface : LAN` `Translated Source IP : 1.2.3.255` `Translated Destination IP : any` `---------------------------`	
Error Messages	N/A	
Related Commands	N/A	

directed-forwarding

Synopsis

directed-forwarding

no directed-forwarding

Option Description	no	Negate Command or Set to Default
	directed-forwarding	Directed Forwarding Enablement
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# directed-forwarding`	
Error Messages	N/A	
Related Commands	N/A	

directed forwarding <index>

Synopsis

directed-forwarding <index> **enable**

directed-forwarding <index> **disable**

directed-forwarding <UINT:index> **overwriteSa**

no directed-forwarding <UINT:index> **overwriteSa**

directed-forwarding <index> **original in-iface** <incoming-interface> **src-ip** <original-source-ip> **dst-ip** <original-destination-ip> **dst-udp-port** <original-udp-destination-port> **translated out-iface** <outgoing-interface> **src-ip** <translated-source-ip> **dst-ip** <translated-destination-ip>

no directed-forwarding <index>

Option Description	directed-forwarding	Directed Forwarding Setting
	index	Directed Forwarding Policy Index
	enable	Enable the Directed Forwarding Policy
	disable	Disable the Directed Forwarding Policy
	overwriteSa	Overwrite Packet's Source MAC Address
	original	Original packet information
	in-iface	Incoming Interface
	incoming-interface	Incoming Interface Name
	src-ip	Original Source IP
	original-source-ip	IP Address
	dst-ip	Original Destination IP
	original-destination-ip	IP Address
	dst-udp-port	Original UDP Destination Port
	original-udp-destination-port	Up to 8 UDP ports (e.g. any, 502, 52,53,54)
	translated	Translated packet information
	out-iface	Outgoing Interface
	outgoing-interface	Outgoing Interface Name
	src-ip	Translated Source IP
	translated_source_ip	IP Address
	dst-ip	Translated Destination IP
	translated_destination_ip	IP Address
	no	Negate Command or Set to Default
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`Firewall/VPN Router 00000# configure` `Firewall/VPN Router 00000(config)# directed-forwarding 20 original in-iface VLAN128 src-ip 123.1.1.1 dst-ip any dst-udp-port 502 translated out-iface LAN src-ip 1.2.3.255 dst-ip any`	
Error Messages	% Directed Forwarding Policy is full	
	% Index needs to be in the range 1-20	
	% Invalid incoming-interface	
	% Invalid original-source-ip	
	% Invalid original-destination-ip	
	% Invalid outgoing-interface	
	% Invalid translated_source_ip	
	% Invalid translated_destination_ip	

	% Incoming Interface cannot be the same
Related Commands	N/A

5. MXsecurity

This chapter describes the commands for the MXsecurity 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 **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information. • Enter configuration mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	(config)#	To exit to privileged EXEC mode, enter **exit**.	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example **interface ethernet** <mod-port> command and press enter	(config-if)#	To exit to global configuration mode, enter **exit**.	A sub-level to configure for example Ethernet port related arguments.

Command Sets

MXsecurity

mxsecurity service-addr

To configure the MXsecurity / MXviewOne MXsecurity Addon address, use the **mxsecurity service-addr** command.

Synopsis

mxsecurity service-addr <addr>

Option Description	service-addr	Configure MXsecurity service address
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# mxsecurity service-addr <addr>` `router(config)# exit`	
Error Messages	% Not support this feature on this platform % Invalid Server Name or Address	

mxsecurity https-port

To configure the MXsecurity / MXviewOne MXsecurity Addon HTTPS port, use the **mxsecurity https-port** command.

Synopsis

mxsecurity https-port <port>

Option Description	https-port	Configure MXsecurity HTTPS port
Defaults	443	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# mxsecurity https-port <port>` `router(config)# exit`	
Error Messages	% Not support this feature on this platform	
	% Range of Port is 1 to 65535	
	^ Parse error	
Related Commands	N/A	

mxsecurity communication-port

To configure the MXsecurity / MXviewOne MXsecurity Addon MQTT port, use the **mxsecurity communication-port** command.

Synopsis

mxsecurity communication-port <port>

Option Description	communication-port	Configure MQTT port for MXsecurity
Defaults	8883	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# mxsecurity communication-port <port>` `router(config)# exit`	
Error Messages	% Not support this feature on this platform	
	% Range of Port is 1 to 65535	
	^Parse error	
Related Commands	N/A	

mxsecurity connect

To establish a connection for the MXsecurity agent on the router to a PC using MXsecurity, use the **mxsecurity connect** command.

Synopsis

mxsecurity connect

Option Description	connect	Establish connection to MXsecurity
Defaults	N/A	
Command Modes	Global configuration, sub-level configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# mxsecurity connect` `router(config)# exit`	
Error Messages	% Not support this feature on this platform	
	% Please set MXsecurity service address and port before connecting	
Related Commands	N/A	

show mxsecurity-service status

To display connection status between the MXsecurity agent on the router to a PC using MXsecurity, use the **show mxsecurity-service status** command.

Synopsis

show mxsecurity-service status

Option Description	status	Show the status of the MXsecurity connection
Defaults	N/A	
Command Modes	Privileged EXEC mode	
Usage Guidelines	N/A	
Examples	`router# show mxsecurity-service status`	
Error Messages	N/A	
Related Commands	show hardware-interface show package	

6. Cellular Functions

This chapter describes the cellular functions for the device.

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 **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Begin a session with your router by using an admin type user account and password.	#	Enter **exit** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information. • Enter configuration mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	(config)#	To exit to privileged EXEC mode, enter **exit**.	First level to configure main router functions.
Sub-level configuration	While in global configuration mode, use for example **interface cellular** command and press enter	(config-if-cell)#	To exit to global configuration mode, enter **exit**.	A sub-level to configure for example Ethernet port related arguments.

> **NOTE**
>
> The commands in the chapter only support the models that come with the cellular functions.

Command Sets

General Settings

enable

To enable cellular interface, use **enable** command.

Synopsis

(config-if-cell)#**enable**

Option Description	enable	Enable the cellular interface
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# enable` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

disable

To disable cellular interface, use **disable** command.

Synopsis

(config-if-cell)# **disable**

Option Description	disable	Disable the cellular interface
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# disable` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

mtu

To configure cellular MTU unit, use **MTU** command.

Synopsis

(config-if-cell)# **MTU** <UINT:bytes>

Option Description	MTU	Configure MTU
	UINT:bytes	MTU unit (in bytes)
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# mtu <UINT:bytes>` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

data_connection enable

To enable cellular operation mode, use **data_connection enable** command.

Synopsis

(config-if-cell)# **data_connection enable**

Option Description	data_connection	Configure data connection operation
	enable	Enable the function
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# opmode router` `router(config-if-cell-router)# data_connection enable` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

sim 1/sim 2 disable

To disable cellular SIM 1/SIM 2, use **sim 1/sim 2 disable** command.

Synopsis

(config-if-cell)# **sim 1 disable**

(config-if-cell)# **sim 2 disable**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	disable	disable the function
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# sim 1 disable` `router(config-if-cell)# sim 2 disable` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

sim 1/sim 2 priority

To configure cellular SIM 1/SIM 2 priority, use **sim 1/sim 2 priority** command.

Synopsis

(config-if-cell)# **sim 1 priority 1**

(config-if-cell)# **sim 2 priority 2**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	priority	Set the priority for the SIM card
	1	Set the SIM card as the first priority
	2	Set the SIM card as the second priority
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# sim 1 priority 1` `router(config-if-cell)# sim 2 priority 2` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

sim 1/sim 2 carrier

To load cellular SIM 1/SIM 2 carrier, use **sim 1/sim 2 carrier** command.

Synopsis

(config-if-cell)# **sim 1 carrier 1**

(config-if-cell)# **sim 2 carrier 2**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	carrier	Set the priority for the SIM card
	STRING:carrier	Set the carrier of the telecom module
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# sim 1 carrier generic` `router(config-if-cell)# sim 2 carrier att` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

sim 1/sim 2 apn

To configure cellular SIM 1/SIM 2 APN value, use **sim 1/sim 2 apn** command.

Synopsis

(config-if-cell)# **sim 1 apn 1 <STRING:apn>**

(config-if-cell)# **sim 2 apn 2 <STRING:apn>**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	apn	Configure the APN setting
	STRING:apn	Input the APN value
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# sim 1 apn internet` `router(config-if-cell)# sim 2 apn emome` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	
Related Commands	show cellular_status	

sim 1/sim 2 pin

To configure cellular SIM1/SIM2 PIN value, use **sim 1/sim 2 pin** command.

Synopsis

(config-if-cell)# **sim 1 pin 1 <STRING:pin>**

(config-if-cell)# **sim 2 pin 2 <STRING:pin>**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	pin	Configure the PIN setting
	STRING:pin	Input the PIN value
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# sim 1 pin 1234` `router(config-if-cell)# sim 2 pin 0000` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

sim 1/sim 2 username

To configure cellular SIM1/SIM2 PIN username, use **sim 1/sim 2 username** command.

Synopsis

(config-if-cell)# **sim 1 username <STRING:username>**

(config-if-cell)# **sim 2 username <STRING::username>**

Option Description	sim 1/sim 2	Configure SIM 1/SIM2
	username	Configure the username setting
	STRING:username	Input the username
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# sim 1 username test 1` `router(config-if-cell)# sim 2 username test 2` `router(config-if-cell)# cellular_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

sim 1/sim 2 password

To configure cellular SIM1/SIM2 PIN password, use **sim1/sim2 password** command.

Synopsis

(config-if-cell)# **sim 1 password <STRING:password>**

(config-if-cell)# **sim 2 password <STRING:password>**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	password	Configure the password setting
	STRING:password	Input the password
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface cellular router(config-if-cell)# sim 1 password 000000 router(config-if-cell)# sim 2 password 123456 router(config-if-cell)# cellular_apply	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

sim 1/sim 2 authentication

To configure cellular SIM1/SIM2 authentication settings, use **sim 1/sim 2 authentication** command.

Synopsis

(config-if-cell)# **sim1 authentication <auto | pap | chap>**

(config-if-cell)# **sim2 authentication <auto | pap | chap>**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	authentication	Configure the authentication setting
	auto	Set the authentication as auto
	pap	Set the authentication as pap
	chap	Set the authentication as chap
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface cellular router(config-if-cell)# sim 1 authentication auto router(config-if-cell)# sim 1 authentication pap router(config-if-cell)# sim 1 authentication chap router(config-if-cell)# sim 2 authentication auto router(config-if-cell)# sim 2 authentication pap router(config-if-cell)# sim 2 authentication chap router(config-if-cell)# cellular_apply	

Error Messages	^Incomplete command
Related Commands	show cellular_status

sim 1/sim 2 band auto

To configure cellular SIM1/SIM2 band as auto mode, use **sim 1/sim 2 band auto** command.

Synopsis

(config-if-cell)# **sim 1 band auto**

(config-if-cell)# **sim 2 band auto**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	band	Configure the band mode
	auto	Set the band mode as auto
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface cellular router(config-if-cell)# sim 1 band auto router(config-if-cell)# sim 2 band auto router(config-if-cell)# cellular_apply	
Error Messages	^Incomplete command	
Related Commands	show cellular_status	

sim 1/sim 2 band manual

To configure cellular SIM1/SIM2 band mode as manual, use **sim 1/2 band manual** command.

Synopsis

(config-if-cell)# **sim 1 band manual**

(config-if-cell)# **sim 2 band manual**

Option Description	sim 1/sim 2	Configure SIM 1/SIM 2
	band	Configure the band mode
	manual	Set the band mode as manual
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router# interface cellular router(config-if-cell)# sim 1 band manual router(config-sim1-band-manual)# band-select 2g all router(config-sim1-band-manual)# band-select 2g none router(config-sim1-band-manual)# band-select 2g <STRING:band_list> router(config-sim1-band-manual)# band-select 3g all	

	router(config-sim1-band-manual)# band-select 3g none router(config-sim1-band-manual)# band-select 3g <STRING:band_list> router(config-sim1-band-manual)# band-select 4g all router(config-sim1-band-manual)# band-select 4g none router(config-sim1-band-manual)# band-select 4g <STRING:band_list> router(config-sim1-band-manual)# exit router(config-if-cell)# sim 2 band manual router(config-sim2-band-manual)# ... router(config-sim2-band-manual)# exit router(config-if-cell)# cellular_apply
Error Messages	^Incomplete command
Related Commands	show cellular_status show cellular connection show glink config

glink enable

To enable the cellular glink, use **glink enable** command.

Synopsis

(config-if-cell)# **glink enable**

Option Description	glink	Configure glink function
	enable	Enable the function
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface cellular router(config-if-cell)# glink enable router(config-if-cell)# glink_apply	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink remote_host1/2 domain

To configure the cellular glink domain name, use **glink remote_host1/host2 domain** command.

Synopsis

(config-if-cell)# **glink remote_host1/2 domain**

Option Description	glink	Configure glink function
	remote_host	Configure the remote host setting
	domain	Domain name for host 1 and host 2
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface cellular router(config-if-cell)# glink remote_host1 domain <STRING:name> router(config-if-cell)# glink remote_host2 domain <STRING:name> router(config-if-cell)# glink_apply	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink remote_host 1/host 2 ipaddr

To configure the cellular glink IP address, use **glink remote_host1/host2 ipaddr** command.

Synopsis

(config-if-cell)# **glink remote_host1/2 ipaddr**

Option Description	glink	Configure glink function
	remote_host	Configure the remote host setting
	ipaddr	IP address for host 1 and host 2
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface cellular router(config-if-cell)# glink remote_host1 ipaddr <IPV4ADDR:ipaddr> router(config-if-cell)# glink remote_host2 ipaddr <IPV4ADDR:ipaddr> router(config-if-cell)# glink_apply	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink check always enable

To enable the cellular glink check always function, use **glink check always enable** command.

Synopsis

(config-if-cell)# **glink check always enable**

Option Description	glink	Configure glink function
	check always	Configure check always function
	enabled	Enable the function
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# glink check always enable` `router(config-if-cell)# glink_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink check always interval

To configure the cellular glink check always interval value, use **glink check always interval** command.

Synopsis

(config-if-cell)# **glink check always interval <UINT:interval>**

Option Description	glink	Configure glink function
	check always	Configure check always function
	interval	Configure the interval
	<UINT:interval>	Interval value
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# glink check always interval <UINT:interval>` `router(config-if-cell)# glink_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink check idle enable

To enable the cellular glink check idle function, use **glink check idle enable** command.

Synopsis

(config-if-cell)# **glink check idle enable**

Option Description	glink	Configure glink function
	check idle	Configure check idle function
	enable	Enable the function
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# glink check idle enable` `router(config-if-cell)# glink_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink check idle interval

To configure the cellular glink check idle interval value, use **glink check idle interval** command.

Synopsis

(config-if-cell)# **glink check always interval <UINT:interval>**

Option Description	glink	Configure glink function
	check idle	Configure check idle function
	interval	Configure the interval
	<UINT:interval>	Interval value
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# glink check idle interval <UINT:interval>` `router(config-if-cell)# glink_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink check signal enable

To enable the cellular glink check signal function, use **glink check signal enable** command.

Synopsis

(config-if-cell)# **glink check idle enable**

Option Description	glink	Configure glink function
	check signal	Configure check signal function
	enable	Enable the function
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# glink check signal enable` `router(config-if-cell)# glink_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink check signal interval

To configure the cellular glink check signal interval value, use **glink check signal interval** command.

Synopsis

(config-if-cell)# **glink check signal interval <UINT:interval>**

Option Description	glink	Configure glink function
	check signal	Configure check signal function
	interval	Configure the interval
	<UINT:interval>	Interval value in minutes: 1 to 600
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# glink check signal interval <UINT:interval>` `router(config-if-cell)# glink_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

glink recovery reconnect

To configure the cellular glink recovery reconnection value, use **glink recovery reconnect** command.

Synopsis

(config-if-cell)# **glink recovery reconnect** <UINT:retry>

Option Description	glink	Configure glink function
	recovery reconnect	Configure check signal function
	<UINT:retry>	Retry value
	cellular_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface cellular` `router(config-if-cell)# glink recovery reconnect <UINT:retry>` `router(config-if-cell)# glink_apply`	
Error Messages	^Incomplete command	
Related Commands	show cellular_status show cellular connection show glink config	

SMS

send_sms

To configure the message content and destination, use **send_sms** command.

Synopsis

(config-sms)# **send_sms <STRING:country code> <STRING:phone><STRING:message)**

Option Description	send_sms	Configure send sms setting
	STRING:country code	Input the country code
	STRING:phone	Input the phone number
	STRING:message	Input the message
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)# send_sms <886> <910123456> <test>`	
Error Messages	^Incomplete command	
Related Commands	N/A	

remote_ctrl enable

To enable remote SMS control, use **remote_ctrl enable** command.

Synopsis

(config-sms)# **remote_ctrl**

(config-sms)# **enable**

Option Description	remote_ctrl	Configure remote SMS
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)# remote_ctrl` `router(config-sms)# enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

remote_ctrl disable

To disable the remote SMS, use **remote_ctrl disable** command.

Synopsis

(config-sms)# **remote_ctrl**

(config-sms)# **disable**

Option Description	remote_ctrl	Configure remote SMS
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)# remote_ctrl` `router(config-sms)# disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

remote_ctrl password

To configure the remote SMS control password, use **remote_ctrl password** command.

Synopsis

(config-sms)# **remote_ctrl**

(config-sms)# **password <STRING:password>**

Option Description	remote_ctrl	Configure remote SMS
	password	Input the password
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# password 123456`	
Error Messages	^Incomplete command	
Related Commands	show sms	

authentication enable

To enable the remote SMS authentication, use **authentication enable** command.

Synopsis

(config-sms-remote)# **authentication enable**

Option Description	authentication	Configure authentication
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# authentication enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

authentication disable

To disable the remote SMS authentication, use **authentication disable** command.

Synopsis

(config-sms-remote)# **authentication disable**

Option Description	authentication	Configure authentication
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# authentication disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

phone_number

To configure the trusted remote SMS phone number, use **remote_ctrl** and **phone_number_1/2/3/4** command.

Synopsis

(config-sms)# **remote_ctrl**

(config-sms-remote)# **phone_number_1 <STRING:name> <STRING:country> <STRING:phone>**

Option Description	<string:name>	Input the name
	<string:country>	Input the country code
	<string:phone>	Input the phone number
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# sms router(config-sms)# remote_ctrl (config-sms-remote)# phone_number_1 test1 886 912345678 (config-sms-remote)# phone_number_2 test2 1 123456789 (config-sms-remote)# phone_number_3 test3 1 234567890 (config-sms-remote)# phone_number_4 test4 886 923456789	
Error Messages	^Incomplete command	
Related Commands	show sms	

sms_receipt enable

To enable the remote SMS receipt function, use **sms_receipt enable** command.

Synopsis

(config-sms-remote)# **sms_receipt enable**

Option Description	sms_receipt	Configure SMS receipt
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# sms router(config-sms)# router(config-sms)# remote_ctrl (config-sms-remote)# sms_receipt enable	
Error Messages	^Incomplete command	
Related Commands	show sms	

sms_receipt disable

To disable the remote SMS receipt function, use **sms_receipt disable** command.

Synopsis

(config-sms-remote)# **sms_receipt disable**

Option Description	sms_receipt	Configure SMS receipt
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# sms_receipt disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

system_restart action enable

To enable the remote SMS system restart action function, use **system_restart action enable** command.

Synopsis

(config-sms-remote)# **system_restart action enable**

Option Description	system_restart action	Configure system restart action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# system_restart action enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

system_restart action disable

To disable the remote SMS system restart action function, use **system_restart action disable** command.

Synopsis

(config-sms-remote)# **system_restart action disable**

Option Description	system_restart action	Configure system restart action
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# system_restart action disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

cellular_report action enable

To enable the remote SMS cellular report action function, use **cellular_report action enable** command.

Synopsis

(config-sms-remote)# **cellular_report action enable**

Option Description	cellular_report action	Configure cellular report action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# cellular_report action enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

cellular_report action disable

To disable the remote SMS cellular report action function, use **cellular_report action disable** command.

Synopsis

(config-sms-remote)# **cellular_report action disable**

Option Description	cellular_report action	Configure cellular report action
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# cellular_report action disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

start cellular_connection action enable

To enable the remote SMS start cellular connection action function, use **start cellular_connecction action enable** command.

Synopsis

(config-sms-remote)# **start cellular_connection action enable**

Option Description	start_cellular connection action	Configure start cellular connection action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# start_cellular_connection action enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

start cellular_connection action disable

To disable the remote SMS start cellular connection action function, use **start cellular_connecction action disable** command.

Synopsis

(config-sms-remote)# **start cellular_connection action disable**

Option Description	start_cellular connection action	Configure start cellular connection action
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# start_cellular_connection action disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

stop cellular_connection action enable

To enable the remote SMS stop cellular connection action function, use **stop cellular_connecction action enable** command.

Synopsis

(config-sms-remote)# **stop cellular_connection action enable**

Option Description	stop_cellular connection action	Configure stop cellular connection action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# stop_cellular_connection action enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

stop cellular_connection action disable

To disable the remote SMS stop cellular connection action function, use **stop cellular_connecction action disable** command.

Synopsis

(config-sms-remote)# **stop cellular_connection action disable**

Option Description	stop_cellular connection action	Configure stop cellular connection action
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# stop_cellular_connection action disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

switch_sim action enable

To enable the remote SMS switch SIM action function, use **switch_sim action enable** command.

Synopsis

(config-sms-remote)# **switch_sim action enable**

Option Description	switch_sim action	Configure switch SIM action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# switch_sim action enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

switch_sim action disable

To disable the remote SMS switch SIM action function, use **switch_sim action disable** command.

Synopsis

(config-sms-remote)# **switch_sim action disable**

Option Description	switch_sim action	Configure switch SIM action
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# sms router(config-sms)# router(config-sms)# remote_ctrl (config-sms-remote)# switch_sim action disable	
Error Messages	^Incomplete command	
Related Commands	show sms	

start_ipsec action enable

To enable the remote SMS start IPsec action function, use **start_ipsec action enable** command.

Synopsis

(config-sms-remote)# **start_ipsec action enable**

Option Description	start_ipsec action	Configure start IPsec action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# sms router(config-sms)# router(config-sms)# remote_ctrl (config-sms-remote)# start_ipsec action enable	
Error Messages	^Incomplete command	
Related Commands	show sms	

start_ipsec action disable

To disable the remote SMS start IPsec action function, use **start_ipsec action disable** command.

Synopsis

(config-sms-remote)# **start_ipsec action disable**

Option Description	start_ipsec action	Configure start IPsec action
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# start_ipsec action disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

stop_ipsec action enable

To enable the remote SMS stop IPsec action function, use **stop_ipsec action enable** command.

Synopsis

(config-sms-remote)# **stop_ipsec action enable**

Option Description	stop_ipsec action	Configure stop IPsec action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# stop_ipsec action enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

stop_ipsec action disable

To disable the remote SMS stop IPsec action function, use **stop_ipsec action disable** command.

Synopsis

(config-sms-remote)# **stop_ipsec action disable**

Option Description	stop_ipsec action	Configure stop IPsec action
	Disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# sms router(config-sms)# router(config-sms)# remote_ctrl (config-sms-remote)# stop_ipsec action disable	
Error Messages	^Incomplete command	
Related Commands	show sms	

set_DO_on action enable

To enable the remote SMS set DO on action function, use **set_DO_on action enable** command.

Synopsis

(config-sms-remote)# **set_DO_on action enable**

Option Description	set_DO_on action	Configure set DO on action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# sms router(config-sms)# router(config-sms)# remote_ctrl (config-sms-remote)# set_DO_on action enable	
Error Messages	^Incomplete command	
Related Commands	show sms	

set_DO_on action disable

To disable the remote SMS set DO on action function, use **set_DO_on action disable** command.

Synopsis

(config-sms-remote)# **set_DO_on action disable**

Option Description	set_DO_on action	Configure set DO on action
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# set_DO_on action disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

set_DO_off action enable

To enable the remote SMS set DO off action function, use **set_DO_off action enable** command.

Synopsis

(config-sms-remote)# **set_DO_off action enable**

Option Description	set_DO_off action	Configure set DO off action
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# set_DO_off action enable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

set_DO_off action disable

To disable the remote SMS set DO off action function, use **set_DO_off action disable** command.

Synopsis

(config-sms-remote)# **set_DO_off action enable**

Option Description	set_DO_off action	Configure set DO off action
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# sms` `router(config-sms)#` `router(config-sms)# remote_ctrl` `(config-sms-remote)# set_DO_off action disable`	
Error Messages	^Incomplete command	
Related Commands	show sms	

show sms

To show SMS configuration, use **show sms** command.

Synopsis

show sms

Option Description	show	Display the information
	sms	SMS configuration
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# show sms`	
Error Messages	^Incomplete command	
Related Commands	N/A	

SMS Notification

sms-warning phone_number

To configure SMS warning notification phone number settings, use **sms-warning phone_number** command.

Synopsis

(config)# **sms-warning phone_number_1/2/3/4** <STRING:name> <STRING:country> <STRING:phone>

Option Description	<string:name>	Input the name
	<string:country>	Input the country code
	<string:phone>	Input the phone number
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# sms-warning phone_number_1 test1 886 912345678 router(config)# sms-warning phone_number_2 test2 1 23456789 router(config)# sms-warning phone_number_3 test3 1 34567890 router(config)# sms-warning phone_number_4 test4 1 45678901 router(config)# exit	
Error Messages	^Incomplete command	
Related Commands	show sms-warning	

GNSS

enable

To enable GNSS, use **enable** command.

Synopsis

(config-gnss)# **gnss**

(config-gnss)# **enable**

(config-gnss)# **gnss_apply**

Option Description	gnss	Configure GNSS function
	enable	Enable the function
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# enable` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

disable

To disable GNSS, use **disable** command.

Synopsis

(config-gnss)# **gnss**

(config-gnss)# **disable**

(config-gnss)# **gnss_apply**

Option Description	gnss	Configure GNSS function
	disable	Enable the function
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# disable` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_client enable

To enable GNSS client, use **gnss_client enable** command.

Synopsis

(config-gnss)# **gnss_client enable**

(config-gnss)# **gnss_apply**

Option Description	gnss_client	Configure GNSS client function
	enable	Enable the function
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_client enable` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_client disable

To disable GNSS client, use **gnss_client disable** command.

Synopsis

(config-gnss)# **gnss_client disable**

(config-gnss)# **gnss_apply**

Option Description	gnss_client	Configure GNSS client function
	disable	Disable the function
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_client disable` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_client report_protocol tcp/udp

To configure GNSS client report protocol, use **gnss_client report protocol tcp/udp** command.

Synopsis

(config-gnss)# **gnss_client report_protocol tcp**

(config-gnss)# **gnss_client report_protocol udp**

(config-gnss)# **gnss_apply**

Option Description	gnss_client report	Configure GNSS client function
	tcp	TCP protocol
	udp	UDP protocol
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_client report_protocol tcp` `router(config-gnss)# gnss_client report_protocol udp` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_client host_address

To configure GNSS client report protocol, use **gnss_client report protocol tcp/udp** command.

Synopsis

(config-gnss)# **gnss_client host_address** <STRING:host_address>

(config-gnss)# **gnss_apply**

Option Description	gnss_client	Configure GNSS client function
	host_address	Host address
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_client host_address test1.com` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_client host_address port

To configure GNSS client host address port, use **gnss_client host_address port** command.

Synopsis

(config-gnss)# **gnss_client host_address port** <STRING:port_num>

(config-gnss)# **gnss_apply**

Option Description	gnss_client	Configure GNSS client function
	host_address	Host address
	<STRING:port_num>	Port number
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# gnss router(config-gnss)# gnss_client host_address port 1234 router(config-gnss)# gnss_apply	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_client report_id

To configure GNSS client report ID, use **gnss_client report_id** command.

Synopsis

(config-gnss)# **gnss_client report_id** <STRING:report_id>

(config-gnss)# **gnss_apply**

Option Description	gnss_client	Configure GNSS client function
	report_id	Configure report ID
	<STRING:report_id>	Report ID
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# gnss router(config-gnss)# gnss_client report_id 2345 router(config-gnss)# gnss_apply	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_server enable

To enable GNSS server, use **gnss_server enable** command.

Synopsis

(config-gnss)# **gnss_server enable**

(config-gnss)# **gnss_apply**

Option Description	gnss_server	Configure GNSS server function
	enable	Enable the function
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# gnss router(config-gnss)# gnss_server enable router(config-gnss)# gnss_apply	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_server disable

To disable GNSS server, use **gnss_server disable** command.

Synopsis

(config-gnss)# **gnss_server disable**

(config-gnss)# **gnss_apply**

Option Description	gnss_server	Configure GNSS server function
	disable	Disable the function
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# gnss router(config-gnss)# gnss_server disable router(config-gnss)# gnss_apply	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_server report_period

To configure GNSS server report period, use **gnss_server report_period** command.

Synopsis

(config-gnss)# **gnss_server report_period** <UINT:report_period>

(config-gnss)# **gnss_apply**

Option Description	gnss_server	Configure GNSS server function
	report_period	Configure report period
	<UINT:report_period>	Report period
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_server report_period 15` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_server port

To configure GNSS server port, use **gnss_server report** command.

Synopsis

(config-gnss)# **gnss_server port** <UINT:port_num>

(config-gnss)# **gnss_apply**

Option Description	gnss_server	Configure GNSS server function
	port	Configure server port
	<UINT:port_num>	Port number
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_server port 1234` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_client report_format

To configure GNSS client report format, use **gnss_client report_format** command.

Synopsis

(config-gnss)# **gnss_client report_format** <nmea | general>

(config-gnss)# **gnss_apply**

Option Description	gnss_client	Configure GNSS client function
	report_format	Configure report format
	nmea	NMEA format
	general	General format
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_client report_format nmea` `router(config-gnss)# gnss_client report_format general` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_server report_format

To configure GNSS server report format, use **gnss_server report_format** command.

Synopsis

(config-gnss)# **gnss_server report_format** <nmea | general>

(config-gnss)# **gnss_apply**

Option Description	gnss_server	Configure GNSS server function
	report_format	Configure report format
	nmea	NMEA format
	general	General format
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_server report_format nmea` `router(config-gnss)# gnss_server report_format general` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

gnss_server report_id

To configure GNSS server report ID, use **gnss_server report_id** command.

Synopsis

(config-gnss)# **gnss_server report_id** <STRING:report_id>

(config-gnss)# **gnss_apply**

Option Description	gnss_server	Configure GNSS server function
	report_id	Configure report ID
	<STRING:report_id>	Report ID
	gnss_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# gnss` `router(config-gnss)# gnss_server report_id 2345` `router(config-gnss)# gnss_apply`	
Error Messages	^Incomplete command	
Related Commands	show gnss	

Power Management

mode enable

To enable the power management mode, use **power_management** and **mode enable** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **mode enable**

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	mode	Configure power management mode
	enable	Enable the function
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `router(config-power_mgmt)# mode enable` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	
Error Messages	^Incomplete command	
Related Commands	show power_management	

mode disable

To disable the power management mode, use **power_management** and **mode disable** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **mode enable**

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	mode	Configure power management mode
	disable	Disable the function
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `router(config-power_mgmt)# mode disable` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	
Error Messages	^Incomplete command	

Related Commands	show power_management

mode scheduling

To enable the power management mode as scheduling, use **power_management** and **mode scheduling** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **mode scheduling**

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	mode	Configure power management mode
	scheduling	Set as scheduling mode
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `router(config-power_mgmt)# mode scheduling` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	
Error Messages	^Incomplete command	
Related Commands	show power_management	

mode ignition

To enable the power management mode as ignition, use **power_management** and **mode ignition** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **mode ignition**

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	mode	Configure power management mode
	ignition	Set as ignition mode
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `router(config-power_mgmt)# mode ignition` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	

Error Messages	^Incomplete command
Related Commands	show power_management

cycle hourly

To enable the power management mode as scheduling and use cycle hourly, use **power_management** and **cycle hourly** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **cycle hourly**

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	cycle hourly	Configure the schedule as cycle hourly
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `router(config-power_mgmt)# cycle hourly` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	
Error Messages	^Incomplete command	
Related Commands	show power_management	

cycle daily

To enable the power management mode as scheduling and use cycle daily, use **power_management** and **cycle daily** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **cycle daily**

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	cycle daily	Configure the schedule as cycle daily
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `router(config-power_mgmt)# cycle daily` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	

Error Messages	^Incomplete command
Related Commands	show power_management

cycle weekly

To enable the power management mode as scheduling and use cycle weekly, use **power_management** and **cycle weekly** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **cycle weekly**

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	cycle weekly	Configure the schedule as cycle weekly
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `router(config-power_mgmt)# cycle weekly` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	
Error Messages	^Incomplete command	
Related Commands	show power_management	

onetime

To enable the power management mode as one time, use **power_management** and **onetime** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **onetime**

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	onetime	Set the power management mode as one time
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `router(config-power_mgmt)# onetime` `router(config-power_mgmt-onetime)#` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	

Error Messages	^Incomplete command
Related Commands	show power_management

ignition wakeup_di high/low

To set the ignition wakeup DI as high or low, use **ignition wakeup_di high/low** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **ignition wakeup_di** <high | low>

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	ignition wakeup	Configure the ignition wake up DI function
	high	Set the ignition wakeup DI as high
	low	Set the ignition wakeup DI as low
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management` `(config-power_mgmt)# ignition wakeup_di high` `(config-power_mgmt)# ignition wakeup_di low` `router(config-power_mgmt)# power_mgmt_apply` `router(config-power_mgmt)#`	
Error Messages	^Incomplete command	
Related Commands	show power_management	

ignition di_sensing_time

To configure the ignition DI sensing time, use **ignition di_sensing_time** command.

Synopsis

(config)# **power_management**

(config-power_mgmt)# **ignition di_sensing_time** <UINT:time>

(config-power_mgmt)# **power_mgmt_apply**

Option Description	power_management	Configure power management function
	ignition	Configure the ignition function
	di_sensing_time	Configure the DI sensing time
	<UINT:time>	DI sensing time value
	power_mgmt_apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# power_management`	

	router(config-power_mgmt)# ignition di_sensing_time 2 router(config-power_mgmt)# power_mgmt_apply router(config-power_mgmt)#
Error Messages	^Incomplete command
Related Commands	show power_management

MRC

mrc enable

To enable MRC service, use **mrc enable** command.

Synopsis

(config-mrc)# **mrc enable**

Option Description	mrc	Configure MRC service
	enable	Enable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config-mrc)# mrc enable` `router(config)# exit`	
Error Messages	^Incomplete command	
Related Commands	show mrc	

mrc disable

To disable MRC service, use **mrc disable** command.

Synopsis

(config-mrc)# **mrc enable**

Option Description	mrc	Configure MRC service
	disable	Disable the function
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config-mrc)# mrc disable` `router(config)# exit`	
Error Messages	^Incomplete command	
Related Commands	show mrc	

Serial

interface serial

To configure serial interface, use **interface serial** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **apply**

Option Description	interface serial	Configure the serial interface
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

op_mode

To show the serial interface operation mode, use **op_mode** and **show** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **show**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	show	Display the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `router(config-if-serial-op_mode)# show`	
Error Messages	^Incomplete command	
Related Commands	N/A	

mode realcom

To configure the serial interface operation mode as RealCom, use **op_mode** and **realcom** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **mode realcom**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	mode realcom	Set the operation mode as RealCom
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `(config-if-serial-op_mode)# mode realcom`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

realcom tcp_chk_interval

To configure the RealCom TCP alive check interval, use **realcom tcp_chk_interval** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **realcom tcp_chk_interval** <UINT:tcp_chk_interval>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	realcom tcp_chk_interval	Configure RealCom TCP alive check interval
	<UINT:tcp_chk_interval>	Input the interval value
	apply	Apply settings
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `(config-if-serial-op_mode)# realcom tcp_chk_interval 15` `(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	

Related Commands	op_mode show

realcom max_conn

To configure the maximum number of RealCom connections, use **realcom max_conn** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **realcom max_conn** <UINT:max_conn>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	realcom max_conn	Configure the maximum number of Realcom connections: 1 to 2
	<UINT:max_conn>	Input the value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `(config-if-serial-op_mode)# realcom max_conn 10` `(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

realcom rts_signal H/L

To configure the RealCom RTS signal as High or Low, use **realcom rts_signal H/L** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **realcom rts_signal H**

(config-if-serial-op_mode)# **realcom rts_signal L**

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	realcom rts_signal H	Set RealCom RTS signal as High
	realcom rts_signal L	Set RealCom RTS signal as Low
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	

Usage Guidelines	N/A
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode (config-if-serial-op_mode)# realcom rts_signal H (config-if-serial-op_mode)# realcom rts_signal L (config-if-serial-op_mode)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

realcom dtr_signal H/L

To configure the RealCom DTR signal as High or Low, use **realcom dtr_signal H/L** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **realcom dtr_signal H**

(config-if-serial-op_mode)# **realcom dtr_signal L**

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	realcom dtr_signal H	Set RealCom DTR signal as High
	realcom dtr_signal L	Set RealCom DTR signal as Low
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode router(config-if-serial-op_mode)# realcom dtr_signal H router(config-if-serial-op_mode)# realcom dtr_signal L router(config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

mode rtc2217

To configure the serial interface operation mode as RTC2217, use **op_mode** and **mode rtc2217** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **mode rtc2217**

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	mode rtc2217	Set the operation mode as RTC2217
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `(config-if-serial-op_mode)# mode rtc2217` `(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

rfc2217 tcp_chk_interval

To configure the RFC2217 TCP alive check interval, use **rfc2217 tcp_chk_interval** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **rfc2217 tcp_chk_interval** <UINT:tcp_chk_interval>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	rfc2217 tcp_chk_interval	Configure RFC2217 TCP alive check interval
	<UINT:tcp_chk_interval>	Input the interval value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `router(config-if-serial-op_mode)# rfc2217 tcp_chk_interval 15`	

	router(config-if-serial-op_mode)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

rfc2217 tcp_data_port

To configure the serial interface RFC2217 TCP data port, use **rfc2217 tcp_data_port** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode) **rfc2217 tcp_data_port** <UINT:tcp_data_port>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	rfc2217 tcp_data_port	Configure RFC2217 TCP data port
	<UINT:tcp_data_port>	Input TCP data port
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode router(config-if-serial-op_mode)# rfc2217 tcp_data_port 2 router(config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

mode tcp_server

To configure the serial interface operation mode as TCP server, use **op_mode** and **mode tcp_server** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **mode tcp_server**

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	mode tcp_server	Set the operation mode as TCP server
	apply	Apply the setting
Defaults	N/A	

Command Modes	Global configuration
Usage Guidelines	N/A
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `(config-if-serial-op_mode)# mode tcp_server` `(config-if-serial-op_mode)# apply`
Error Messages	^Incomplete command
Related Commands	op_mode show

tcp_server tcp_chk_interval

To configure the TCP server TCP alive check interval, use **tcp_server tcp_chk_interval** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **tcp_server tcp_chk_interval** <UINT:tcp_chk_interval>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_server tcp_chk_interval	Configure TCP server TCP alive check interval
	<UINT:tcp_chk_interval>	Input the interval value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `router(config-if-serial-op_mode)# tcp_server tcp_chk_interval 10` `router(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

tcp_server rts_signal H/L

To configure the TCP server RTS signal as High or Low, use **tcp_server rts_signal H/L** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **tcp_server rts_signal H**

(config-if-serial-op_mode)# **tcp_server rts_signal L**

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_server rts_signal H	Set TCP server RTS signal as High
	tcp_server rts_signal L	Set TCP server RTS signal as Low
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `router(config-if-serial-op_mode)# tcp_server rts_signal H` `router(config-if-serial-op_mode)# tcp_server rts_signal L` `router(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

tcp_server dtr_signal H/L

To configure the TCP server DTR signal as High or Low, use **tcp_server dtr_signal H/L** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **tcp_server dtr_signal H**

(config-if-serial-op_mode)# **tcp_server dtr_signal L**

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_server dtr_signal H	Set TCP server DTR signal as High
	tcp_server dtr_signal L	Set TCP server DTR signal as Low
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	

Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode router(config-if-serial-op_mode)# tcp_server dtr_signal H router(config-if-serial-op_mode)# tcp_server dtr_signal L router(config-if-serial-op_mode)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

tcp_server tcp_data_port

To configure the serial interface TCP server TCP data port, use **tcp_server tcp_data_port** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode) **tcp_server tcp_data_port** <UINT:tcp_data_port>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_server tcp_data_port	Configure TCP server TCP data port
	<UINT:tcp_data_port>	Input TCP data port
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode router(config-if-serial-op_mode)# tcp_server tcp_data_port 2 router(config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

tcp_server tcp_com_port

To configure the serial interface TCP server TCP command port, use **tcp_server tcp_com_port** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode) **tcp_server tcp_cmd_port** <UINT:tcp_data_port>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_server tcp_cmd_port	Configure TCP server TCP command port
	<UINT:tcp_data_port>	Input TCP data port
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `router(config-if-serial-op_mode)# tcp_server tcp_cmd_port 4` `router(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

tcp_server serial_inactivity_time

To configure the serial interface TCP server inactivity time, use **tcp_server serial_inactivity_time** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode) **tcp_server serial_inactivity_time** <UINT:serial_inactivity_time>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_server serial inactivity time	Configure TCP server serial inactivity time
	<UINT:serial_inactivity_time>	Input serial inactivity time value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode`	

	(config-if-serial-op_mode)# tcp_server serial_inactivity_time 10 (config-if-serial-op_mode)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

tcp_server max_conn

To configure the TCP server maximum connection, use **tcp_server max_conn** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **tcp_server max_conn** <UINT:max_conn>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_server max_conn	Configure TCP server maximum connection
	<UINT:max_conn>	Input the value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode (config-if-serial-op_mode)# tcp_server max_conn 10 (config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

mode tcp_client

To configure the serial interface operation mode as TCP client, use **op_mode** and **mode tcp_client** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **mode tcp_client**

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	mode tcp_client	Set the operation mode as TCP client
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `(config-if-serial-op_mode)# mode tcp_client` `(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

tcp_client serial_inactivity_time

To configure the serial interface TCP client inactivity time, use **tcp_client serial_inactivity_time** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode) **tcp_client serial_inactivity_time** <UINT:serial_inactivity_time>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_client serial inactivity time	Configure TCP client serial inactivity time
	<UINT:serial_inactivity_time>	Input serial inactivity time value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode`	

	(config-if-serial-op_mode)# tcp_client serial_inactivity_time 10 (config-if-serial-op_mode)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

tcp_client conn_control

To configure the serial interface TCP client connection control, use **tcp_client conn_control** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode) **tcp_client conn_control** <0 to 6>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_client conn_control	Configure TCP client connection control
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode (config-if-serial-op_mode)# tcp_client conn_control 0 (config-if-serial-op_mode)# tcp_client conn_control 1 (config-if-serial-op_mode)# tcp_client conn_control 2 (config-if-serial-op_mode)# tcp_client conn_control 3 (config-if-serial-op_mode)# tcp_client conn_control 4 (config-if-serial-op_mode)# tcp_client conn_control 5 (config-if-serial-op_mode)# tcp_client conn_control 6 (config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

tcp_client tcp_chk_interval

To configure the TCP client TCP alive check interval, use **tcp_client tcp_chk_interval** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **tcp_client tcp_chk_interval** <UINT:tcp_chk_interval>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_client tcp_chk_interval	Configure TCP client TCP alive check interval
	<UINT:tcp_chk_interval>	Input the interval value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `router(config-if-serial-op_mode)# tcp_client tcp_chk_interval 10` `router(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

tcp_client dst add ip

To add an IP address to the TCP client destination, use **tcp_client dst add ip** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **tcp_client dst add ip** <STRING:ip>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_client dst add ip	Configure TCP client destination IP address
	<STRING:ip)	Input the IP address
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `(config-if-serial-op_mode)# tcp_client dst add ip 192.168.27.153`	

	config-if-serial-op_mode)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

tcp_client dst edit

To edit the TCP client destination IP, use **tcp_client dst edit** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **tcp_client dst edit** <UINT:idx>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_client dst edit	Edit the TCP client destination IP address
	<UINT:idx>	Input the IP address
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode (config-if-serial-op_mode)# tcp_client dst edit 192.168.27.157 config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

tcp_client dst del

To delete the TCP client destination IP, use **tcp_client dst del** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **tcp_client dst del** <UINT:idx>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	tcp_client dst del	Delete the TCP client destination IP address
	<UINT:idx>	Input the IP address
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode (config-if-serial-op_mode)# tcp_client dst del 192.168.27.157 config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

mode udp

To configure the serial interface operation mode as UDP, use **op_mode** and **mode udp** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **mode udp**

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	mode udp	Set the operation mode as UDP
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode (config-if-serial-op_mode)# mode udp (config-if-serial-op_mode)# apply	

Error Messages	^Incomplete command
Related Commands	op_mode show

udp udp_data_port

To configure the serial interface UDP data port, use **udp udp_data_port** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode) **udp udp_data_port** <UINT:udp_data_port>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	udp udp_data_port	Configure UDP data port
	<UINT:udp_data_port>	Input UDP data port
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `router(config-if-serial)# op_mode` `router(config-if-serial-op_mode)# udp udp_data_port 2` `router(config-if-serial-op_mode)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

udp dst add start_ip/end_ip/data_port

To configure the UDP destination IP range and data port, use **udp dst add start_ip/end_ip/data_port** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **udp dst add start_ip** <STRING:s_ip> **end_ip** <STRING:e_ip> **data_port** <UINT:data_port>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	udp dst add start_ip	Configure the UDP destination start IP address
	<STRING:s_ip)	Input the start IP address
	end_ip	Configure the UDP destination end IP address
	<STRING:e_ip)	Input the end IP address
	data_port	Configure the data port

	<UINT:data_port>	Input the data port
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode (config-if-serial-op_mode)# udp dst add start_ip 192.168.127.0 end_ip 192.168.127.255 data_port 10 config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

udp dst del

To delete the UDP destination IP, use **udp dst del** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **op_mode**

(config-if-serial-op_mode)# **udp dst del** <UINT:idx>

(config-if-serial-op_mode)# **apply**

Option Description	interface serial	Configure the serial interface
	op_mode	Configure operation mode
	udp dst del	Delete the UDP destination IP address
	<UINT:idx>	Input the IP address
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial router(config-if-serial)# op_mode (config-if-serial-op_mode)# udp dst del 192.168.27.157 config-if-serial-op_mode)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

interface serial/port/enable

To enable the serial interface, use **interface serial, port** and **enable** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **enable**

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	enable	Enable the setting
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# port` `(config-if-serial-port)# enable` `(config-if-serial-port)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

interface serial/port/disable

To disable the serial interface, use **interface serial, port** and **disable** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **disable**

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	disable	Disable the setting
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# port` `(config-if-serial-port)# disable` `(config-if-serial-port)# apply`	

Error Messages	^Incomplete command
Related Commands	op_mode show

interface serial/port/enable

To configure the serial port interface type, use **interface serial, port** and **interface_type** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **interface_type rs232**

(config-if-serial-port)# **interface_type rs422**

(config-if-serial-port)# **interface_type rs485-2**

(config-if-serial-port)# **interface_type rs485-4**

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	interface_type rs232	Set the interface type as RS-232
	interface_type rs422	Set the interface type as RS-422
	interface_type rs485-2	Set the interface type as RS-485 2-wire
	interface_type rs485-4	Set the interface type as RS-485 4-wire
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# port` `(config-if-serial-port)# interface_type rs232` `(config-if-serial-port)# interface_type rs422` `(config-if-serial-port)# interface_type rs485-2` `(config-if-serial-port)# interface_type rs485-4` `(config-if-serial-port)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

baud_rate

To configure the serial port baud rate, use **baud_rate** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **baud_rate** <UINT:baud_rate> (300 | 600 | 1200 | 1800 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 | 230400 | 460800 | 921600)

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	baud_rate	Configure the baud rate
	<UINT:baud_rate>	Input the baud rate value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# port` `(config-if-serial-port)# baud_rate 9600` `(config-if-serial-port)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

data_bit

To configure the serial port data bit, use **data_bit** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **data_bit** <UINT:data_bit> (5 | 6 | 7 | 8)

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	data_bit	Configure the data bit
	<UINT:data_bit>	Input the data bit value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# port`	

	(config-if-serial-port)# data_bit 8 (config-if-serial-port)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

stop_bit

To configure the serial port stop bit, use **stop_bit** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **stop_bit** <UINT:stop_bit> (1 | 1.5 | 2)

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	stop_bit	Configure the stop bit
	<UINT:stop_bit>	Input the stop bit value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial (config-if-serial)# port (config-if-serial-port)# stop_bit 2 (config-if-serial-port)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

parity

To configure the serial port parity, use **parity** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **parity** <none | odd | even >

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	parity	Configure the stop bit
	none	Set the parity as none
	odd	Set the parity as odd
	even	Set the parity as even
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# port` `(config-if-serial-port)# parity none` `(config-if-serial-port)# parity odd` `(config-if-serial-port)# parity even` `(config-if-serial-port)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

flow_control

To configure the serial port flow control, use **flow_control** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **flow_control** <none | rts_cts | xon_off >

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	flow_control	Configure the flow control
	none	Set the flow control as none
	rts/cts	Set the flow control as RTS/CTS
	xon_off	Set the flow control as XO/OFF
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	

Usage Guidelines	N/A
Examples	router# configure router(config)# interface serial (config-if-serial)# port (config-if-serial-port)# flow_control none (config-if-serial-port)# flow_control rts_cts (config-if-serial-port)# flow_control xon_off (config-if-serial-port)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

data_log enable/disable

To enable or disable the serial interface data log, use **data_log** and **enable/disable** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **data_log enable**

(config-if-serial-port)# **data_log disable**

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	data_log	Configure the data log
	enable	Enable the setting
	disable	Disable the setting
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial (config-if-serial)# port (config-if-serial-port)# data_log enable (config-if-serial-port)# data_log disable (config-if-serial-port)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

port_buffer enable/disable

To enable or disable the serial interface port buffer, use **port_buffer** and **enable/disable** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **port**

(config-if-serial-port)# **port_buffer enable**

(config-if-serial-port)# **port_buffer disable**

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	port	Configure the port
	port_buffer	Configure the port buffer
	enable	Enable the setting
	disable	Disable the setting
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# port` `(config-if-serial-port)# port_buffer enable` `(config-if-serial-port)# port_buffer disable` `(config-if-serial-port)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

data_pack/pkt_length

To configure the serial port data packet and the data packet length, use **data_pack** and **pkt_length** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **data_pack**

(config-if-serial-data_pack)# **pkt_length** <UINT:pkt_length>

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	data_pack	Configure the data packet
	pkt_length	Configure the data packet length
	<UINT:pkt_length>	Input the packet length value in bytes: 0 to 1024
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	

Examples	router# configure router(config)# interface serial (config-if-serial)# data_pack (config-if-serial-data_pack)# pkt_length 12 (config-if-serial-data_pack)# apply
Error Messages	^Incomplete command
Related Commands	op_mode show

data_pack/force_transmit_interval

To configure the serial port data packet and the force transmission interval, use **data_pack** and **force_transmit_interval** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **data_pack**

(config-if-serial-data_pack)# **force_transmit_interval** <UINT:force_transmit_interval>

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	data_pack	Configure the data packet
	force_transmit_interval	Configure the force transmission interval
	<UINT:force_transmit_interval>	Input the interval value in milliseconds: 0 to 65535
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# configure router(config)# interface serial (config-if-serial)# data_pack (config-if-serial-data_pack)# force_transmit_interval 10 (config-if-serial-data_pack)# apply	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

Delimiter1/2 enable/disable

To enable or disable the serial interface delimiter, use **delimiter** and **enable/disable** commands.

Synopsis

(config)# **interface serial**

(config-if-serial)# **data_pack**

(config-if-serial-data_pack)# **delimiter1 disable**

(config-if-serial-data_pack)# **delimiter1 enable**

(config-if-serial-data_pack)# **delimiter2 disable**

(config-if-serial-data_pack)# **delimiter2 enable**

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	data_pack	Configure the data pack
	delimiter	Configure the delimiter
	enable	Enable the setting
	disable	Disable the setting
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# data_pack` `(config-if-serial-data_pack)# delimiter1 disable` `(config-if-serial-data_pack)# delimiter1 enable` `(config-if-serial-data_pack)# delimiter2 disable` `(config-if-serial-data_pack)# delimiter2 enable` `(config-if-serial-data_pack)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

delimiter1/2 hex

To configure the serial port delimiter in hex format, use **delimiter hex** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **data_pack**

(config-if-serial-data_pack)# **delimiter1 hex** <STRING:hex_digit>

(config-if-serial-data_pack)# **delimiter2 hex** <STRING:hex_digit>

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	data_pack	Configure the data packet
	delimiter hex	Configure the delimiter in hex format
	<STRING:hex_digit>	Input the interval value
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# data_pack` `(config-if-serial-data_pack)# delimiter1 hex 2B` `(config-if-serial-data_pack)# delimiter2 hex 44` `(config-if-serial-data_pack)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

delimiter_process

To configure the serial port delimiter process, use **delimiter process** command.

Synopsis

(config)# **interface serial**

(config-if-serial)# **data_pack**

(config-if-serial-data_pack)# **delimiter_process delimiter**

(config-if-serial-data_pack)# **delimiter_process +1**

(config-if-serial-data_pack)# **delimiter_process +2**

(config-if-serial-data_pack)# **delimiter_process strip**

(config-if-serial-port)# **apply**

Option Description	interface serial	Configure the serial interface
	data_pack	Configure the data packet
	delimiter_process	Configure the delimiter process
	delimiter	Set delimiter as the delimiter process
	+1	Set +1 as the delimiter process
	+2	Set +2 as the delimiter process
	strip	Set strip as the delimiter process
	apply	Apply the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router# configure` `router(config)# interface serial` `(config-if-serial)# data_pack` `(config-if-serial-data_pack)# delimiter_process delimiter` `(config-if-serial-data_pack)# delimiter_process +1` `(config-if-serial-data_pack)# delimiter_process +2` `(config-if-serial-data_pack)# delimiter_process strip` `(config-if-serial-data_pack)# apply`	
Error Messages	^Incomplete command	
Related Commands	op_mode show	

IT SCATS System

For SCATS configurations, refer to the commands below.

show scatse.g

To show SCATS configurations and status, use this command.

Synopsis

show scatse.g

Option Description	show	Display configuration or status
	scatse.g	SCATS information
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	router# show scatse.g. ----- SCATS Settings SCATS Service: Disabled Serial Port Configuration HDLC-1200 : Enabled Non-HDLC-1200 : Disabled HDLC-9600 : Disabled Non-HDLC-300 : Disabled Authentication Server : 1. Addr: 192.168.0.1, Port: 2012 2. Addr: 192.168.0.12, Port: 2012 3. Addr: N/A, Port: N/A ----- SCATS Status Status : Service Disabled Regional Computer Information IP Addr: N/A Port: N/A Controller Information Site ID : N/A Using Config : N/A -----	
Error Messages	^Incomplete command	
Related Commands	N/A	

To enable/disable SCATS service, use this command.

Synopsis

router(config-if-serial-scats)# **enable/disable**

Option Description	enable	Enable SCATS service
	disable	Disable SCATS service
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router(config-if-serial-scats) enable`	
Error Messages	^Incomplete command	
Related Commands	N/A	

To enable/disable SCATS set configurations, use the commands below.

Synopsis

router(config-if-serial-scats)# **port_config** <enable | disable> $config_list

Option Description	port_config	Configure port setting
	enable	Enable SCATS service
	disable	Disable SCATS service
	$config_list	Select configuration options
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router(config-if-serial-scats)# port_config enable $config_list` `$config_list - Select the following options, separated by commas (e.g. 1,2,3):` `1) HDLC-1200` `2) Non-HDLC-1200` `3) HDLC-9600` `4) Non-HDLC-300`	
Error Messages	^Incomplete command	
Related Commands	N/A	

To delete Authentication Server settings, use this command.

Synopsis

router(config-if-serial-scats)# **auth_server delete** $idx

Option Description	auth_server	Configure authentication server
	delete	Delete the setting
	$idx	Index of Authentication Server (2-3)
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router(config-if-serial-scats)# auth_server delete $idx` `$idx - Index of Authentication Server setting, index:[2-3]`	
Error Messages	^Incomplete command	
Related Commands	N/A	

To edit Authentication Server settings, use this command.

Synopsis

router(config-if-serial-scats)# **auth_server edit** $idx $addr $port

Option Description	auth_server	Configure authentication server
	edit	Edit the setting
	$idx	Index of Authentication Server (1-3)
	$addr	Address of Authentication Server
	$port	Port of Authentication Server (1-65535)
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router(config-if-serial-scats)# auth_server edit $idx $addr $port` `$idx - Index of Authentication Server setting, index:[1-3]` `$addr - Address of Authentication Server` `$port - Port of Authentication Server, port:[1-65535]`	
Error Messages	^Incomplete command	
Related Commands	N/A	

To apply the SCATS settings, use this command.

Synopsis

router(config-if-serial-scats)# **apply**

Option Description	apply	Apply the settings
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router(config-if-serial-scats)#apply`	
Error Messages	^Incomplete command	
Related Commands	N/A	

To exit the SCATS settings, use this command.

Synopsis

router(config-if-serial-scats)# **exit**

Option Description	exit	Exit the setting
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	`router(config-if-serial-scats)#exit`	
Error Messages	^Incomplete command	
Related Commands	N/A	

7. 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.

8. 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 **layer2-filter** logging-capacity email-warning **layer2-filter** logging-capacity over-size-action overwrite-oldest **layer2-filter** logging-capacity over-size-action stop-recording **layer2-filter**	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 **l2-policy** <UINT:index> enable **l2-policy** <UINT:index> disable no **l2-policy** <UINT:index> logging-capacity snmp-trap-warning **layer2-policy** logging-capacity email-warning **layer2-policy** logging-capacity over-size-action overwrite-oldest **layer2-policy** logging-capacity over-size-action stop-recording **layer2-policy** logging-capacity <UINT:threshold> **layer2-policy**	V3.3

Index	Deprecated CLI	Fine-tuned CLI	Version Since
	logging-capacity <UINT:threshold> **layer2-filter** no logging-capacity snmp-trap-warning **layer2-filter** no logging-capacity email-warning **layer2-filter** no logging-capacity **layer2-filter**	no logging-capacity snmp-trap-warning **layer2-policy** no logging-capacity email-warning layer2-policy no logging-capacity **layer2-policy**	
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-**policy** log show logging event-log l2-**policy** // show l2-policy log with severity show logging event-log l2-**policy** severity <STRING:range> show l2-**policy** clear logging event-log l2-**policy**	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 **icmp-flood** <UINT:limit> no dos **icmp-flood** dos **tcp-sessions-without-syn** no dos **tcp-sessions-without-syn**	V3.3
6	ip dhcp-relay option82 remote-id-type ip	ip dhcp-relay option82 remote-id-type **interface** <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
8	(config-wan-backup)# interface <STRING:name> priority <UINT:priority> remotehostip <IPV4ADDR:ipaddr> (config-wan-backup)# no interface <STRING:name>	(config-wan-backup)# interface <STRING:name> enable (config-wan-backup)# no interface <STRING:name> enable (config-wan-backup)# interface <STRING:name> priority <UINT:priority> (config-wan-backup)# interface <STRING:name> remotehostip <IPV4ADDR:ipaddr>	V3.6
9	(config)# ip ping-response (config)# no ip ping-response	keep deprecated CLI	V3.12
10	(config)# warning-notification system-event firewall-policy-changed action <UINT:combination> (config)# warning-notification system-event firewall-policy-changed severity <UINT:type> (config)# warning-notification system-event firewall-policy-changed active	(config)# warning-notification system-event l3l7-policy-changed action <UINT:combination> (config)# warning-notification system-event l3l7-policy-changed severity <UINT:type> (config)# warning-notification system-event l3l7-policy-changed active (config)# no warning-notification system-event l3l7-policy-changed active	V3.14

Index	Deprecated CLI	Fine-tuned CLI	Version Since
	(config)# no warning-notification system-event firewall-policy-changed active		