NAT-108 CLI Command Set User Manual

Version 1.0, March 2025

www.moxa.com/products

NAT-108 CLI Command Set User Manual

Copyright Notice

Trademarks

Disclaimer

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Overview

Supported Series and Firmware Versions

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

Moxa Router Series	Firmware Version
NAT 108 Series	V3.16

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

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

Document Conventions

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

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

Notation	Description
Bold **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> |
{**scp** | **sftp**} <account> <password> <ip> <cfg-path-name>}

Restore configuration file:

copy { **tftp** <ip> **config-file** <cfg-path-name> |
{**scp** | **sftp**} <account> <password> <ip> **config-file** <cfg-path-name>}

Option Description	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-level>] |
privilege <privilege-level>}

(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

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 ---------- ---------- admin System admin configadmin Configuration admin user user test System admin	
Error messages	^Parse error	
	^Incomplete command	
Related Commands	username	

Password Policy

password-policy

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

Synopsis

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

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

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	
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}

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} [**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
	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)!!	
	% 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 Engine ID : 800021f3030090e8a9ed13 First Community : public Second Community : private Admin Auth. Type : md5 Admin Data Encryption Key : Enable ********* User Auth. Type : md5 User Data Encryption Key : Disable Trap Settings Trap Server 1 IP/Name : 9.1.1.1 Trap Server 2 IP/Name : 9.1.1.2 Trap Server 3 IP/Name : 9.1.1.3 Trap Community : public Trap Mode Mode : Trap V3 User : trapv3-user Auth : sha Priv : Enable Private MIB information Switch Object ID : enterprise.8691.6.100	
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	

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 ~ 12
	day	1 ~ 31
	year	2000 ~ 2037
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	

Examples	Set system time to Jan 31 , 2022 14:45:30.
	`router# configure`
	`router(config)# clock set 14:45:30 1 31 2022`
	`router(config)# exit`	

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	

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	

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	

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

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

Synopsis

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

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

Option Description	lan	Specifies LAN interface
	ip	IP address
	netmask	Subnet mask for this IP address
	enable	Enables specified accessible IP address
	disable	Disables specified accessible IP address
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.	

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`	

Error Messages	^Parse error	
	^Incomplete command	
Related Commands	show interfaces trusted-access settingcheck	

show interfaces trusted-access

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

Synopsis

show interfaces trusted-access

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`	

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 radius** global configuration command. To return to the default, use the **no** form of this command.

Synopsis

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

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

Option Description	server	Specifies RADIUS primary or backup servers
	primary	Specifies primary RADIUS authentication server
	server-ip	IP address of the RADIUS authentication server
	port	Specifies a port number of the remote RADIUS Server
	server-port	Port of the RADIUS authentication server, integer ranges from 1 to 65535, default value is 1812
	key	Specifies a shared-key of the remote RADIUS Server
	shared-key	Shared key of the RADIUS authentication server, 1 to 64 characters and must consist of the characters a-z, A-Z, 0-9 or - _ @ ! # $ % & * ( ) . + = { } [ ] | : ; , ~, and no spaces are allowed.
	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	N/A	

Examples	Specify and enable the primary RADIUS,Local 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 local`
	`router(config)# exit`	

Error Messages	% Radius index must be 1~2	
	% Must be greater than 0 and smaller than 65536	
	% The length of Shared Key must be greater than 0 and smaller than 65.	
	^Parse error	
	^Incomplete command	
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  : 192.168.1.5`
	`  Primary Server Port  : 2812`
	`  Primary Shared key  : ********`
	`  Backup Auth server  :`
	`  Backup Server Port  : 1812`
	`  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	
	% The length of Shared Key must be greater than 0 and smaller than 65.	
	% Timeout must be 5~120	
	% Retransmit must be 0~5	
	^Parse error	
	^Incomplete command	
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	

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.
	`router# show interfaces counters`
	`Port Tx Packets Rx Packets`
	`---- ---------- ----------`
	`1/ 1 0 0`
	`1/ 2 442490 673826`
	`1/ 3 0 0`
	`1/ 4 0 0`
	`1/ 5 0 0`
	`1/ 6 0 0`
	`1/ 9 0 0`
	`1/10 0 0`
	`1/11 0 0`
	`1/12 0 0`
	`1/13 0 0`
	`1/14 0 0`
	`1/15 0 0`
	`1/16 0 0`
	`Trk1 7273 6897`	

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) | 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 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) • 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`	

	% Invalid action value or non-support this combination action	

Error messages	% 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 | 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>]
sender <sender-email>}

(config)# **no email-warning** {**server** |
account |
sender |
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
	sender	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 sender 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	

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 }]

Option Description	dos	Enables/disables event logging for DoS function
	severity	Specifies severity of logging for DoS function
	severity-level	Specifies an integer for: {Emergency(0) | Alert(1) | Critical(2) | Error(3) | Warning(4) | Notice(5) | Information(6) | Debug(7)}
	flash	Specifies writing event logs into flash.
	syslog	Specifies sending event logs to syslog server
	trap	Specifies sending event logs via SNMP trap
	ipsec	Enables/disables event logging for IPsec function
	trusted-access	Enables/disables event logging for Trusted-Access function
	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}
	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)!!	
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 <2/4/6>

To configure traffic overload actions, use this command.

Synopsis

(config-if)# **warning-notification port-event event traffic-overload action <2/4/6>**

Option Description	N/A	
Defaults	Action Number: 0	
Command Modes	Global Configuration	
Usage Guidelines	Specified <Action number> must be 2 or 4 or 6, 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 <active)

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

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	

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> **message-format** { rfc3164 | rfc5424 }

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 support 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 support 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 support 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 support 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 support 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 support 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}	

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	

Tools

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	

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

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

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

Save and Exit DHCP pool configuration

(dhcp-config)# **exit**

Enable / Disable the DHCP pool

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

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
	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
	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)# exit`

Error Messages	% Invalid parameter!
	% Invalid Index
	% Please configure offered network first.
	^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**}

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

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
	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)# 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

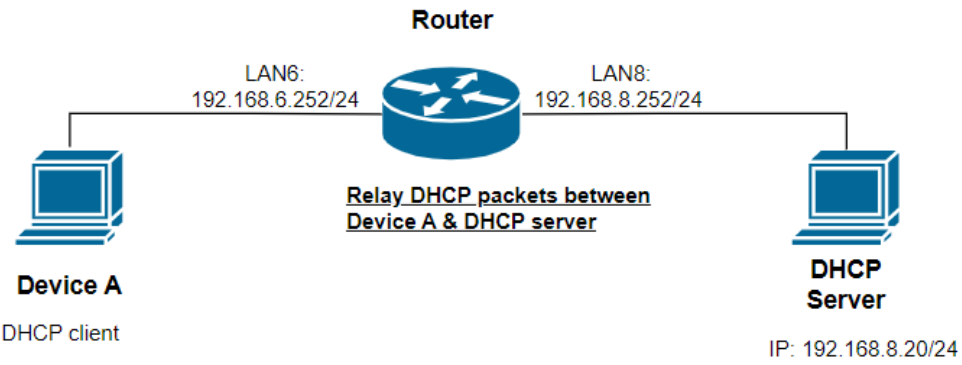
To enable a DHCP relay agent, use the **ip dhcp-relay** global configuration command. To disable DHCP relay agent, use **no** form of this command.

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**

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.
	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
	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)# 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.
	`router # show ip dhcp static`
	`Static DHCP Pool List`
	`----------`
	`Name : P6-static State : Enable`
	`Host IP Address : 192.168.6.1 Host Netmask : 255.255.255.0`
	`MAC Address : 00:90:E8:00:F2:AC Lease Time(min): 2880`
	`Default Gateway : 192.168.6.254 NTP Server : 192.168.8.9`
	`DNS Server 1 : 8.8.8.8 DNS Server 2 : 192.168.8.8`
	`----------`
	• Display dynamic DHCP client list.
	`router # show ip dhcp binding`
	`Name MAC Address IP Address Time Left`
	`---------- ---------- ---------- ----------`
	`Moxa-1 00:90:e8:00:00:41 192.168.5.1 44 h: 34 m: 25 s`	

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 : 7 State : Enable`
	`Static IP Address : 192.168.7.22 Netmask : 255.255.255.0`
	`Lease Time(min) : 1440`
	`Default Gateway : 192.168.7.252 NTP Server : 192.168.8.9`
	`DNS Server 1 : 8.8.8.8 DNS Server 2 : 192.168.8.8`
	`----------`	

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	

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	

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	

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

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	

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 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 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	
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 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`
	`IP Address: 192.168.2.254`
	`Subnet Mask: 255.255.255.0`
	`VLAN ID: 2`	

Error Messages	^Parse error	
	^Incomplete command	
Related Commands	interface vlan	

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.	

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	
Related Commands	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 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 Vlan ID : 3 Connect Mode : Enable Connect Type : Static IP Address : 192.168.3.154 Netmask : 255.255.255.0 Gateway : 0.0.0.0 PPTP Connection : Disable PPTP IP Address : 0.0.0.0 PPTP User Name : PPTP Password : ******** PPTP MPPE Encryption: Disable DNS Server : 0.0.0.0 0.0.0.0 0.0.0.0 • When the connection type is Dynamic IP, display current status. router# show interfaces wan status WAN Connect Type : DHCP IP Address : 10.123.24.12 Netmask : 255.255.252.0 Gateway : 10.123.24.1 DNS Server : 10.123.200.11 10.123.200.12 0.0.0.0	
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	
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	

Maximum Transmission Unit

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	

Routing

Unicast Route

ip route static

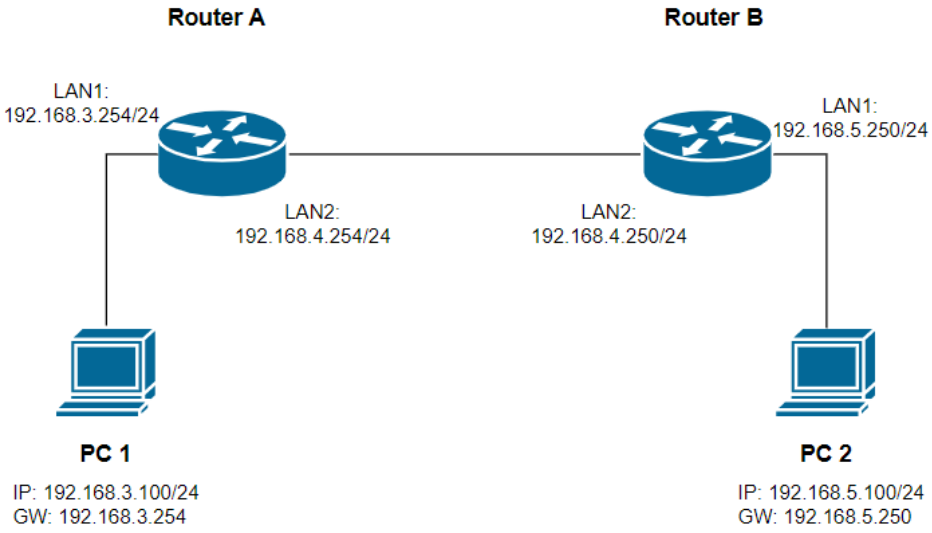
To create a static route entry, use the **ip route static** global configuration command. To delete the static route entry, use the **no** form of this command.

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

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	

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	
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	
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	
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	
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	
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 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 |
ip-twins-mapping}
(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**

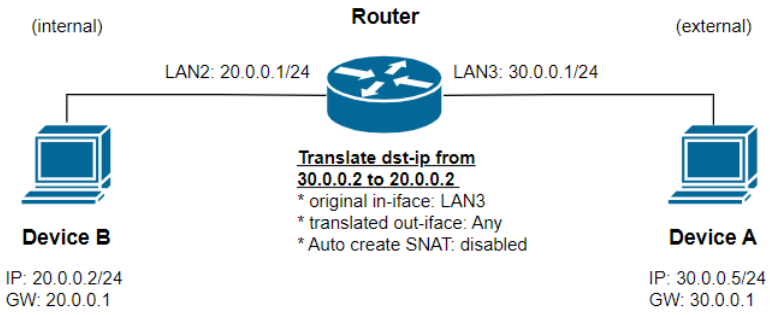
Show NAT configuration
(config-nat)# **show**

Abort NAT configuration
(config-nat)# **abort**

Save and Exit NAT configuration.
(config-nat)# **exit**

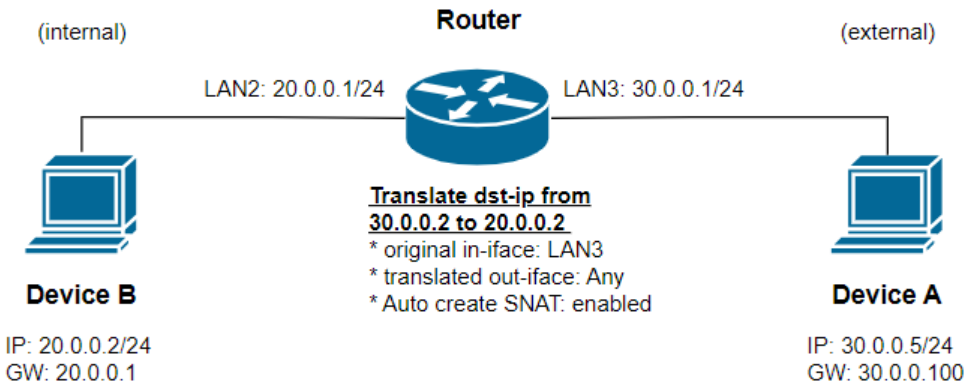
Option Description		
	nat-index	Index of existing NAT rule. The new NAT rule will be created at this position and original index after this value will be incremented by 1. If <nat-index> is not given, a new NAT rule will be created and appended to the end of the list.
	mode	Specifies the NAT mode selection
	1-1	1-to-1 NAT
	n-1	N-to-1 NAT
	pat	Port forward NAT
	advance	Advanced NAT
	ip-twins-mapping	IP Twins Mapping (duplicate IP mapping)
	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).

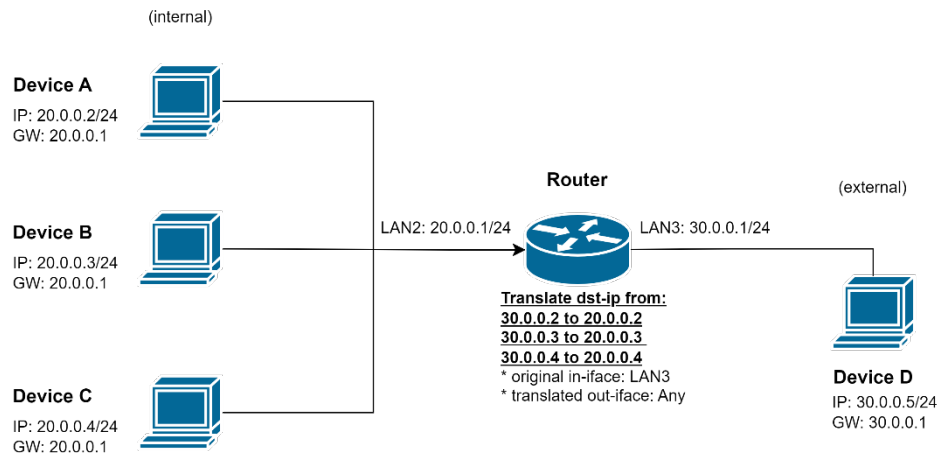
Commands:

```
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:

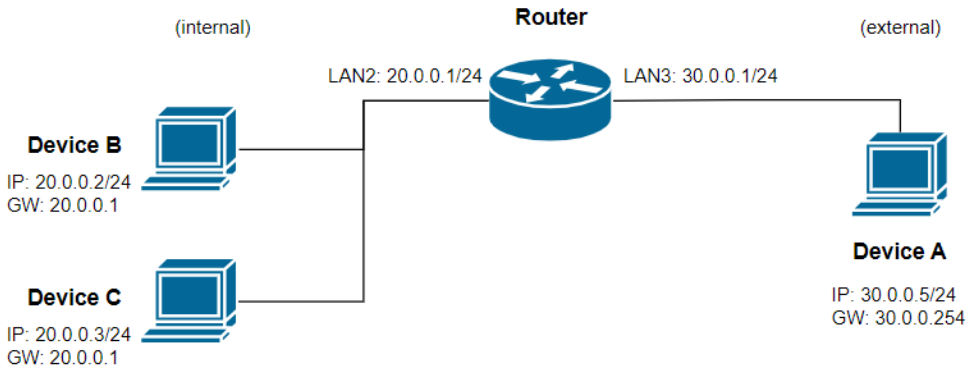
```
router# configure
router(config)# ip nat
router(config-nat)# mode 1-1
router(config-nat)# original in-iface LAN3 src-ip any src-port any
dst-ip 30.0.0.2-30.0.0.4 dst-port any
router(config-nat)# translated out-iface any src-ip any src-port any
dst-ip 20.0.0.2-20.0.0.4 dst-port any
router(config-nat)# 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:

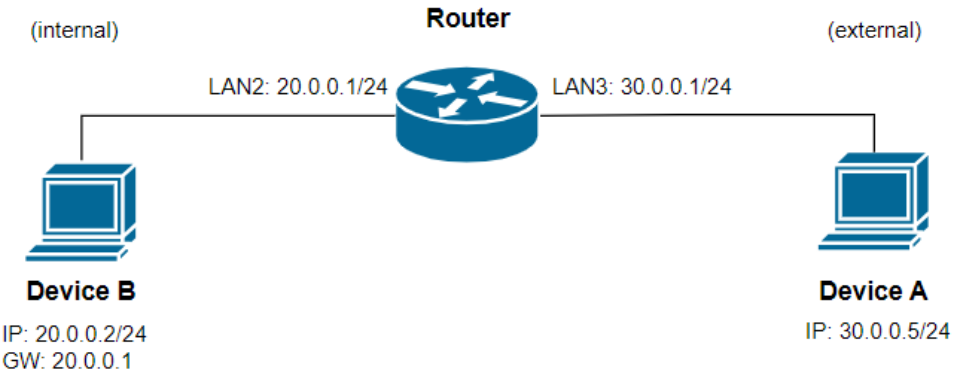
```
router# configure
router(config)# ip nat
router(config-nat)# mode n-1
router(config-nat)# original in-iface any src-ip 20.0.0.2-20.0.0.4
src-port any dst-ip any dst-port any
router(config-nat)# translated out-iface LAN3 src-ip any src-port any
dst-ip any dst-port any
router(config-nat)# desc n-1_example
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.

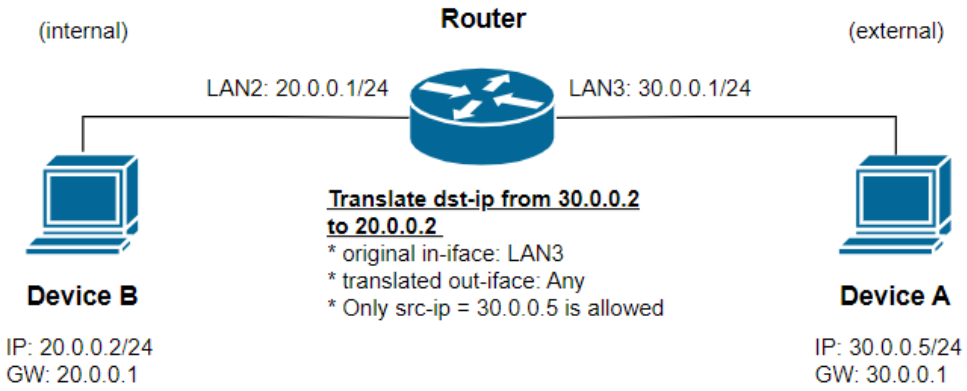
```
Commands:
router# configure
router(config)# ip nat
router(config-nat)# mode pat
router(config-nat)# original in-iface LAN3 src-ip any src-port any
dst-ip any dst-port 2222
router(config-nat)# translated out-iface any src-ip any src-port any
dst-ip 20.0.0.2 dst-port 22
router(config-nat)# protocol 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
```

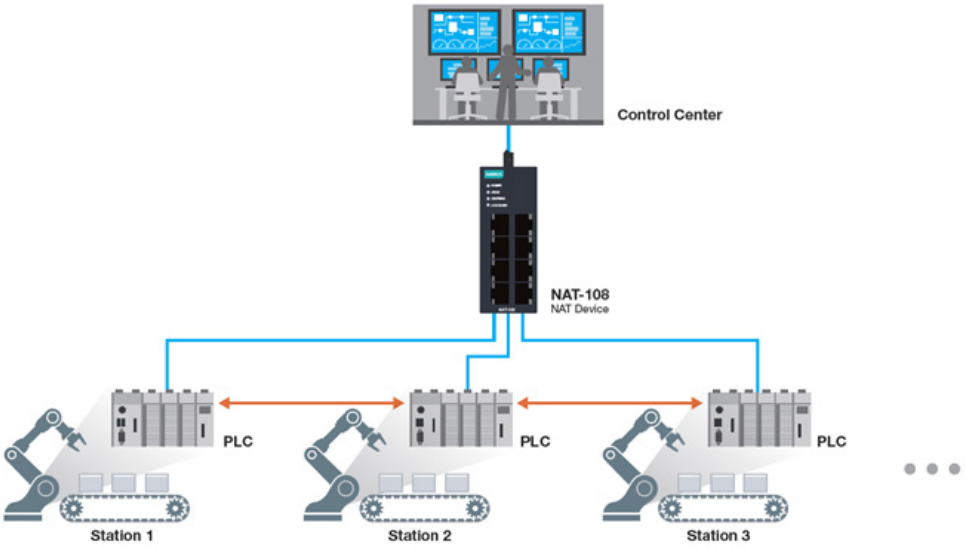
Apart from the aforementioned command, it is also necessary to manually create a secondary IP address (30.0.0.2) on LAN3:

```
router(config)# interface vlan 3
router(config-vif)# ip address   30.0.0.2 255.255.255.0 secondary
router(config-vif)# exit
```

Managing Multiple Devices with Identical LAN IPs Using IP Twins Mapping

In an industrial automation environment, multiple devices, such as PLCs, may be assigned identical LAN IP addresses due to factory default settings or operational constraints. In this scenario, Line1, Line2, and Line3 share the same LAN IP (192.168.1.1) but need to communicate independently with the control center.

To resolve this issue, IP Twins Mapping is used to differentiate identical LAN IPs by mapping them to unique external addresses before forwarding traffic to the control center.



Prerequisites:

The user must set a secondary IP

Commands:

Rule for Station1

```
router(config-nat)# mode ip-twins-mapping
router(config-nat)#set-out-iface "Control Center"
router(config-nat)# original in-iface "Station1" src-ip any src-port
any  dst-ip "Secondary IP Interface for Line 1" dst-port any

router(config-nat)# translated out-iface any src-ip any src-port any
dst-ip 192.168.1.1 dst-port any
router(config-nat)# no source-nat
router(config-nat)# exit
```

Rule for Station2

```
router(config-nat)# mode ip-twins-mapping
router(config-nat)#set-out-iface "Control Center"
```

	router(config-nat)# original in-iface "Station2" src-ip any src-port any dst-ip "Secondary IP Interface for Line 2" dst-port any router(config-nat)# translated out-iface any src-ip any src-port any dst-ip 192.168.1.1 dst-port any router(config-nat)# no source-nat router(config-nat)# exit # Rule for Station3 router(config-nat)# mode ip-twins-mapping router(config-nat)#set-out-iface "Control Center" router(config-nat)# original in-iface "Station3" src-ip any src-port any dst-ip "Secondary IP Interface for Line 3" dst-port any router(config-nat)# translated out-iface any src-ip any src-port any dst-ip 192.168.1.1 dst-port any router(config-nat)# no source-nat router(config-nat)# 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	
	% Invalid Index. It must be 1 - .	

Error Messages	^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	

Firewall

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

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	