



# CLI Reference Guide

# CONTENTS

<b>Preface .....</b>	<b>6</b>
<b>Chapter 1 Using the CLI .....</b>	<b>8</b>
1 Accessing the CLI.....	8
1.1.1 Logon by a console port.....	8
1.1.2 Logon by SSH .....	8
2 CLI Command Modes.....	10
3 Conventions.....	12
3.1.1 Format Conventions.....	12
3.1.2 Special Characters .....	12
3.1.3 Parameter Format .....	12
<b>Chapter 2 Public Commands.....</b>	<b>13</b>
2.1 help .....	13
2.2 exit.....	13
2.3 enable .....	14
2.4 disable .....	14
2.5 config .....	14
2.6 show history .....	15
2.7 clear history.....	15
2.8 reboot .....	16
2.9 show system-info.....	16
2.10 ping.....	17
2.11 tracert.....	17
<b>Chapter 3 User Management Commands.....</b>	<b>19</b>
3.1 local-user username password.....	19
<b>Chapter 4 DHCP Commands .....</b>	<b>20</b>
4.1 service dhcp server.....	20
4.2 ip dhcp server pool.....	20
4.3 ip-mask.....	21
4.4 vlan-id .....	22
4.5 lease .....	22
4.6 default-gateway.....	23
4.7 domain-name.....	23
4.8 dns-server.....	24
4.9 option.....	25

4.10 ip dhcp relay helper-address.....	26
4.11 show dhcp relay .....	26
4.12 show ip dhcp server pool .....	27
4.13 show ip dhcp server status.....	27
4.14 show dhcp server client-list .....	28
4.15 show dhcp server .....	28
<b>Chapter 5 Port Mirroring Commands .....</b>	<b>29</b>
5.1 monitor session enable .....	29
5.2 monitor session port.....	29
5.3 monitor session source port .....	30
5.4 monitor session mode .....	31
5.5 show monitor session .....	31
<b>Chapter 6 IEEE 802.1Q VLAN Commands.....</b>	<b>33</b>
6.1 vlan.....	33
6.2 router vlan .....	34
6.3 name.....	34
6.4 router port.....	35
6.5 switchport acceptable frame .....	35
6.6 interface.....	36
6.7 description.....	36
6.8 switchport pvid.....	37
6.9 show interface .....	37
6.10 show vlan summary .....	38
6.11 show vlan .....	38
6.12 show interface status .....	39
<b>Chapter 7 NAT Commands.....</b>	<b>40</b>
7.1 show nat one-to-one .....	40
7.2 show nat virtual-server .....	40
7.3 show nat alg.....	41
7.4 nat one-to-one .....	41
7.5 interface one-to-one .....	42
7.6 original-ip.....	42
7.7 translated-ip.....	43
7.8 dmz forwarding .....	44
7.9 description-one .....	44
7.10 nat virtual-server.....	45
7.11 interface virtual-server.....	45

7.12 external port .....	46
7.13 internal port.....	47
7.14 internal server-ip.....	47
7.15 protocol.....	48
7.16 nat alg.....	48
<b>Chapter 8 Static Routing Commands .....</b>	<b>50</b>
8.1 show ip route static .....	50
8.2 ip route.....	50
8.3 no ip route .....	51
<b>Chapter 9 RIP Commands .....</b>	<b>52</b>
9.1 router rip .....	52
9.2 rip version.....	52
9.3 rip distance .....	53
9.4 auto-summary .....	53
9.5 timers basic update.....	54
9.6 timers basic timeout .....	54
9.7 timers basic garbage-collect .....	55
9.8 no timers basic .....	55
9.9 rip network .....	56
9.10 ip rip send version .....	56
9.11 ip rip receive version .....	57
9.12 ip rip split-horizon.....	58
9.13 ip rip poison-reverse .....	58
9.14 ip rip authentication-mode .....	59
9.15 show ip rip.....	59
<b>Chapter 10 OSPF Commands.....</b>	<b>61</b>
10.1 router ospf.....	61
10.2 router-id .....	61
10.3 area-id.....	62
10.4 compatible rfc1583 .....	62
10.5 ospf-network.....	63
10.6 ospf-distance.....	63
10.7 timers throttle spf.....	64
10.8 maximum-paths .....	65
10.9 passive-interface default .....	65
10.10 ip ospf priority .....	66
10.11 ip ospf hello-interval .....	66

10.12 ip ospf dead-interval.....	67
10.13 ip ospf transmit-delay .....	67
10.14 ip ospf retransmit-interval.....	68
10.15 ip ospf cost.....	68
10.16 ip ospf passive .....	69
10.17 ip ospf mtu-ignore .....	69
10.18 ip ospf authentication .....	70
10.19 ip ospf network .....	71
10.20 show ip ospf database.....	71
10.21 show ip ospf neighbor.....	72
10.22 show ip ospf interface.....	72
10.23 show ip ospf .....	73
10.24 show network .....	73
<b>Chapter 11 IPSec Commands .....</b>	<b>74</b>
11.1 crypto policy.....	74
11.2 hash.....	74
11.3 encryption .....	75
11.4 group .....	76
11.5 exchange-mode .....	76
11.6 ike-lifetime.....	77
11.7 crypto isakmp key .....	77
11.8 dpd .....	78
11.9 dpd-interval.....	79
11.10 crypto ipsec transform-set.....	79
11.11 lifetime.....	80
11.12 encapsulation-mode .....	81
11.13 pfs .....	81
11.14 crypto map .....	82
11.15 set peer .....	82
11.16 set transform-set.....	83
11.17 localsubnet.....	84
11.18 remotesubnet.....	84
11.19 negotiation-mode.....	85
11.20 ipsec map.....	85
11.21 show policy.....	86
11.22 show transform-set .....	87
11.23 show crypto map .....	87
11.24 show crypto ipsec sa.....	88

<b>Chapter 12 ACL Commands .....</b>	<b>89</b>
12.1 show access-list .....	89
12.2 access-list ip .....	89
<b>Chapter 13 SSH Commands .....</b>	<b>92</b>
13.1 show ssh configuration .....	92
13.2 ssh server .....	92
<b>Chapter 14 SNMP Commands.....</b>	<b>94</b>
14.1 snmp-server v3 .....	94
14.2 snmp-server v1-v2c .....	94
14.3 snmp-server v1-v2c host.....	95
14.4 snmp-server v1-v2c contact .....	96
14.5 snmp-server v1-v2c device-name .....	96
14.6 snmp-server v1-v2c community .....	97
14.7 snmp-server v1-v2c location .....	97
14.8 show snmp-server .....	98
<b>Chapter 15 HTTP and HTTPS Commands.....</b>	<b>99</b>
15.1 ip http port.....	99
15.2 ip http server redirect-to-https.....	99
15.3 ip http secure-port.....	100
15.4 ip http secure-server .....	100
15.5 ip http session timeout.....	101
15.6 show ip http configuration .....	101
<b>Chapter 16 Time Management Commands.....</b>	<b>103</b>
16.1 show time-range .....	103
16.2 time-range week- date time-slice.....	103
16.3 show system-time.....	104
16.4 system-time manual.....	105
16.5 system-time ntp timezone server .....	105
<b>Chapter 17 ARP Commands .....</b>	<b>108</b>
17.1 show arp.....	108

# Preface

This Guide is intended for network administrator to provide referenced information about CLI (Command Line Interface). The device mentioned in this Guide stands for Omada Business Router that supports the CLI function without any explanation. Some models featured in this guide may be unavailable in your country or region. For local sales information, visit <https://www.tp-link.com>.

## Overview of this Guide

### Chapter 1: Using the CLI

About how to use the CLI, CLI Command Modes, and some Conventions.

### Chapter 2: Public Commands

About the commands relating to general operations, such as viewing the available commands, rebooting the device, and testing the network connectivity.

### Chapter 3: User Management Commands

About the commands used for user management.

### Chapter 4: DHCP Commands

About the commands used for DHCP settings.

### Chapter 5: Port Mirroring Commands

About the commands used for configuring the Port Mirror function.

### Chapter 6: IEEE 802.1Q VLAN Commands

About the commands used for configuring IEEE 802.1Q VLAN.

### Chapter 7: NAT Commands

About the commands used for configuring the NAT.

### Chapter 8: Static Routing Commands

About the commands used for configuring the static routing rules.

### Chapter 9: RIP Commands

About the commands used for configuring the RIP function.

### Chapter 10: OSPF Commands

About the commands used for configuring the OSPF function.

### Chapter 11: IPSec Commands

About the commands used for configuring the IPSec settings.

### Chapter 12: ACL Commands

About the commands used for configuring the ACL.

**Chapter 13: SSH Commands**

About the commands used for configuring the SSH settings.

**Chapter 14: SNMP Commands**

About the commands used for configuring the SNMP settings.

**Chapter 15: HTTP and HTTPS Commands**

About the commands used for configuring the HTTP and HTTPS logon.

**Chapter 16: Time Management Commands**

About the commands used for the time-range settings, and the system time settings.

**Chapter 17: ARP Commands**

About the commands used for the ARP function.



# Chapter 1 Using the CLI

## 1 Accessing the CLI

You can log on to the router and access the CLI by the following two methods.

- 1 Logon Via the Console Port (Only for certain models).
- 2 Logon By SSH.

### 1.1.1 Logon by a console port



**Note:** Console port is only available on certain devices.

#### ■ Console Port

Some models are equipped with an RJ-45 console port. Take the following steps to log on to the device via the console port.

1. Connect the Console port of the router to the management PC using an RJ45 console cable.
2. Start the terminal emulation program (such as the HyperTerminal) on the PC and configure the terminal emulation program as follows:
  - Baud rate: 115200 bps
  - Data bits: 8
  - Parity: none
  - Stop bits: 1
  - Flow control: none
3. In the Hyper Terminal main window, press **Enter** and ">" will appear, indicating that you have successfully logged in to the router and you can use the CLI now.



**Note:** The username "admin" in the figure above is for demonstration only. Please enter the username and password according to the real situation.

### 1.1.2 Logon by SSH

To log on by SSH, you are recommended to use the software PuTTY via password authentication. You need to first prepare the username and password you set for logging in to the router's web management page.



**Note:**

Before SSH login, you should enable **Remote Assistance** for the router. Follow the steps:

1. Go to the router's management page.
2. Go to **System Tools > Diagnostics > Remote Assistance**
3. In Remote Assistance section, enable **Remote Assistance**, and click **Save**.

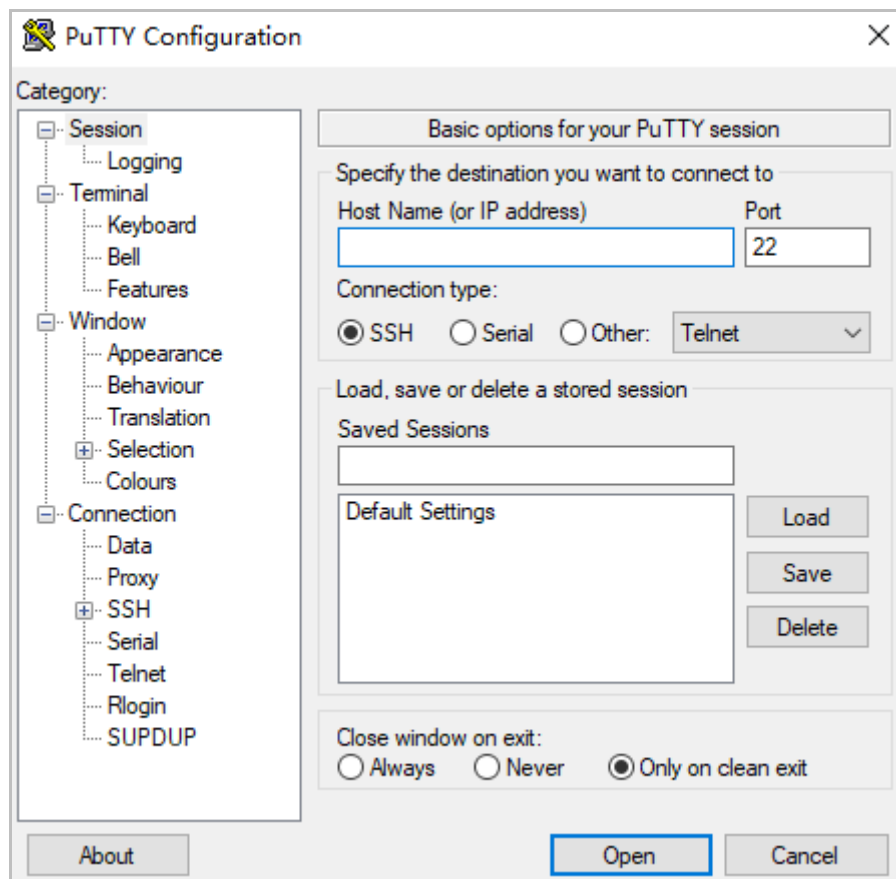
Remote Assistance

It is recommended not to enable Remote Assistance. Enable this function with the help of technicians if needed.

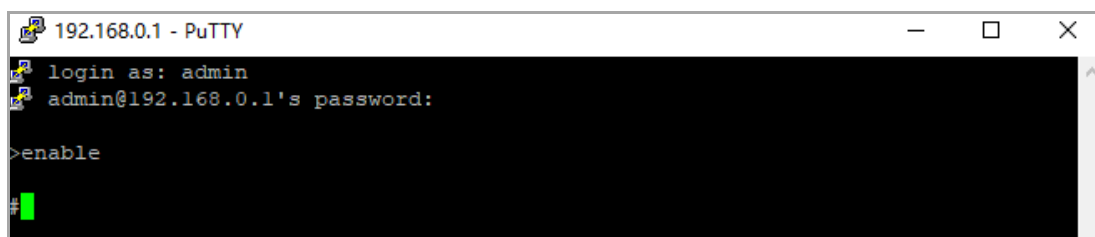
Remote Assistance:  Enable

Save

1. Open the software to log on to the interface of PuTTY. Enter the IP address of the router into **Host Name** field; keep the default value 22 in the **Port** field; select **SSH** as the Connection type.



2. Click the **Open** button in the above figure to log on to the router. Enter the login user name and password to log on the router, and then enter **enable** to go to Public Mode, so you can continue to configure the router.



## 2 CLI Command Modes

The CLI is divided into three main modes: **User EXEC Mode**, **Public Mode**, and **Global Configuration Mode**. Global Configuration Mode is further divided into various subsidiary modes including Config DHCP Mode, Config VLAN Mode, Interface Mode Config NAT OTO Mode, Config NAT VS Mode, Config RIP Mode, OSPF Mode, IPSEC\_ISAKMP Mode, IPSEC\_TRANSFORM Mode, and IPSEC\_MAP Mode.

For the main modes, the accessing path, prompt, and ways to log out or access the next mode are presented below:

Mode	Accessing path	Prompt	Logout or access the subsidiary mode
User EXEC Mode	Primary mode once you log in to the CLI interface.	>	No exit. Use the <b>enable</b> command to go to Public Mode.
Public Mode	Use the <b>enable</b> command to enter this mode from User EXEC Mode.	#	Enter the <b>disable</b> or the <b>exit</b> command to return to User EXEC Mode. Enter <b>configure</b> command to access Global Configuration Mode.
Global Configuration Mode	Use the <b>config</b> command to enter this mode from Public Mode.	(config)#	Use the <b>exit</b> command or press <b>Ctrl+Z</b> to return to Public Mode. To go to the subsidiary modes, refer to specific commands: <a href="#">4.2 ip dhcp server pool</a> <a href="#">6.2 router vlan</a> <a href="#">6.4 router port</a> <a href="#">6.6 interface</a> <a href="#">7.4 nat one-to-one</a> <a href="#">7.10 nat virtual-server</a> <a href="#">9.1 router rip</a> <a href="#">10.1 router ospf</a> <a href="#">11.1 crypto policy</a> <a href="#">11.10 crypto ipsec transform-set</a> <a href="#">11.14 crypto map</a>

 **Note:**

1. The user is automatically in User EXEC Mode after the connection between the PC and the router is established by an SSH connection.
2. Each command mode has its own set of specific commands. To configure some commands, you should access the corresponding command mode firstly.
3. Some commands can be performed in all modes.

## 3 Conventions

### 3.1.1 Format Conventions

The following conventions are used in this Guide:

- Items in square brackets [] are optional
- Items in braces {} are required
- Alternative items are grouped in braces and separated by vertical bars. For example: **speed** {10 | 100 | 1000 }
- Bold indicates an unalterable keyword. For example: **show logging**
- Normal Font indicates a constant (several options are enumerated and only one can be selected). For example: **mode** {dynamic | static | permanent}
- Italic Font indicates a variable (an actual value must be assigned). For example: **bridge aging-time** *aging-time*

### 3.1.2 Special Characters

- These six characters " < > , \ & cannot be input.
- Special characters in this guide are the space and the question mark. Typing a space means you are about to enter the next parameter or command. Enter a question mark in the position of a parameter, and a tip will appear, indicating what you are supposed to type in. You can't use the space and the question mark as a username or password.

### 3.1.3 Parameter Format

Some parameters must be entered in special formats which are shown as follows:

- MAC address must be enter in the format of xx:xx:xx:xx:xx:xx.
- One or several values can be typed for a port-list or a vlan-list using comma to separate. Use a hyphen to designate a range of values. For example: **(config)#monitor session 1 source port 2, 3-5**

## Chapter 2 Public Commands

### 2.1 help

#### Description

The **help** command is used to view all the available commands of the current mode.

#### Syntax

**help**

#### Command Mode

All

#### Example

View the available commands of the Global Configuration Mode:

```
>enable  
#config  
(config)#help
```

### 2.2 exit

#### Description

The **exit** command is used to return to the previous mode from the current mode.

#### Syntax

**exit**

#### Command Mode

All

#### Example

Return to Public Mode from Global Configuration Mode:

```
(config)#exit
```

## 2.3 enable

### Description

The **enable** command is used to access Public mode from User EXEC mode.

### Syntax

**enable**

### Command Mode

User EXEC Mode

### Example

Go to Public Mode from User EXEC Mode:

```
>enable
```

## 2.4 disable

### Description

The **disable** command is used to return to the User EXEC mode from Public mode.

### Syntax

**disable**

### Command Mode

Public Mode

### Example

Return to the User EXEC Mode from Public Mode :

```
#disable
```

## 2.5 config

### Description

The **config** command is used to enter the Global Configuration mode from the Public mode.

### Syntax

**config**

## Command Mode

Public Mode

## Example

Enter the Global Configuration Mode from the Public Mode:

```
#config
```

## 2.6 show history

### Description

The **show history** command is used to display the latest 20 commands you have entered.

### Syntax

```
show history
```

### Command Mode

All

### Example

In Public Mode, view the history command you have entered:

```
>enable  
#show history
```

## 2.7 clear history

### Description

The **clear history** command is used to clear the commands history. Therefore, these commands will not appear next time you use the **show history** command.

### Syntax

```
clear history
```

### Command Mode

All



## Example

In Public Mode, clear the commands you have entered:

```
>enable  
#clear history
```

## 2.8 reboot

### Description

The **reboot** command is used to reboot your router. To avoid damage, please don't turn off the device while rebooting.

### Syntax

```
reboot
```

### Command Mode

Public Mode

### Example

To reboot your device:

```
>enable  
#reboot  
This will reboot device. Continue? (Y/N): Y
```

## 2.9 show system-info

### Description

The **show system-info** command is used to display System Description, System Name, Contact Information, Hardware Version, Firmware Version, Mac Address, System Time, Running Time, etc.

### Syntax

```
show system-info
```

### Command Mode

All

## Example

View the system information of your router:

```
(config)#show system-info
```

## 2.10 ping

### Description

The **ping** command is used to test the connectivity between the router and the tested host and measure the round-trip time. Only IPv4 addresses are supported.

### Syntax

```
ping address
```

### Parameter

*address* —— Enter the IPv4 address of the tested host.

### Command Mode

Public Mode

### Example

To test the connectivity between the router and a tested host (e.g., 192.168.0.100) through the **ping** command:

```
>enable  
#ping 192.168.0.100
```

## 2.11 tracert

### Description

The **tracert** command is used to display the route (path) your router has passed to reach the tested host and measure transit delays of packets across an Internet Protocol network. Only the IPv4 addresses are supported.

### Syntax

```
tracert address
```

### Parameter

*address* —— Enter the IPv4 address of the tested host.

## Command Mode

Public Mode

## Example

To test the connectivity between the router and a tested host (e.g., 192.168.0.100) through the **tracert** command:

```
>enable  
# tracert 192.168.0.100
```

## Chapter 3 User Management Commands

### 3.1 local-user username password

#### Description

The **local-user username password** command is used to set a new username or password for you to log in to the router. Using this command will make the SSH to reload.

#### Syntax

**local-user username** *username* **password** *password*

#### Parameter

*username* — Specify a username for the local user account (1-64 letters, digits or special characters).

*password* — Specify a password for the local user account (6-64 letters, digits or special characters).

#### Command Mode

Global Configuration Mode

#### Example

Set the username as "admin", and the password as "12345678":

```
(config)#local-user username admin password 12345678
```

## Chapter 4 DHCP Commands

DHCP (Dynamic Host Configuration Protocol) is a network configuration protocol for hosts on TCP/IP networks, and it provides a framework for distributing configuration information to hosts. DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them.

### 4.1 service dhcp server

#### Description

The **service dhcp server** command is used to enable DHCP service. To disable DHCP service, please use the **no service dhcp server** command.

#### Syntax

```
service dhcp server  
no service dhcp server
```

#### Command Mode

Global Configuration Mode

#### Example

Enable DHCP server of the router:

```
(config)#service dhcp server
```

### 4.2 ip dhcp server pool

#### Description

The **ip dhcp server pool** command is used to create an address pool of the DHCP server and enter the Config DHCP Server mode. You should set the network address, subnet mask, and VLAN ID for an address pool in the config-dhcp-server mode for it to work. An unfinished address pool will be saved into the cache, and you can continue to configure it using the **ip dhcp server pool** command. Likewise, the **ip dhcp server pool** command allows you to edit the existing address pools.

To delete an address pool, please use the **no ip dhcp server pool** command.

#### Syntax

```
ip dhcp server pool pool-name  
no ip dhcp server pool pool-name
```

## Parameter

*pool-name* — Enter the address pool name within 40 characters with letters, numbers, or underscores.

## Command Mode

Global Configuration Mode

## Example

Create an address pool named "P1":

```
(config)#ip dhcp server pool P1
```

# 4.3 ip-mask

## Description

The **ip-mask** command is used to specify the network address and subnet mask of the network pool. It is one of the prerequisites for a newly created address pool to take effect.

## Syntax

```
ip-mask {network-address} {subnet-mask}
```

## Parameter

*network-address* — Specify the network address of the pool, with the format A.B.C.D. All the IP addresses in the same subnet are allocable except the reserved addresses and specific addresses.

*subnet-mask* — Specify the subnet mask of the pool, with the format A.B.C.D.

## Command Mode

Config DHCP Server Mode

## Example

For address pool "P1", set its network address as "192.168.3.1", and the subnet mask as "255.255.255.0":

```
(config)#ip dhcp server pool P1  
(config-dhcp-server)#ip-mask 192.168.3.1 255.255.255.0
```

## 4.4 vlan-id

### Description

The **vlan-id** command is used to set a VLAN for a DHCP server. It is one of the prerequisites for a newly created address pool to take effect.

### Syntax

```
vlan-id vlan-id
```

### Parameter

*vlan-id* — Specify the VLAN ID for the DHCP server. The value ranges from 1 to 4094.

### Command Mode

Config DHCP Server Mode

### Example

Set the VLAN of the address pool "P1" as "2":

```
(config)#ip dhcp server pool P1  
(config-dhcp-server)#vlan-id 2
```

## 4.5 lease

### Description

The **lease** command is used to specify the lease time for DHCP clients. Lease time defines how long the clients can use the IP address assigned by the DHCP server. Generally, the client will automatically request the DHCP server for extending the lease time before the lease expired. If the request failed, the client will have to stop using that IP address when the lease finally expired, and try to get a new IP address from the other DHCP servers.

### Syntax

```
lease lease-time
```

### Parameter

*lease-time* — Specify the lease time ranging from 1 to 2880 minutes. The default value is 120 minutes.

### Command Mode

Config DHCP Server Mode

## Example

Specify the lease time of address pool "P1" as "180" minutes:

```
(config)#ip dhcp server pool P1
(config-dhcp-server)#lease 180
```

## 4.6 default-gateway

### Description

The **default-gateway** command is used to specify the default gateway for the address pool. To delete the configuration, please use the **no default-gateway** command.

### Syntax

```
default-gateway gateway
no default-gateway
```

### Parameter

*gateway*—— Enter the default gateway for the address pool.

### Command Mode

Config DHCP Server Mode

### Example

For the address pool *P1*, set its default gateway as "192.168.3.1":

```
(config)#ip dhcp server pool P1
(config-dhcp-server)#default-gateway 192.168.3.1
```

## 4.7 domain-name

### Description

The **domain-name** command is used to specify the domain name for the DHCP client. To delete the domain name, please use the **no domain-name** command.

### Syntax

```
domain-name domainname
no domain-name
```



## Parameter

*domainname* — Specify the domain name for the DHCP client.

## Command Mode

Config DHCP Server Mode

## Example

For address pool "P1", specify its DHCP client's domain name as "example.com":

```
(config)#ip dhcp server pool P1
(config-dhcp-server)#domain-name example.com
```

# 4.8 dns-server

## Description

The **dns-server** command is used to specify the DNS server of the address pool. To delete this configuration, please use the **no dns-server** command.

## Syntax

```
dns-server {dns1 primarydns | dns2 secondarydns}
no dns-server
```

## Parameter

*primarydns* — Enter the primary DNS server address provided by your ISP. If you are not sure, please consult your ISP.

*secondarydns* — Enter the secondary DNS server address provided by your ISP. If you are not sure, please consult your ISP.

## Command Mode

Config DHCP Server Mode

## Example

For address pool "P1", specify its primary DNS as "192.168.0.1":

```
(config)#ip dhcp server pool P1
(config-dhcp-server)#dns-server dns1 192.168.0.1
```

For address pool "P1", specify its secondary DNS as "192.168.1.1":

```
(config)#ip dhcp server pool P1
(config-dhcp-server)#dns-server dns2 192.168.1.1
```

## 4.9 option

### Description

The **option** command is used to specify an option for the DHCP client. To delete the option, please use the **no option command**.

### Syntax

**option** {60 | 66 | 67 | 150 | 159 | 160 | 176 | 242} {*value*}

**option138 ip-address** *ip-address*

**no option** {60 | 66 | 67 | 138 | 150 | 159 | 160 | 176 | 242}

### Parameter

60 — DHCP clients use this field to optionally identify the vendor type and configuration of a DHCP client. Mostly, it is used in the scenario where the APs apply for different IP addresses from different servers according to the needs. For detailed information, please consult the vendor. For TP-Link, the parameter *value* should be TP-Link.

66 — Option 66 specifies the TFTP server information and supports a single TFTP server IP address.

67 — Option 67 specifies the boot file name.

150 — Option 150 specifies the TFTP server information and supports multiple TFTP server IP addresses.

160 — Option 160 is used to configure DHCP captive portal.

176 — Option 176 is used to configure parameters for IP phones.

242 — Option 242 is used to provide the TMS address automatically.

*value* — The value you specified for an option to take effect.

*ip-address* — Enter the management address of an Omada Controller for it to discover the router. Option 138 is used in discovering the devices by an Omada controller.

### Command Mode

Config DHCP Server Mode

### Example

Set the file name of DHCP Network Boot as "Example":

```
(config-dhcp-server)#option 67 Example
```

## 4.10 ip dhcp relay helper-address

### Description

The **ip dhcp relay helper-address** command is used to enable DHCP relay, and specify a server address. If you select DHCP Relay as the DHCP Mode, the gateway will relay DHCP requests from LAN clients to the DHCP server in another network. Then the DHCP server will assign IP addresses to the LAN clients.

To disable DHCP relay, please use the **no ip dhcp relay helper-address** command.

### Syntax

```
ip dhcp relay helper-address ip-address  
no ip dhcp relay helper-address
```

### Parameter

*ip-address*—— Enter the IP address of the DHCP server.

### Command Mode

Config DHCP Server Mode

### Example

For address pool "P1", enable DHCP Relay and set the Server Address as "192.168. 3.1":

```
(config)#ip dhcp server pool P1  
(config-dhcp-server)#ip dhcp relay helper-address 192.168.3.1
```

## 4.11 show dhcp relay

### Description

The **show dhcp relay** command is used to display the information of the DHCP Relay mode.

### Syntax

```
show dhcp relay
```

### Command Mode

Global Configuration Mode

## Example

To view the router's DHCP relay information:

```
(config)#show dhcp relay
```

## 4.12 show ip dhcp server pool

### Description

The **show ip dhcp server pool** command is used to display the configuration of the address pool.

### Syntax

```
show ip dhcp server pool
```

### Command Mode

Global Configuration Mode

### Example

Display the configured address pool:

```
(config)#show ip dhcp server pool
```

## 4.13 show ip dhcp server status

### Description

The **show ip dhcp server status command** is used to display the status of the DHCP server.

### Syntax

```
show ip dhcp server status
```

### Command Mode

Global Configuration Mode

### Example

Display the status of DHCP server:

```
(config)#show ip dhcp server status
```

## 4.14 show dhcp server client-list

### Description

The **show dhcp server client-list** command is used to display the DHCP server client information.

### Syntax

```
show dhcp server client-list
```

### Command Mode

Global Configuration Mode

### Example

Display the DHCP server client information:

```
(config)#show dhcp server client-list
```

## 4.15 show dhcp server

### Description

The **show dhcp server** command is used to display the settings of the DHCP servers you created and the unfinished DHCP servers saved in the cache.

### Syntax

```
show dhcp server
```

### Command Mode

Global Configuration Mode

### Example

Display the information of the DHCP servers:

```
(config)#show dhcp server
```

# Chapter 5 Port Mirroring Commands

Port Mirror function allows the router to forward packet copies of the monitored ports to a specific monitoring port. Then you can analyze the copied packets to monitor network traffic and troubleshoot network problems.

## 5.1 monitor session enable

### Description

The **monitor session enable** command is used to enable the Port Mirror function. To disable this function, please use the **no monitor session enable** command.

### Syntax

```
monitor session session_num enable  
no monitor session session_num enable
```

### Parameter

*session\_num* — The monitor session number, can only be specified as 1.

### Command Mode

Global Configuration Mode

### Example

Enable the Port Mirror function and create monitor session "1":

```
(config)#monitor session 1 enable
```

## 5.2 monitor session port

### Description

The **monitor session port** command is used to configure the monitoring port (the mirroring port). Each monitor session has only one monitoring port. To change the monitoring port, please edit the port-id of the **monitor session port** command.

### Syntax

```
monitor session session_num port port-id
```

## Parameter

*session\_num* — The monitor session number, can only be specified as 1.

*port-id* — The monitoring port number ranging from 1 to 5.

## Command Mode

Global Configuration Mode

## Example

For monitor session 1, configure port 1 as the monitoring port:

```
(config)#monitor session 1 port 1
```

# 5.3 monitor session source port

## Description

The **monitor session source port** command is used to configure the monitored port (the mirrored port). To delete the corresponding monitored port, please use the **no monitor session source port** command.

## Syntax

```
monitor session session_num source port port-id
```

```
no monitor session session_num source port port-id
```

## Parameter

*session\_num* — The monitor session number, can only be specified as 1.

*port-id* — The monitored port number, cannot be the same as the monitoring port. To create or delete multiple monitored ports, separate the port-id with a comma in the command.

## Command Mode

Global Configuration Mode

## Example

For monitor session 1, configure port 2 and 3 as the monitored port:

```
(config)#monitor session 1 source port 2,3
```

## 5.4 monitor session mode

### Description

The **monitor session mode** command is used to set the monitor mode (the Mirror Mode). The command includes three options: ingress, egress, and both.

### Syntax

```
monitor session session_num{ingress | egress | both}
```

### Parameter

*session\_num* — The monitor session number, can only be specified as 1.

ingress — The packets received by the mirrored port will be copied to the mirroring port.

egress — The packets sent by the mirrored port will be copied to the mirroring port.

both — Both the incoming and outgoing packets through the mirrored port will be copied to the mirroring port

### Command Mode

Global Configuration Mode

### Example

For monitor session 1, set the monitor mode as "ingress":

```
(config)#monitor session 1 ingress
```

## 5.5 show monitor session

### Description

The **show monitor session** command is used to display the port monitoring configuration.

### Syntax

```
show monitor session [session_num]
```

### Parameter

*session\_num* — The monitor session number, can only be specified as 1. It is optional.

### Command Mode

Global Configuration Mode



## Example

Display the monitoring configuration of monitor session 1:

```
(config)#show monitor session 1
```

## Chapter 6 IEEE 802.1Q VLAN Commands

VLAN enables you to divide the LAN into multiple logical networks and control the traffic among them in a convenient and flexible way. The LAN can be logically segmented by departments, application, or types of users, without regard to geographic locations. VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

### 6.1 vlan

#### Description

The **vlan** command is used to create IEEE 802.1Q VLAN. To delete the IEEE 802.1Q VLAN, please use the **no vlan** command.

#### Syntax

```
vlan vlan-list  
no vlan vlan-list
```

#### Parameter

*interface* — Specify IEEE 802.1Q VLAN ID list, ranging from 2 to 4094. It is multi-optional.

To create a new VLAN, enter in the format of vlan 2.

To create new VLANs in batches, enter in the format of vlan 2-5.

To delete a VLAN, enter in the format of no vlan 2.

To create the VLANs in batches, enter in the format of vlan 2,3,4,5.

#### Command Mode

Global Configuration Mode

#### Example

Create VLAN 2-5:

```
(config)#vlan 2-5
```

Delete VLAN 2:

```
(config)#no vlan 2
```

## 6.2 router vlan

### Description

The **router vlan** command is used to go to the Config VLAN Mode, in which you can configure a VLAN separately.

### Syntax

```
router vlan vlan-id
```

### Parameter

*vlan-id* — Enter the ID of a VLAN you want to configure. This value ranges from 1 to 4094.

### Command Mode

Global Configuration Mode

### Example

Enter the Config VLAN Mode and configure VLAN 1:

```
(config)#router vlan 1
```

## 6.3 name

### Description

The **name** command is used to assign a description to a VLAN. To clear the description, please use **no name** command.

### Syntax

```
name vlan-name
```

```
no name
```

### Parameter

*vlan-name* — Enter the VLAN ID you want to configure with letters, numbers, or underscores of less than 50 characters.

### Command Mode

Config VLAN Mode

### Example

Name VLAN 1 as "group1":

```
(config)#router vlan 1
```

```
(config-vlan)#name group1
```

## 6.4 router port

### Description

The **router port** command is used to enter the Config Port Mode, so you can configure the port settings for a VLAN.

### Syntax

```
router port port-id
```

### Parameter

*port-id* — Enter the number of the port you want to configure. The range of this value depends on the number of physical interfaces of your product.

### Command Mode

Config VLAN Mode

### Example

Enter the Config Port Mode, and configure the settings of port 2 for VLAN 1:

```
(config)#router vlan 1  
(config-vlan)#router port 2
```

## 6.5 switchport acceptable frame

### Description

The **switchport acceptable frame** command is used to set the acceptable frame type of a port in a VLAN.

### Syntax

```
switchport acceptable frame {untagged | tagged}
```

### Parameter

untagged — Choose to enter this value in the command, and the egress rule of the packets transmitted by the port will be “Untagged”.

tagged — Choose to enter this value in the command, and the egress rule of the packets transmitted by the port will be “Tagged”.

### Command Mode

Config Port Mode

## Example

For VLAN 1, set the acceptable frame of port 2 as "untagged":

```
(config)#router vlan 1
(config-vlan)#router port 2
(config-port)#switchport acceptable frame untagged
```

## 6.6 interface

### Description

The **interface** command is used to go to the corresponding Interface Mode according to the port-id or vlan-id you enter.

### Syntax

```
interface {switchport port-id | vlan vlan-id}
```

### Parameter

*port-id* — Enter the port number to go to the Interface Mode. This value depends on the number of physical interfaces of your product.

*vlan-id* — Enter the VLAN ID to go to the Interface Mode. This value ranges from 1 to 4094. You should enter an existing VLAN ID.

### Command Mode

Global Configuration Mode

### Example

Go to the Interface Mode, and configure port 2:

```
(config)#interface switchport 2
```

Go to the Interface Mode, and configure VLAN 1:

```
(config)#interface vlan 1
```

## 6.7 description

### Description

The **description** command is used to add a description for a port or a VLAN. To clear a description, please use the **no description** command.

## Syntax

**description** *description*  
**no description**

## Parameter

*description*—— Enter a description within 50 characters.

## Command Mode

Interface Mode

## Example

For VLAN 5, set its description as "example".

```
(config)#interface vlan 5
(config-interface) #description example
```

# 6.8 switchport pvid

## Description

The **switchport pvid** command is used to configure the PVID for a port.

## Syntax

**switchport pvid** *vlan-id*

## Parameter

*vlan-id* —— VLAN ID, ranging from 1 to 4094. You should enter an existing VLAN ID.

## Command Mode

Interface Mode

## Example

For port 2, set its PVID as "5".

```
(config)#interface switchport 2
(config-interface)#switchport pvid 5
```

# 6.9 show interface

## Description

The **show interface** command is used to display the information of a port or a VLAN you chose.

## Syntax

```
show interface {switchport interface | vlan vlan-id}
```

## Parameter

*interface*—— Enter the port number you want to check.

*vlan-id*—— Enter the VLAN ID you want to check.

## Command Mode

All

## Example

View the information of port 2:

```
>enable  
#show interface switchport 2
```

View the information of VLAN 1:

```
(config)#show interface vlan 1
```

# 6.10 show vlan summary

## Description

The **show vlan summary** command is used to display the summarized information of IEEE 802.1Q VLAN.

## Syntax

```
show vlan summary
```

## Command Mode

Global Configuration Mode

## Example

Display the summarized information of IEEE 802.1Q VLAN:

```
(config)#show vlan summary
```

# 6.11 show vlan

## Description

The **show vlan** command is used to display the detailed information of IEEE 802.1Q VLAN.

## Syntax

**show vlan**

## Command Mode

Global Configuration Mode

## Example

Display the detailed information of IEEE 802.1Q VLAN:

```
(config)#show vlan
```

# 6.12 show interface status

## Description

The **show interface status** command is used to display the connection status of all ports.

## Syntax

**show interface status**

## Command Mode

Global Configuration Mode

## Example

Display the connection status of all ports:

```
(config)#show interface status
```



## Chapter 7 NAT Commands

NAT (Network Address Translation) is the translation between private IP and public IP. NAT provides a way to allow multiple private hosts to access the public network using one public IP at the same time, which alleviates the shortage of IP addresses. Furthermore, NAT strengthens the LAN (Local Area Network) security since the address of LAN host never appears on the internet.

### 7.1 show nat one-to-one

#### Description

The **show nat one-to-one** command is used to display the detailed information of the One-to-One NAT entries.

#### Syntax

```
show nat one-to-one
```

#### Command Mode

All

#### Example

Display the detailed information of the One-to-One NAT entries:

```
>enable  
#show nat one-to-one
```

### 7.2 show nat virtual-server

#### Description

The **show nat virtual-server** command is used to display the detailed information of the Virtual Server entries.

#### Syntax

```
show nat virtual-server
```

#### Command Mode

All

## Example

Display the detailed information of the Virtual Server entries:

```
>enable
# show nat virtual-server
```

## 7.3 show nat alg

### Description

The **show nat alg** command is used to display the ALG settings.

### Syntax

```
show nat alg
```

### Command Mode

All

## Example

Display the ALG settings:

```
>enable
# show nat alg
```

## 7.4 nat one-to-one

### Description

The **nat one-to-one** command is used to enable the One-to-One NAT function by creating a new One-to-One NAT entry. You also use this command to enter the Config NAT OTO Mode.

The newly created One-to-One NAT entry takes effect only when you configure its Interface, Original IP, Translated IP, DMZ Forwarding parameters using the commands of **interface one-to-one**, **original-ip**, **translated-ip**, and **dmz forwarding**.

To disable this function, please use the **no nat one-to-one** command.

**Note:** One-to-One NAT takes effect only when the WAN connection type is Static IP.

### Syntax

```
nat one-to-one name
no nat one-to-one name
```

## Parameter

*name* — Enter the name of the One-to-One NAT entry you want to create or delete with letters, numbers or underscores.

## Command Mode

Global Configuration Mode

## Example

Create a new One-to-One NAT entry named "example":

```
(config)#nat one-to-one example
```

# 7.5 interface one-to-one

## Description

The **interface one-to-one** command is used to specify an interface for an One-to-One NAT rule.

## Syntax

```
interface one-to-one interface_name_one
```

## Parameter

*interface\_name\_one* — Specify an interface for an One-to-One NAT entry by entering its VLAN ID.

## Command Mode

Config NAT OTO Mode

## Example

For an One-to-One NAT entry "example", set the WAN port as its interface. The VLAN ID of the WAN port is "4094":

```
(config)#nat one-to-one example  
(config-nat-oto)#interface one-to-one 4094
```

# 7.6 original-ip

## Description

The **original-ip** command is used to specify a private IP address for a One-to-One NAT entry.

## Syntax

**original-ip** *original\_ip*

## Parameter

*original\_ip* — Specify an original IP address which cannot be the broadcast address or the IP address of the LAN interface.

## Command Mode

Config NAT OTO Mode

## Example

For the One-to-One NAT entry "example", set the original IP address as "192.168.0.5":

```
(config)#nat one-to-one example
(config-nat-oto)#original-ip 192.168.0.5
```

# 7.7 translated-ip

## Description

The **translated-ip** command is used to specify a public IP address for a One-to-One NAT entry.

## Syntax

**translated-ip** *translated\_ip*

## Parameter

*translated\_ip* — Specify a translated IP address which cannot be the broadcast address or the IP address of the WAN interface.

## Command Mode

Config NAT OTO Mode

## Example

For the One-to-One NAT entry "example", set the translated IP address as "192.168.0.6":

```
(config)#nat one-to-one example
(config-nat-oto)#translated-ip 192.168.0.6
```

## 7.8 dmz forwarding

### Description

The **dmz forwarding** command is used to enable or disable DMZ Forwarding. If DMZ Forwarding is enabled, the packets transmitted to the translated IP address will be forwarded to the host of the original IP address.

### Syntax

**dmz forwarding** {on | off}

### Parameter

On — Enter this value to enable DMZ Forwarding.

Off — Enter this value to disable DMZ Forwarding.

### Command Mode

Config NAT OTO Mode

### Example

For the One-to-One NAT entry "example", enable DMZ Forwarding:

```
(config)#nat one-to-one example
(config-nat-oto)#dmz forwarding on
```

## 7.9 description-one

### Description

The **description-one** command is used to add a description to a One-to-One NAT entry.

### Syntax

**description-one** *description*

### Parameter

*description* — Add a brief description.

### Command Mode

Config NAT OTO Mode

## Example

For the One-to-One NAT entry “example”, add a description “example description”:

```
(config)#nat one-to-one example
(config-nat-oto)#description-one example description
```

## 7.10 nat virtual-server

### Description

The **nat virtual-server** command is used to enable the Virtual Server function by creating a new Virtual Server entry. You also use this command to enter the Config NAT VS Mode.

The newly created Virtual Server entry takes effect only when you configure its Interface, External Port, Internal Port, Internal Server IP, and Protocol using the commands of **interface virtual-server**, **external port**, **internal port**, **internal server-ip**, and **protocol**.

To disable this function, please use the **no nat virtual-server** command.

### Syntax

```
nat virtual-server name
no nat virtual-server name
```

### Parameter

*name* — Enter the name of the Virtual Server entry you want to create or delete with letters, numbers or underscores.

### Command Mode

Global Configuration Mode

### Example

Create a new Virtual Server entry named “example”:

```
(config)#nat virtual-server example
```

## 7.11 interface virtual-server

### Description

The **interface virtual-server** command is used to specify an interface for a Virtual Server rule.

## Syntax

**interface virtual-server** *interface\_vlan*

## Parameter

*interface\_vlan* — Specify an interface for a Virtual Server entry by entering its VLAN ID.

## Command Mode

Config NAT VS Mode

## Example

For a Virtual Server entry "example", set the WAN port as its interface. The VLAN ID of the WAN port is "4094":

```
(config)#nat one-to-one example
(config-nat-vs)#interface virtual-server 4094
```

# 7.12 external port

## Description

The **external port** command is used to specify an external port for a Virtual Server rule.

## Syntax

**external port** *external\_port*

## Parameter

*external\_port* — Enter the service port the router provided for accessing external network. This value ranges from 1 to 65535, and cannot overlap with the external ports of other virtual server rules.

## Command Mode

Config NAT VS Mode

## Example

For a Virtual Server entry "example", set the external port as "66":

```
(config)#nat virtual-server example
(config-nat-vs)#external port 66
```

## 7.13 internal port

### Description

The **internal port** command is used to specify an internal port for a Virtual Server rule.

### Syntax

**internal port** *internal\_port*

### Parameter

*internal\_port* — Specify the service port of the LAN host as a virtual server. This value ranges from 1 to 65535.

### Command Mode

Config NAT VS Mode

### Example

For a Virtual Server entry "example", set the internal port as "67":

```
(config)#nat virtual-server example
(config-nat-vs)#internal port 67
```

## 7.14 internal server-ip

### Description

The **internal server-ip** command is used to specify an internal server IP for a Virtual Server rule. All the requests from the internet to the specified LAN port will be redirected to this host.

### Syntax

**internal server-ip** *server\_ip*

### Parameter

*server\_ip* — Enter the IP address of the specified internal server for the entry.

### Command Mode

Config NAT VS Mode



## Example

For a Virtual Server entry "example", set the internal server IP as "192.168.0.4":

```
(config)#nat virtual-server example
(config-nat-vs)#internal server-ip 192.168.0.4
```

## 7.15 protocol

### Description

The **protocol** command is used to specify the protocol used for the entry.

### Syntax

```
protocol {ALL | TCP | UDP}
```

### Parameter

ALL — Choose to enter this value in the command, and the Virtual Server rule will use TCP and UDP as the protocols.

TCP — Choose to enter this value in the command, and the Virtual Server rule will use TCP as the protocol.

UDP — Choose to enter this value in the command, and the Virtual Server rule will use UDP as the protocol.

### Command Mode

Config NAT VS Mode

### Example

For a Virtual Server entry "example", select TCP as its protocol:

```
(config)#nat virtual-server example
(config-nat-vs)#protocol TCP
```

## 7.16 nat alg

### Description

The **nat alg** command is used to enable an ALG function.

To disable an ALG function, please use the **no nat alg** command.

### Syntax

```
nat alg {ftp | ipsec | pptp | sip | h.323}
```

**no nat alg** {ftp | ipsec | pptp | sip | h.323}

## Parameter

ftp — Choose to enter this value in the command, and the FTP ALG will be enabled or disabled.

ipsec — Choose to enter this value in the command, and the IPsec ALG will be enabled or disabled.

pptp — Choose to enter this value in the command, and the PPTP ALG will be enabled or disabled.

sip — Choose to enter this value in the command, and the SIP ALG will be enabled or disabled.

h.323 — Choose to enter this value in the command, and the H.323 ALG will be enabled or disabled.

## Command Mode

Global Configuration Mode

## Example

Disable SIP ALG:

```
(config)#no nat alg sip
```

# Chapter 8 Static Routing Commands

## 8.1 show ip route static

### Description

The **show ip route static** command is used to show the static route information.

### Syntax

```
show ip route static
```

### Command Mode

All

### Example

Show the static route information:

```
>enable  
#show ip route static
```

## 8.2 ip route

### Description

The **ip route** command is used to create a static routing entry.

### Syntax

```
ip route {name} {target} {netmask} {gateway} {interface} {metric}
```

### Parameter

*name*—— Specify a name for the entry.

*target*—— Enter the destination IP of the static routing entry.

*netmask*—— Specify the subnet mask of the destination network.

*gateway*—— Specify the IP address to which the packet should be sent next.

*interface*—— Specify the physical network interface through which this route is accessible by entering its VLAN ID.

*metric*—— Define the priority of the route. This value ranges from 0-15, and a smaller value means a higher priority.

## Command Mode

Global Configuration Mode

## Example

Create a static routing rule with the following settings:

Name: Example

Destination IP: 10.31.41.60

Subnet Mask: 255.255.255.0

Next Hop: 172.31.53.45

Interface: WAN (with the VLAN ID "4094")

Metric: 5

```
(config)#ip route Example 10.31.41.60 255.255.255.0 172.31.53.45 4094 5
```

## 8.3 no ip route

### Description

The **no ip route** command is used to delete a static routing entry.

### Syntax

```
no ip route index
```

### Parameter

*index*— Enter the ID of the static routing entry you want to delete.

## Command Mode

Global Configuration Mode

## Example

Delete a static routing entry whose ID is "1":

```
(config)#no ip route 1
```

# Chapter 9 RIP Commands

RIP (Routing Information Protocol) is a dynamic router protocol with Distance Vector Algorithms.

## 9.1 router rip

### Description

The **router rip** command is used to enable the RIP function and enter the Config RIP Mode.

To disable RIP, please use the **no router rip** command.

### Syntax

**router rip**  
**no router rip**

### Command Mode

Global Configuration Mode

### Example

Enable the RIP function and enter the Config RIP Mode:

```
(config)#router rip
```

## 9.2 rip version

### Description

The **rip version** command is used to set the global RIP version.

To restore the RIP version to the default, please use the **no version** command.

### Syntax

**version** {default | ripv1 | ripv2}  
**no version**

### Parameter

default — Send with RIP version 2 and receive with both RIP version 1 and 2.

ripv1 — Send and receive RIP version 1 formatted packets via broadcast.

ripv2 — Send and receive RIP version 2 packets using multicast.

## Command Mode

Config RIP Mode

## Example

Set the RIP version as "RIPv1":

```
(config-rip)#version ripv1
```

## 9.3 rip distance

### Description

The **rip distance** command is used to set the global RIP distance.

To restore the RIP version to the default (120), please use the **no distance** command.

### Syntax

**distance** *distance\_value*

**no distance**

### Parameter

*distance\_value*——Enter a value from 1 to 255.

## Command Mode

Config RIP Mode

## Example

Set the RIP distance as "130":

```
(config-rip)#distance 130
```

## 9.4 auto-summary

### Description

The **auto-summary** command is used to enable the Auto Summary function globally to summarize entries to their main class boundary.

To disable Auto Summary, please use the **no auto-summary** command.

### Syntax

**auto-summary**

**no auto-summary**

## Command Mode

Config RIP Mode

## Example

Enable Auto Summary:

```
(config-rip)#auto-summary
```

# 9.5 timers basic update

## Description

The **timers basic update** command is used to set the update timer globally, which can generate a complete response to every neighboring gateway.

## Syntax

```
timers basic update timers_value
```

## Parameter

*timers\_value*——Enter a value from 5 to 100 seconds.

## Command Mode

Config RIP Mode

## Example

Set the update timer to "40" seconds:

```
(config-rip)#timers basic update 40
```

# 9.6 timers basic timeout

## Description

The **timers basic timeout** command is used to set the timeout timer globally. Upon the expiration of the timeout, the route is no longer valid and set to unreachable.

## Syntax

```
timers basic timeout timers_value
```

## Parameter

*timers\_value*——Enter a value from 5 to 300 seconds.

## Command Mode

Config RIP Mode

## Example

Set the timeout timer to "200" seconds:

```
(config-rip)#timers basic timeout 200
```

# 9.7 timers basic garbage-collect

## Description

The **timers basic garbage-collect** command is used to set the garbage timer globally. Upon the expiration of the garbage-collection timer, the route will be finally removed.

## Syntax

```
timers basic garbage-collect timers_value
```

## Parameter

*timers\_value*——Enter a value from 5 to 500 seconds.

## Command Mode

Config RIP Mode

## Example

Set the garbage timer to "300" seconds:

```
(config-rip)#timers basic garbage-collect 300
```

# 9.8 no timers basic

## Description

The **no timers basic** command is used to restore the update timer, timeout timer, and garbage timer to the default.

## Syntax

```
no timers basic
```

## Command Mode

Config RIP Mode



## Example

Restore the update timer, timeout timer, and garbage timer to the default:

```
(config-rip)#no timer basic
```

## 9.9 rip network

### Description

The **rip network** command is used to add a network to the router's RIP network list. To remove a network from the list, please use the **no network** command.

### Syntax

```
network {ipaddress} {mask}  
no network ipaddress
```

### Parameter

*ipaddress*—— The IP address of the network.

*mask*—— The subnet mask of the network.

### Command Mode

Config RIP Mode

### Example

Add a network (IP address: 192.168.0.4, subnet mask: 255.255.255.0) to the router's RIP network list:

```
(config-rip)#network 192.168.0.4 255.255.255.0
```

## 9.10 ip rip send version

### Description

The **ip rip send version** command is used to configure the RIP send version for the specified interface.

To restore the send version to the default (RIPv2), please use the **no ip rip send version** command.

### Syntax

```
ip rip send version {ripv1|ripv2}  
no ip rip send version
```

## Parameter

ripv1 — Send RIP version 1 formatted packets via broadcast.

ripv2 — Send RIP version 2 packets using multicast.

## Command Mode

Interface Mode

## Example

For the interfaces in VLAN 1, set the RIP send version as "ripv1" :

```
(config)#interface vlan 1
(config-interface)#ip rip send version ripv1
```

# 9.11 ip rip receive version

## Description

The **ip rip receive version** command is used to configure the RIP receive version for the specified interface.

To restore the receive version to the default (Both), please use the **no ip rip receive version** command.

## Syntax

**ip rip receive version** {ripv1| ripv2 | both}

**no ip rip receive version**

## Parameter

ripv1 — Accept only RIP version 1 formatted packets.

ripv2 — Accept only RIP version 2 formatted packets.

both — Accept both RIP version 1 and RIP version 2 formatted packets.

## Command Mode

Interface Mode

## Example

For the interfaces in VLAN 1, set the RIP receive version as "ripv1" :

```
(config)#interface vlan 1
(config-interface)#ip rip receive version ripv1
```

## 9.12 ip rip split-horizon

### Description

The **ip rip split-horizon** command is used to set the Split Horizon Mode to Split-horizon for the specified interface.

If you don't want to set the Split Horizon Mode, please use the **no ip rip split-horizon** command to disable Split-horizon.

### Syntax

```
ip rip split-horizon
no ip rip split-horizon
```

### Command Mode

Interface Mode

### Example

For the interfaces in VLAN 1, set the Split Horizon Mode to Split-horizon :

```
(config)#interface vlan 1
(config-interface)#ip rip split-horizon
```

## 9.13 ip rip poison-reverse

### Description

The **ip rip poison-reverse** command is used to set the Split Horizon Mode to Poison Reverse for the specified interface.

If you don't want to set the Split Horizon Mode, please use the **no ip rip poison-reverse** command to disable Poison Reverse.

### Syntax

```
ip rip poison-reverse
no ip rip poison-reverse
```

### Command Mode

Interface Mode

### Example

For the interfaces in VLAN 1, set the Split Horizon Mode to Poison Reverse:

```
(config)#interface vlan 1
(config-interface)#ip rip poison-reverse
```

## 9.14 ip rip authentication-mode

### Description

The **ip rip authentication-mode** command is used to set the RIP authentication mode for the specified interface.

To restore the authentication mode to the default (None), please use the **no ip rip authentication-mode** command.

### Syntax

```
ip rip authentication-mode {simple key| md5 key-id key-string}  
no ip rip authentication-mode
```

### Parameter

**simple** — Choose to enter this value, and the router will use the simple password to authenticate. You need to enter the *key*.

*key* — The key used for simple authentication.

**md5** — Choose to enter this value, and the router will use the md5 message-digest algorithm to authenticate. You need to enter the *key-id* and the *key-string*.

*key-id* — The key ID used for md5 authentication.

*key-string* — The key used for md5 authentication.

### Command Mode

Interface Mode

### Example

For the interfaces in VLAN 1, set the authentication type as "Simple", and set the key as "12345678":

```
(config)#interface vlan 1  
(config-interface)#ip rip authentication-mode simple 12345678
```

## 9.15 show ip rip

### Description

The **show ip rip** command is used to show the detailed information of the RIP settings.

### Syntax

```
show ip rip
```

## Command Mode

All

## Example

Show the detailed information of the RIP settings:

```
>enable  
#show ip rip
```

# Chapter 10 OSPF Commands

OSPF (Open Shortest Path First) is an Interior Gateway Protocol (IGP) used to make routing decisions in a single autonomous system (AS).

## 10.1 router ospf

### Description

The **router ospf** command is used to enable the OSPF globally, and to enter the OSPF Mode.

To disable the OSPF, please use the **no router ospf** command.

### Syntax

**router ospf**  
**no router ospf**

### Command Mode

Global Configuration Mode

### Example

Enable the OSPF globally, and to enter the OSPF Mode:

```
(config)#router ospf
```

## 10.2 router-id

### Description

The **router-id** command is used to set a Router ID for the OSPF.

### Syntax

**router-id** *router-id*

### Parameter

*router-id*— Enter the Router ID in dotted decimal format.

### Command Mode

OSPF Mode

## Example

Set the Router ID as "192.168.0.4" :

```
(config-ospf)#router-id 192.168.0.4
```

## 10.3 area-id

### Description

The **area-id** command is used to set an Area ID for the OSPF.

### Syntax

```
area-id area-id
```

### Parameter

*area-id*—— Enter a value from 0- 4294967295.

### Command Mode

OSPF Mode

### Example

Set the Area ID as "1" :

```
(config-ospf)#area-id 1
```

## 10.4 compatible rfc1583

### Description

The **compatible rfc1583** command is used to enable RFC 1583 Compatibility for the OSPF.

To disable RFC 1583 Compatibility, please use the **no compatible rfc1583** command.

### Syntax

```
compatible rfc1583  
no compatible rfc1583
```

### Command Mode

OSPF Mode

## Example

Enable RFC 1583 Compatibility:

```
(config-ospf)#compatible rfc1583
```

## 10.5 ospf-network

### Description

The **ospf-network** command is used to create a network interface for the OSPF, which will be shown on the Network Table of the web management page.

To delete an entry, please use the **no ospf-network** command.

### Syntax

```
ospf-network {ip_adress} {mask}
```

```
no ospf-network ip_adress
```

### Parameter

*ip\_adress* — Enter the IP address of the network in the format of 100.100.0.0.

*mask* — Enter the wildcard mask of the network in the format of 0.0.255.255. Normal subnet mask is also supported.

### Command Mode

OSPF Mode

### Example

Create a network interface with the IP Address "192.168.0.0" and Wildcard Mask "0.0.255.255":

```
(config-ospf)#ospf-network 192.168.0.0 0.0.255.255.
```

## 10.6 ospf-distance

### Description

The **ospf-distance** command is used to specify OSPF route distance. When more than two protocols have routes to the same destination, only the route that has smallest distance will be inserted to IP routing table.

### Syntax

```
ospf-distance distance
```



## Parameter

*distance*—— Specify OSPF route distance from 0-255.

## Command Mode

OSPF Mode

## Example

Set the OSPF route distance as "95":

```
(config-ospf)#ospf-distance 95
```

# 10.7 timers throttle spf

## Description

The **timers throttle spf** command is used to set the SPF Delay Time, SPF Hold Init Time, and SPF Hold Max Time.

## Syntax

```
timers throttle spf {spf-delay} {spf-init_holdtime} {spf-max_holdtime}
```

## Parameter

*spf-delay*—— The number of seconds from when OSPF receives a topology change to the start of the next SPF calculation. The valid value ranges from 0 to 600 000 msec.

*spf-init\_holdtime* —— The number of seconds from when OSPF receives a topology change to the start of the next SPF calculation. The valid value ranges from 0 to 600 000 msec.

*spf-max\_holdtime* —— Maximum hold time (msec). The valid value ranges from 0 to 600000 msec.

## Command Mode

OSPF Mode

## Example

Set the SPF Delay Time as "10", the SPF Hold Init Time "40", and the SPF Hold Max Time "6000":

```
(config-ospf)#timer throttle spf 10 40 6000
```

## 10.8 maximum-paths

### Description

The **maximum-paths** command is used to set the number of paths that OSPF can report for a given destination.

### Syntax

**maximum-paths** *max-paths*

### Parameter

*max-paths* — Specify the Maximum Paths for the OSPF by entering a value from 1-16.

### Command Mode

OSPF Mode

### Example

Set the Maximum Paths as "5":

```
(config-ospf)#maximum-paths 5
```

## 10.9 passive-interface default

### Description

The **passive-interface default** command is used to configure the global passive mode settings for all OSPF interfaces. Use this command will overwrite any present interface level passive mode settings.

To disable Passive Default, please use the **no passive-interface default** command.

### Syntax

**passive-interface default**  
**no passive-interface default**

### Command Mode

OSPF Mode

### Example

Enable the Passive Default for the OSPF:

```
(config-ospf)#passive-interface default enable
```

## 10.10 ip ospf priority

### Description

The **ip ospf priority** command is used to configure the router priority for the interface you selected.

### Syntax

```
ip ospf priority priority
```

### Parameter

*priority* — Enter a value from 0-255. 0 indicates that the router is not eligible to become the designated router on this network.

### Command Mode

Interface Mode

### Example

For the interfaces in VLAN 1, set the Router Priority as "1".

```
(config)#interface vlan 1  
(config-interface)#ip ospf priority 1
```

## 10.11 ip ospf hello-interval

### Description

The **ip ospf hello-interval** command is used to set the hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network.

### Syntax

```
ip ospf hello-interval hello-interval
```

### Parameter

*hello-interval* — Enter a value from 1 to 65535 seconds.

### Command Mode

Interface Mode

### Example

For the interfaces in VLAN 1, set the Hello Interval as "15" seconds.

```
(config)#interface vlan 1
```

```
(config-interface)#ip ospf hello-interval 15
```

## 10.12 ip ospf dead-interval

### Description

The **ip ospf dead-interval** command is used to set the dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network.

### Syntax

```
ip ospf dead -interval dead-interval
```

### Parameter

*dead-interval*—— Enter a value from 1 to 65535 seconds.

### Command Mode

Interface Mode

### Example

For the interfaces in VLAN 1, set the Dead Interval as "15" seconds.

```
(config)#interface vlan 1  
(config-interface)#ip ospf dead-interval 15
```

## 10.13 ip ospf transmit-delay

### Description

The **ip ospf transmit-delay** command is used to set the Transmit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface.

### Syntax

```
ip ospf transmit-delay transmit-delay
```

### Parameter

*transmit-delay*—— Enter a value from 1 to 65535 seconds.

### Command Mode

Interface Mode

## Example

For the interfaces in VLAN 1, set the Transmit Delay as "15" seconds.

```
(config)#interface vlan 1
(config-interface)# ip ospf transmit-delay 15
```

## 10.14 ip ospf retransmit-interval

### Description

The **ip ospf retransmit-interval** command is used to set the retransmit interval for the specified interface. Retransmit interval is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets.

### Syntax

```
ip ospf retransmit-interval retransmit-interval
```

### Parameter

*retransmit-interval*—— Enter a value from 1 to 65535 seconds.

### Command Mode

Interface Mode

## Example

For the interfaces in VLAN 1, set the Retransmit Interval as "15" seconds.

```
(config)#interface vlan 1
(config-interface)# ip ospf retransmit-interval 15
```

## 10.15 ip ospf cost

### Description

The **ip ospf cost** command is used to set the link cost. OSPF uses the link cost in computing shortest paths.

### Syntax

```
ip ospf cost cost
```

### Parameter

*cost*—— Enter a value from 1 to 65535 seconds.

## Command Mode

Interface Mode

## Example

For the interfaces in VLAN 1, set the link cost as "90".

```
(config)#interface vlan 1
(config-interface)# ip ospf cost 90
```

# 10.16 ip ospf passive

## Description

The **ip ospf passive** command is used to enable or disable the passive mode for the specified interface. The passive mode is disabled by default.

## Syntax

```
ip ospf passive {enable | disable}
```

## Parameter

enable — Choose to enter this value, and the passive mode of the specified interface will be enabled.

disable — Choose to enter this value, and the passive mode of the specified interface will be disabled.

## Command Mode

Interface Mode

## Example

For the interfaces in VLAN 1, enable the passive mode.

```
(config)#interface vlan 1
(config-interface)# ip ospf passive enable
```

# 10.17 ip ospf mtu-ignore

## Description

The **ip ospf mtu-ignore** command is used to enable or disable the MTU Ignore for the specified interface. If MTU Ignore is enabled, the OSPF MTU mismatch detection will be disabled on received database description packets. MTU Ignore is disabled by default.

## Syntax

**ip ospf mtu-ignore** {enable | disable}

## Parameter

**enable** — Choose to enter this value, and the MTU Ignore of the specified interface will be enabled.

**disable** — Choose to enter this value, and the MTU Ignore of the specified interface will be disabled.

## Command Mode

Interface Mode

## Example

For the interfaces in VLAN 1, enable the MTU Ignore:

```
(config)#interface vlan 1
(config-interface)# ip ospf mtu-ignore enable
```

# 10.18 ip ospf authentication

## Description

The **ip ospf authentication** command is used to set the OSPF authentication type for the specified interface.

## Syntax

**ip ospf authentication** {None | Simple *simple-key* | MD5 *md5-key-id md5-key*}

## Parameter

**None** — Choose to enter this value, and there won't be any authentication.

**Simple** — Choose to enter this value, and the router will use the simple password to authenticate. You need to enter the *simple-key*.

*simple-key* — The key used for simple authentication.

**MD5** — Choose to enter this value, and the router will use the md5 message-digest algorithm to authenticate. You need to enter the *md5-key-id* and the *md5-key*.

*md5-key-id* — The key ID used for md5 authentication.

*md5-key* — The key used for md5 authentication.

## Command Mode

Interface Mode

## Example

For the interfaces in VLAN 1, set the authentication type as "Simple", and set the simple-key as "12345678":

```
(config)#interface vlan 1
(config-interface)#ip ospf authentication Simple 12345678
```

## 10.19 ip ospf network

### Description

The **ip ospf network** command is used to set the OSPF network type on the interface. The default network type for Ethernet interfaces is Broadcast.

### Syntax

```
ip ospf network {point-to-point | broadcast}
```

### Parameter

point-to-point — Enter this value to set the OSPF network type as Point-to-point.

broadcast — Enter this value to set the OSPF network type as Broadcast.

### Command Mode

Interface Mode

### Example

For the interfaces in VLAN 1, set the OSPF network type as Point-to-point:

```
(config)#interface vlan 1
(config-interface)#ip ospf network point-to-point
```

## 10.20 show ip ospf database

### Description

The **show ip ospf database** command is used to show the OSPF link state database.

### Syntax

```
show ip ospf database
```

### Command Mode

All



## Example

Show the OSPF link state database.

```
>enable
#show ip ospf database
```

## 10.21 show ip ospf neighbor

### Description

The **show ip ospf neighbor** command is used to show the OSPF neighbor table information.

### Syntax

```
show ip ospf neighbor
```

### Command Mode

All

### Example

Show the OSPF neighbor table information:

```
>enable
#show ip ospf neighbor
```

## 10.22 show ip ospf interface

### Description

The **show ip ospf interface** command is used to show the OSPF interface information.

### Syntax

```
show ip ospf interface
```

### Command Mode

All

### Example

Show the OSPF interface information:

```
>enable
```

```
#show ip ospf interface
```

## 10.23 show ip ospf

### Description

The **show ip ospf** command is used to show the OSPF information globally.

### Syntax

```
show ip ospf
```

### Command Mode

All

### Example

Show the OSPF information globally:

```
>enable  
#show ip ospf
```

## 10.24 show network

### Description

The **show network** command is used to show the OSPF network information.

### Syntax

```
show network
```

### Command Mode

All

### Example

Show the OSPF network information:

```
>enable  
#show network
```

# Chapter 11 IPsec Commands

IPsec (IP Security) can provide security services such as data confidentiality, data integrity, and data origin authentication at the IP layer. IPsec uses IKEv1 (Internet Key Exchange version 1) to handle the negotiation of protocols and algorithms based on the user-specified policy, and generate the encryption and authentication keys to be used by IPsec. IKEv1 negotiation includes two phases, which are IKEv1 Phase-1 and IKEv1 Phase-2.

## 11.1 crypto policy

### Description

The **crypto policy** command is used to create an IKEv1 or IKEv2 policy, and enter the IPSEC\_ISAKMP Mode. You can use the **crypto policy** command to edit an existing policy.

To delete an IPsec policy, please use the **no crypto policy** command.

### Syntax

```
crypto {ikev1 | ikev2} policy policy_name  
no crypto {ikev1 | ikev2} policy policy_name
```

### Parameter

*ikev1* — Choose to enter this value to create or edit an policy with the protocol version of IKEV1.

*ikev2* — Choose to enter this value to create or edit an policy with the protocol version of IKEV2

*policy\_name* — Specify a policy name within 32 characters.

### Command Mode

Global Configuration Mode

### Example

Create an IKEv1 policy named "example":

```
(config)#crypto ikev1 policy example
```

## 11.2 hash

### Description

The **hash** command is used to configure the authentication algorithm in Phase-1.

Note that the authentication algorithms sha256 / sha384 / sha512 are not compatible with the encryption algorithm des or the DH algorithms dh1 / dh2.

### Syntax

**hash** {md5 | sha1 | sha256 | sha384 | sha512}

### Parameter

{md5 | sha1 | sha256 | sha384 | sha512} — Select to enter one value as the authentication algorithm.

### Command Mode

IPSEC\_ISAKMP Mode

### Example

For an IKEv1 policy named "example", set "md5" as the authentication algorithm:

```
(config)#crypto ikev1 policy example
(config-ikev1-policy)#hash md5
```

## 11.3 encryption

### Description

The **encryption** command is used to configure the encryption algorithm in Phase-1.

Note that the encryption algorithm des is not compatible with the authentication algorithms sha256, sha384, or sha512.

### Syntax

**encryption** {des | 3des | aes128 | aes196 | aes256}

### Parameter

{des | 3des | aes128 | aes196 | aes256} — Select to enter one value as the encryption algorithm.

### Command Mode

IPSEC\_ISAKMP Mode

### Example

For an IKEv1 policy named "example", set "3des" as the encryption algorithm:

```
(config)#crypto ikev1 policy example
```

```
(config-ikev1-policy)#encryption 3des
```

## 11.4 group

### Description

The **group** command is used to configure the DH group in Phase-1.

Note that the DH group dh1 / dh2 are not compatible with the authentication algorithms sha256, sha384, or sha512.

### Syntax

```
group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 21 | 25 | 26}
```

### Parameter

{1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 21 | 25 | 26} — Select to enter one value as the DH group.

### Command Mode

IPSEC\_ISAKMP Mode

### Example

For an IKEv1 policy named "example", set "dh14" as the DH group:

```
(config)#crypto ikev1 policy example  
(config-ikev1-policy)#group 14
```

## 11.5 exchange-mode

### Description

The **exchange-mode** command is used to configure the IKE exchange mode in Phase-1. Note that this command is supported only for IKEv1.

Aggressive Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection, or scenarios that there is a NAT device (e.g. modem) in front of the devices at both ends of the IPsec.

Main mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection. It is the default mode.

### Syntax

```
exchange-mode {aggressive | main}
```

## Parameter

aggressive — Enter this value to set the exchange mode as Aggressive.

main — Enter this value to set the exchange mode as Main.

## Command Mode

IPSEC\_ISAKMP Mode

## Example

For an IKEv1 policy named "example", set "Aggressive" as the exchange mode:

```
(config)#crypto ikev1 policy example
(config-ikev1-policy)#exchange-mode aggressive
```

# 11.6 ike-lifetime

## Description

The **ike-lifetime** command is used to configure the SA lifetime in Phase-1.

## Syntax

**ike-lifetime** *time*

## Parameter

*time* — Enter a value from 60 to 604800 seconds. And the default is 28800 seconds.

## Command Mode

IPSEC\_ISAKMP Mode

## Example

For an IKEv1 policy named "example", set the SA lifetime of the Phase-1 Settings to "30000" seconds:

```
(config)#crypto ikev1 policy example
(config-ikev1-policy)#ike-lifetime 30000
```

# 11.7 crypto isakmp key

## Description

The **crypto isakmp key** command is used to specify the unique pre-shared key for both peers' authentication.

## Syntax

**crypto isakmp key** *keyword*

## Parameter

*keyword*—— Specify a keyword within 128 characters.

## Command Mode

IPSEC\_ISAKMP Mode

## Example

For an IKEv1 policy named "example", set the pre-shared key as "example123456":

```
(config)#crypto ikev1 policy example
(config-ikev1-policy)#crypto isakmp key example123456
```

# 11.8 dpd

## Description

The **dpd** command is used to enable or disable DPD (Dead Peer Detect) in Phase-1. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.

The DPD function is enabled by default.

## Syntax

**dpd** {enable | disable}

## Parameter

enable —— Enter this value to enable DPD.

disable —— Enter this value to disable DPD.

## Command Mode

IPSEC\_ISAKMP Mode

## Example

For an IKEv1 policy named "example", disable DPD in Phase-1:

```
(config)#crypto ikev1 policy example
(config-ikev1-policy)#dpd disable
```

## 11.9 dpd-interval

### Description

The **dpd-interval** command is used to specify the interval between sending DPD requests.

The DPD interval works only when the DPD function is enabled.

### Syntax

**dpd-interval** *time*

### Parameter

*time* — Specify a value from 1 to 300 seconds, and the default is 10.

### Command Mode

IPSEC\_ISAKMP Mode

### Example

For an IKEv1 policy named "example", when DPD is enabled, set the DPD interval to "20" seconds:

```
(config)#crypto ikev1 policy example
(config-ikev1-policy)#dpd-interval 20
```

## 11.10 crypto ipsec transform-set

### Description

The **crypto ipsec transform-set** command is used to create a transform-set and to enter the IPSEC\_TRANSFORM Mode. You can use this command to edit an existing transform-set.

To delete a transform-set, please use the **no crypto transform-set** command.

The encryption algorithm des is not compatible with the authentication algorithms sha256, sha384, or sha512.

### Syntax

```
crypto ipsec transform-set {tset_name} {esp-des | esp-3des | esp-aes128 |
esp-aes196 | esp-aes256} {esp-md5 | esp-sha1 | esp-sha256 | esp-sha384 |
esp-sha512}
no crypto transform-set tset_name
```

### Parameter

*tset\_name* — Specify a transform-set name within 32 characters.



{esp-des | esp-3des | esp-aes128 | esp-aes196 | esp-aes256} — The protocol and encryption algorithm of the Phase-2 Settings. Select to enter one in the command.

{esp-md5 | esp-sha1 | esp-sha256 | esp-sha384 | esp-sha512} — The protocol and authentication algorithm of the Phase-2 Settings. Select to enter one in the command.

## Command Mode

Global Configuration Mode

## Example

Create a transform-set named "example1", and set the protocol as "esp", the encryption algorithm "3des", and the authentication algorithm "sha1":

```
(config)#crypto ipsec transform-set example1 esp-3des esp-sha1
```

# 11.11 lifetime

## Description

The **lifetime** command is used to configure the SA lifetime in Phase-2.

## Syntax

**lifetime** *time*

## Parameter

*time* — Enter a value from 120 to 604800 seconds. And the default is 28800 seconds.

## Command Mode

IPSEC\_TRANSFORM Mode

## Example

For the transform-set named "example1", set the SA lifetime in Phase-2 to "30000" seconds:

```
(config)#crypto ipsec transform-set example1 esp-3des esp-sha1
```

```
(config-transform-set)#lifetime 30000
```

## 11.12 encapsulation-mode

### Description

The **encapsulation-mode** command is used to set the encapsulation mode in Phase-2 as Tunnel Mode or Transport Mode. The default mode is Tunnel Mode.

### Syntax

```
encapsulation-mode {tunnel | transport}
```

### Parameter

tunnel — Choose to enter this value in the command to set the encapsulation mode as Tunnel Mode.

transport — Choose to enter this value in the command to set the encapsulation mode as Transport Mode.

### Command Mode

IPSEC\_TRANSFORM Mode

### Example

For the transform-set named "example1", set the encapsulation mode as Transport Mode:

```
(config)#crypto ipsec transform-set example1 esp-3des esp-sha1  
(config-transform-set)#encapsulation-mode transport
```

## 11.13 pfs

### Description

The **pfs** command is used to specify a DH group to enable PFS (Perfect Forward Security) for IKE mode, then the key generated in phase-2 will be irrelevant with the key in phase-1, which enhance the network security. If you select None, it means PFS is disabled and the key in phase-2 will be generated based on the key in phase-1. The default is None.

### Syntax

```
pfs {none | 1 | 2 | 5 | 14}
```

### Parameter

{none | 1 | 2 | 5 | 14} — The DH groups. Choose to enter one value in the command.

## Command Mode

IPSEC\_TRANSFORM Mode

## Example

For the transform-set named "example1", specify "dh5" to enable the PFS function:

```
(config)#crypto ipsec transform-set example1 esp-3des esp-sha1
(config-transform-set)#pfs 5
```

# 11.14 crypto map

## Description

The **crypto map** command is used to create a new map, specify the map name, and apply a well configured IPsec policy to the map. You can also use the **crypto map** command to edit an existing map, and enter the IPSEC\_MAP Mode.

The map will appear on the IPsec Policy List of the web management page.

To delete a map, please use the **no crypto map** command.

## Syntax

```
crypto map {map_name} {policy_name}
no crypto map map_name
```

## Parameter

{map\_name} — Enter the name of the map with 32 characters.

{policy\_name} — Enter the name of a well configured IPsec policy.

## Command Mode

Global Configuration Mode

## Example

Create a map named "map1", and apply an IPsec policy named "example" to the map:

```
(config)#crypto map map1 example
```

# 11.15 set peer

## Description

The **set peer** command is used to set the remote gateway for the map.

## Syntax

**set peer** *remote\_peer*

## Parameter

*remote\_peer*—— Enter an IP address or a domain name (1 to 255 characters) as the remote gateway. 0.0.0.0 represents any IP address. Only when the negotiation mode is set to Responder Mode can you enter 0.0.0.0.

## Command Mode

IPSEC\_MAP Mode

## Example

For a map named "map1" with an IPsec policy named "example", set the remote gateway as "10.13.41.60":

```
(config)#crypto map map1 example
(config-map)#set peer 10.31.41.60
```

# 11.16 set transform-set

## Description

The **set transform-set** command is used to set the transform-set applying to the map. The transform-set should be well configured.

## Syntax

**set transform-set** *tset\_name*

## Parameter

*tset\_name*—— Enter the name of a well configured transform-set.

## Command Mode

IPSEC\_MAP Mode

## Example

For a map named "map1" with an IPsec policy named "example", apply a transform-set named "example1" to it:

```
(config)#crypto map map1 example
(config-map)#set transform-set example1
```

## 11.17 localsubnet

### Description

The **localsubnet** command is used to specify a local subnet for the map. It's always the IP address range of LAN on the local side of the VPN tunnel. After the IPsec tunnel is established, the peer can access the local subnet.

### Syntax

```
localsubnet {ip}/{mask}
```

### Parameter

*ip*—— Enter an valid local IP address.

*mask*—— Enter the subnet mask of the IP address.

### Command Mode

IPSEC\_MAP Mode

### Example

For a map named "map1" with an IPsec policy named "example", set the local subnet as "192.168.0.0/24":

```
(config)#crypto map map1 example  
(config-map)#localsubnet 192.168.0.0/24
```

## 11.18 remotesubnet

### Description

The **remotesubnet** command is used to specify a remote subnet for the map. It's always the IP address range of LAN on the remote peer of the VPN tunnel. Only the traffic to the remote subnet will be forwarded through the IPsec tunnel.

### Syntax

```
remotesubnet {ip}/{mask}
```

### Parameter

*ip*—— Enter an valid remote IP address.

*mask*—— Enter the subnet mask of the IP address.

### Command Mode

IPSEC\_MAP Mode

## Example

For a map named "map1" with an IPSec policy named "example", set the remote subnet as "192.168.1.0/24":

```
(config)#crypto map map1 example
(config-map)#remotesubnet 192.168.1.0/24
```

## 11.19 negotiation-mode

### Description

The **negotiation-mode** command is used to set the negotiation mode for the map. Initiator Mode is the default mode.

Responder Mode: The local device responds a connection to the peer.

### Syntax

```
negotiation-mode {initiator | responder}
```

### Parameter

initiator — Enter this value to set the negotiation mode as the Initiator Mode, and the local device will initiate a connection to the peer.

responder — Enter this value to set the negotiation mode as the Responder Mode, and the local device will respond a connection to the peer.

### Command Mode

IPSEC\_MAP Mode

### Example

For a map named "map1" with an IPSec policy named "example", set the negotiation mode as the Responder Mode:

```
(config)#crypto map map1 example
(config-map)#negotiation-mode responder
```

## 11.20 ipsec map

### Description

The **ipsec map** command is used to bind a map to your desired WAN ports, and distribute the map.

### Syntax

```
ipsec map map_name
```

## Parameter

*map\_name* — Enter the name of the map you created.

## Command Mode

Interface Mode

## Example

Bind a map named "map1" to a WAN port of the router, and the VLAN ID of that WAN port is "4094":

```
(config)#interface vlan 4094
(config-interface)#ipsec map map1
```

# 11.21 show policy

## Description

The **show policy** command is used to display the settings of the IKEv1 policy or the IKEv2 policy.

To view the settings of all the existing IKEv1 policies or IKEv2 policies, please use the **show all policy** command.

## Syntax

```
show {ikev1| ikev2} policy policy_name
show all {ikev1| ikev2} policy
```

## Parameter

*ikev1* — Choose to enter this value, if you want to view the settings of the IKEv1 policy.

*ikev2* — Choose to enter this value, if you want to view the settings of the IKEv2 policy.

*policy\_name* — Enter the name of the IKEv1 or IKEv2 policy you want to view.

## Command Mode

All

## Example

View the settings of an IKEv1 policy named "example":

```
(config)#show ikev1 policy example
```

View the settings of all the IKEv2 policies you have created:

```
(config)#show all ikev2 policy
```

## 11.22 show transform-set

### Description

The **show transform-set** command is used to display the settings of a specified transform-set.

To view the settings of all the existing transform-set entries, please use the **show all transform-set** command.

### Syntax

```
show transform-set tset_name  
show all transform-set
```

### Parameter

*tset\_name* — Enter the name of the transform-set you want to view its details.

### Command Mode

All

### Example

View the settings of a transform-set named "example1":

```
(config)#show transform-set example1
```

## 11.23 show crypto map

### Description

The **show crypto map** command is used to display the settings of a specified map.

To view the settings of all the existing maps, please use the **show all crypto map** command.

### Syntax

```
show crypto map map_name  
show all crypto map
```

### Parameter

*map\_name* — Enter the name of the map you want to view its details.



## Command Mode

All

## Example

View the settings of a map named "map1":

```
(config)#show crypto map map1
```

# 11.24 show crypto ipsec sa

## Description

The **show crypto ipsec sa** command is used to display the SA settings of an established map.

## Syntax

```
show crypto ipsec sa map_name
```

## Parameter

*map\_name*—— Enter the name of a map.

## Command Mode

All

## Example

View the SA settings of a map named "map1":

```
(config)#show crypto ipsec sa map1
```

# Chapter 12 ACL Commands

ACL (Access Control List) is used to filter data packets by configuring a series of match conditions, operations and time ranges. It provides a flexible and secured access control policy and facilitates you to control the network security.

## 12.1 show access-list

### Description

The **show access-list** command is used to display the access control rules. The order in which the rules are listed is the order in which they take effect.

### Syntax

```
show access-list
```

### Command Mode

Global Configuration Mode

### Example

Display the access control rules:

```
(config)#show access-list
```

## 12.2 access-list ip

### Description

The **access-list ip** command is used to add an access control rule. You can use this command to edit an existing rule.

To delete the corresponding rule, please use **no access-list ip** command.

### Syntax

```
access-list ip acl-name rule [position] {deny | permit} {ALL | FTP | SSH |  
TELNET | SMTP | DNS | HTTP | POP3 | SNTP | H323 | ICMPv6 } {WAN | LAN |  
LAN-LAN | ALL} [sip-address] [dip-address] [time-range]
```

```
no access-list ip acl-name
```

### Parameter

*acl-name* — Specify a rule name which should be 6 to 64 characters with letters, numbers, or underscores.

*position* — Enter a number to define the priority for the rule. A smaller value means a higher priority.

{deny | permit} — Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

{ALL | FTP | SSH | TELNET | SMTP | DNS | HTTP | POP3 | SNTP | H323 | ICMPv6 }  
— Specify the service type by selecting one in the command.

{WAN | LAN | LAN-LAN | ALL} — Specify the effective traffic direction for the rule.

{*sip-address*} — The source network for the rule. You can only choose to enter one of these parameters: {LAN | IPGROUP\_ANY | IPGROUP\_LAN}. If you set the traffic direction as “LAN”, you can only enter “LAN”. If you set the traffic direction as “WAN”, “LAN-LAN”, or “ALL”, you can enter “IPGROUP\_ANY” or “IPGROUP\_LAN”.

{*dip-address*} — The destination network for the rule. You can only choose to enter one of these parameters: {LAN | IPGROUP\_ANY | IPGROUP\_LAN}. If you set the traffic direction as “LAN”, you can only enter “LAN”. If you set the traffic direction as “WAN”, “LAN-LAN”, or “ALL”, you can enter “IPGROUP\_ANY” or “IPGROUP\_LAN”.

*time-range* — Enter the name of a time range entry you created. If you haven’t created any time range, you can only enter “Any”, which is the name of the default time range. To create a time range, refer to [16.2 time-range week- date time-slice](#).

**Note:** When using the CLI, you can enter a question mark in the position of a parameter, and the corresponding tip will show.

## Command Mode

Global Configuration Mode

## Example

Create an access control rule with the following settings:

Name: example

Priority: 1

Policy: Permit

Service Type: FTP

Direction: All

Source: IPGROUP\_ANY

Destination: IPGROUP\_ANY

Effective Time: Any

```
(config)#access-list ip example rule 1 permit FTP ALL IPGROUP_ANY  
IPGROUP_ANY Any
```

# Chapter 13 SSH Commands

SSH (Security Shell) can provide the unsecured remote management with security and powerful authentication to ensure the security of the management information.

## 13.1 show ssh configuration

### Description

The **show ssh configuration** command is used to display the global configuration of SSH.

### Syntax

```
show ssh configuration
```

### Command Mode

All

### Example

Display the global configuration of SSH:

```
>enable  
#show ssh configuration
```

## 13.2 ssh server

### Description

The **ssh server** command is used to enable the SSH function. To disable the SSH function, please use the **no ssh server** command.

**Note:** The SSH terminal you are using will be disabled if you use the **no ssh server** command.

### Syntax

```
ssh server  
no ssh server
```

### Command Mode

Global Configuration Mode

## Example

Enable the SSH function:

```
(config)#ssh server
```

# Chapter 14 SNMP Commands

SNMP (Simple Network Management Protocol) functions are used to manage the network devices for a smooth communication, which can facilitate the network administrators to monitor the network nodes and implement the proper operation.

## 14.1 snmp-server v3

### Description

The **snmp-server v3** command is used to enable SNMPv3 and set a username and password.

To disable SNMPv3, please use the **no snmp-server v3** command.

### Syntax

**snmp-server v3 username *username* password *password* enable**  
**no snmp-server v3**

### Parameter

*username* — Enter the username within 42 characters with letters, numbers, or underscores.

*password* — Enter the password within 32 characters with letters, numbers, or underscores.

### Command Mode

Global Configuration Mode

### Example

Enable SNMPv3, set the username as "example", and the password as "12345678":

```
(config)#snmp-server v3 username example password 12345678 enable
```

## 14.2 snmp-server v1-v2c

### Description

The **snmp-server v1-v2c** command is used to enable SNMPv1&v2c.

To disable SNMPv1&v2c, please use the **no snmp-server v1-v2c enable** command.

## Syntax

```
snmp-server v1-v2c enable;  
no snmp-server v1-v2c enable
```

## Command Mode

Global Configuration Mode

## Example

Enable SNMPv1&v2c:

```
(config)#snmp-server v1-v2c enable
```

# 14.3 snmp-server v1-v2c host

## Description

The **snmp-server v1-v2c host** command is used to set the Get Trusted Host. The trusted IP address can serve as Get Community to read the SNMP information of this device.

To restore the Get Trusted Host value to the default (0.0.0.0), use the **no snmp-server v1-v2c host** command.

## Syntax

```
snmp-server v1-v2c host ip-address  
no snmp-server v1-v2c host
```

## Parameter

*ip-address*—— Enter a valid IPv4 address.

## Command Mode

Global Configuration Mode

## Example

Set "192.168.0.4" as the trusted host:

```
(config)#snmp-server v1-v2c host 192.168.0.4
```



## 14.4 snmp-server v1-v2c contact

### Description

The **snmp-server v1-v2c contact** command is used to set a textual identification of the contact person for this device. The default value is `www.tp-link.com`.

To delete your settings, use the **no snmp-server v1-v2c contact** command.

### Syntax

**snmp-server v1-v2c contact** *contact*

**no snmp-server v1-v2c contact**

### Parameter

*contact* — Enter a valid URL (a domain name).

### Command Mode

Global Configuration Mode

### Example

Delete the contact settings:

```
(config)#no snmp-server v1-v2c contact
```

## 14.5 snmp-server v1-v2c device-name

### Description

The **snmp-server v1-v2c device-name** command is used to set the device name for the SNMP settings.

To delete your settings, use the **no snmp-server v1-v2c device-name** command.

### Syntax

**snmp-server v1-v2c device-name** *device-name*

**no snmp-server v1-v2c device-name**

### Parameter

*device-name* — Enter a name for your router with 64 characters.

### Command Mode

Global Configuration Mode

## Example

Set the device name as "example":

```
(config)# snmp-server v1-v2c device-name example
```

## 14.6 snmp-server v1-v2c community

### Description

The **snmp-server v1-v2c community** command is used to set the Get Community for the SNMP settings.

To restore the Get Community value to the default (public), use the **no snmp-server v1-v2c community** command.

### Syntax

```
snmp-server v1-v2c community community
```

```
no snmp-server v1-v2c community
```

### Parameter

*community*—— Enter the community string with 64 characters.

### Command Mode

Global Configuration Mode

### Example

Add a community "public":

```
(config)# snmp-server v1-v2c community public
```

## 14.7 snmp-server v1-v2c location

### Description

The **snmp-server v1-v2c location** command is used to set the location of the SNMP server. For example, you can set the building, floor number, or room number as the location.

To delete the location, use the **no snmp-server v1-v2c location** command.

### Syntax

```
snmp-server v1-v2c location location
```

```
no snmp-server v1-v2c location
```

## Parameter

*location* — Specify the location string with 64 characters.

## Command Mode

Global Configuration Mode

## Example

Set the SNMP server location as "Building":

```
(config)# snmp-server v1-v2c location Building
```

# 14.8 show snmp-server

## Description

The **show snmp-server** command is used to display the SNMP server settings.

## Syntax

```
show snmp-server
```

## Command Mode

All

## Example

View the SNMP server information:

```
>enable  
#show snmp-server
```

# Chapter 15 HTTP and HTTPS Commands

With the help of HTTP (HyperText Transfer Protocol) or HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer), you can manage the switch through a standard browser.

## 15.1 ip http port

### Description

The **ip http port** command is used to configure the port number of the HTTP server within the router.

### Syntax

**ip http port** *port-num*

### Parameter

*port-num* — Enter the port number. This value ranges from 1024 to 65535, and cannot overlap with the HTTPS server port number.

### Command Mode

Global Configuration Mode

### Example

Set the port number of the HTTP server as "1800":

```
(config)# ip http port 1800
```

## 15.2 ip http server redirect-to-https

### Description

With the **ip http server redirect-to-https** command, you will access the web management interface by HTTPS protocol, which is considered as a more secured way.

To disable the Redirect HTTP to HTTPS function, please use the **no ip http server redirect-to-https** command.

### Syntax

**ip http server redirect-to-https**

**no ip http server redirect-to-https**

## Command Mode

Global Configuration Mode

## Example

Enable the Redirect HTTP to HTTPS function:

```
(config)#ip http server redirect-to-https
```

# 15.3 ip http secure-port

## Description

The **ip http secure-port** command is used to configure the port number of the HTTPS server within the router.

## Syntax

```
ip http secure-port port-num
```

## Parameter

*port-num* — Enter the port number. This value can be specified as 443, or 443-65535. It cannot overlap with the HTTP server port number.

## Command Mode

Global Configuration Mode

## Example

Set the port number of the HTTPS server as "2800":

```
(config)# ip http secure-port 2800
```

# 15.4 ip http secure-server

## Description

The **ip http secure-server** command is used to enable the HTTPS server, then you can access the management interface via HTTPS server.

To disable this function, please use the **no ip http secure-server** command.

## Syntax

```
ip http secure-server  
no ip http secure-server
```

## Command Mode

Global Configuration Mode

## Example

Enable the HTTPS server:

```
(config)# ip http secure- server
```

## 15.5 ip http session timeout

### Description

The **ip http session timeout** command is used to configure the web idle timeout. The web session will log out for security if there is no operation within the specified time.

### Syntax

```
ip http session timeout timeout
```

### Parameter

*timeout* — The timeout time, ranging from 5 to 60 in minutes. By default, the value is 6.

### Command Mode

Global Configuration Mode

### Example

Set the web idle timeout as "30" minutes:

```
(config)# ip http session timeout 30
```

## 15.6 show ip http configuration

### Description

The **show ip http configuration** command is used to display the settings of the HTTP server and the HTTPS server.

### Syntax

```
show ip http configuration
```

### Command Mode

All

## Example

View the settings of the HTTP server and the HTTPS server:

```
(config)# show ip http configuration
```

# Chapter 16 Time Management Commands

## 16.1 show time-range

### Description

The **show time-range** command is used to display the information of the existing time range entries.

### Syntax

```
show time-range
```

### Command Mode

Global Configuration Mode

### Example

View the information of the existing time range entries:

```
(config)#show time-range
```

## 16.2 time-range week- date time-slice

### Description

The **time-range week-date time-slice** command is used to create time range rules by specifying the period in a day and days in a week. The configured time range can be used for features like ACL, saving you from repeatedly setting up the same information.

To delete a time range entry, please use the **no time-range** command.

### Syntax

```
time-range name week-date daytime-slice time1 [time2] [time3] [time4]  
no time-range name
```

### Parameter

*name* — Enter a name for the time range entry within 16 characters with letters, digits, or underscores. The default time range named "Any" cannot be created, edited, or deleted, so "Any" cannot be entered in the command.

*day* — Enter the day in a week the time range takes effect. Supports sequential input from 1 to 7, and supports shorthand, such as "3-5", or "1,2-4".



*time1* — Enter a time slice in the 24-hour clock format. The starting time should not be greater than the ending time. The valid examples are 03:00-05:00, or 06:15-19:04.

*time2* — This field is optional. Enter the second time slice in the 24-hour clock format. The starting time should not be greater than the ending time, and the new time slice cannot overlap with the existing ones.

*time3* — This field is optional. Enter the third time slice in the 24-hour clock format. The starting time should not be greater than the ending time, and the new time slice cannot overlap with the existing ones.

*time4* — This field is optional. Enter the fourth time slice in the 24-hour clock format. The starting time should not be greater than the ending time, and the new time slice cannot overlap with the existing ones.

## Command Mode

Global Configuration Mode

## Example

Create a time range entry named "example", and let it work every Tuesday to Thursday, from 05:00 to 15:00, and 22:02-23:09:

```
(config)#time-range example week-date 2-4 time-slice 05:00-15:00
22:02-23:09
```

# 16.3 show system-time

## Description

The **show system-time** command is used to show system time, or the system time zone and the NTP server address.

## Syntax

```
show system-time [ntp]
```

## Parameter

**ntp** — This is optional. Enter this value, the system time zone and NTP server address will show. Otherwise, the system time will show.

## Command Mode

Global Configuration Mode

## Example

View the system time:

```
(config)#show system-time
```

View the system time zone and NTP server address:

```
(config)#show system-time ntp
```

## 16.4 system-time manual

### Description

The **system-time manual** command is used to set the system time according to your needs.

### Syntax

```
system-time manual time
```

### Parameter

*time* —— Enter your desired system time in the format of MM/DD/YYYY-HH:MM:SS

### Command Mode

Global Configuration Mode

### Example

Set the system time to "03/04/2005-06:07:08":

```
(config)#system-time manual 03/04/2005-06:07:08
```

## 16.5 system-time ntp timezone server

### Description

The **system-time ntp timezone server** command is used to set the system time zone and the NTP server. The router will get UTC automatically if it is connected to an NTP Server.

### Syntax

```
system-time ntp timezone timezone ntp-server1 ntp-server1 [ntp-server2  
ntp-server2]
```

### Parameter

*timezone* —— Specify a time zone. The range is from UTC-12:00 to UTC+13:00.

The detailed information of each time-zone are displayed:

UTC-12:00 —— TimeZone for International Date Line West.

UTC-11:00 —— TimeZone for Coordinated Universal Time-11.

UTC-10:00 — TimeZone for Hawaii.  
UTC-09:00 — TimeZone for Alaska.  
UTC-08:00 — TimeZone for Pacific Time (US Canada).  
UTC-07:00 — TimeZone for Mountain Time (US Canada).  
UTC-06:00 — TimeZone for Central Time (US Canada).  
UTC-05:00 — TimeZone for Eastern Time (US Canada).  
UTC-04:30 — TimeZone for Caracas.  
UTC-04:00 — TimeZone for Atlantic Time (Canada).  
UTC-03:30 — TimeZone for Newfoundland.  
UTC-03:00 — TimeZone for Buenos Aires, Salvador, Brasilia.  
UTC-02:00 — TimeZone for Mid-Atlantic.  
UTC-01:00 — TimeZone for Azores, Cape Verde Is.  
UTC — TimeZone for Dublin, Edinburgh, Lisbon, London.  
UTC+01:00 — TimeZone for Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna.  
UTC+02:00 — TimeZone for Cairo, Athens, Bucharest, Amman, Beirut, Jerusalem.  
UTC+03:00 — TimeZone for Kuwait, Riyadh, Baghdad.  
UTC+03:30 — TimeZone for Tehran.  
UTC+04:00 — TimeZone for Moscow, St.Petersburg, Volgograd, Tbilisi, Port Louis.  
UTC+04:30 — TimeZone for Kabul.  
UTC+05:00 — TimeZone for Islamabad, Karachi, Tashkent.  
UTC+05:30 — TimeZone for Chennai, Kolkata, Mumbai, New Delhi.  
UTC+05:45 — TimeZone for Kathmandu.  
UTC+06:00 — TimeZone for Dhaka, Astana, Ekaterinburg.  
UTC+06:30 — TimeZone for Yangon (Rangoon).  
UTC+07:00 — TimeZone for Novosibirsk, Bangkok, Hanoi, Jakarta.  
UTC+08:00 — TimeZone for Beijing, Chongqing, Hong Kong, Urumqi, Singapore.  
UTC+09:00 — TimeZone for Seoul, Irkutsk, Osaka, Sapporo, Tokyo.  
UTC+09:30 — TimeZone for Darwin, Adelaide.  
UTC+10:00 — TimeZone for Canberra, Melbourne, Sydney, Brisbane.  
UTC+11:00 — TimeZone for Solomon Is., New Caledonia, Vladivostok.  
UTC+12:00 — TimeZone for Fiji, Magadan, Auckland, Wellington.  
UTC+13:00 — TimeZone for Nuku'alofa, Samoa  
*ntp-server1* — The IP address of the primary NTP server.  
*ntp-server2* — The IP address of the secondary NTP server. This value is optional.

## Command Mode

Global Configuration Mode

## Example

Configure the system time mode as NTP, the time zone "UTC-12:00", the primary NTP server "133.100.9.2":

```
(config)#system-time ntp timezone UTC-12:00 ntp-server1 133.100.9.2
```

# Chapter 17 ARP Commands

## 17.1 show arp

### Description

The **show arp** command is used to display the ARP entry information.

### Syntax

```
show arp
```

### Command Mode

All

### Example

Display the ARP entry information:

```
(config)#show arp
```