



Milesight UR Series

Quagga vtysh CLI Reference Manual

View: This document covers only commands under the **configure terminal** (CONFIG_NODE) view.

Entry: Enter by executing **configure terminal** in vtysh.nbsp.

Contents

1. System & Management

- 1.1 Web Access Timeout
- 1.2 HTTP Access Control
- 1.3 HTTPS Access Control
- 1.4 Telnet Access Control
- 1.5 SSH Access Control
- 1.6 Remote Access Control

2. Network Status Query

- 2.1 Show WAN Port Running Info
- 2.2 Show WAN Port Configuration
- 2.3 Show WAN Port Name List
- 2.4 Show LAN Port Configuration
- 2.5 Show Ethernet Port Info
- 2.6 Show Ethernet Port Status
- 2.7 Show Unclassified Interface Info
- 2.8 Show Network Connection Status
- 2.9 Show Interface Name List
- 2.10 Show Interface Detailed Info
- 2.11 Show VLAN Interface Info
- 2.12 Show Switch Configuration
- 2.13 Show Switch Running Status
- 2.14 Show Switch Port Speed
- 2.15 Show Switch Port Duplex Mode
- 2.16 Show Switch Port Operating Mode
- 2.17 Show Bridge Member Ports
- 2.18 Show Bridge Configuration
- 2.19 Show Wi-Fi Channel List
- 2.20 Show Wi-Fi Interface Configuration
- 2.21 Show Wireless Client Association List
- 2.22 Show Wireless Access Point Info
- 2.23 Show DHCP Server Configuration
- 2.24 Show DHCP Address Binding Table
- 2.25 Show DHCP Server Running Status
- 2.26 Show DHCP Relay Information
- 2.27 Show Routing Table

3. Time & Synchronization

- 3.1 Set System Time Manually
- 3.2 Set Timezone Offset
- 3.3 Set Timezone Name
- 3.4 Set Timezone Type
- 3.5 NTP Immediate Sync
- 3.6 Configure NTP Primary Server
- 3.7 Configure NTP Secondary Server
- 3.8 NTP Sync Interval
- 3.9 GPS Time Sync Interval

4. Log Management

- 4.1 Remote Log Server
- 4.2 Console Logging
- 4.3 Local Storage Logging

4.4 External Storage Logging

4.5 Global Log Level

5. SNMP Management

5.1 SNMP Community string

5.2 SNMP Trap Destination

5.3 SNMP Contact & Location

5.4 Enable/Disable SNMP

6. User & Authentication (AAA)

6.1 Local User Management

6.2 RADIUS Server Configuration

6.3 TACACS+ Server Configuration

6.4 LDAP Server Configuration

6.5 AAA Authentication Policy

6.6 Apply AAA Configuration

7. Cellular Network

7.1 SMS Mode

7.2 SMS Polling Interval

7.3 Dial Redial Interval

7.4 Dial Max Retries

7.5 APN Configuration

7.6 Authentication Method

7.7 Dial Username/Password

7.8 PLMN Selection

7.9 LTE Band Configuration

7.10 SIM PIN Code

7.11 Data Usage Limit

7.12 Data Statistics Reset Day

7.13 ICMP Link Detection

7.14 Force Reload Module

8. PPP Dial-up

8.1 Create Dialer Interface

8.2 PPP Protocol type

8.3 PPP Authentication Configuration

8.4 PPP MTU/MRU

8.5 PPP Heartbeat Detection

8.6 NAT & Global Traffic Forwarding

9. WireGuard VPN

9.1 Enter WireGuard Interface Configuration

9.2 Interface IP Address

9.3 Listening Port

9.4 Private Key Configuration

9.5 DNS Configuration

9.6 MTU Setting

9.7 Peer Configuration

9.8 Enable/Disable Interface

10. GRE Tunnel

10.1 Enter GRE Tunnel Configuration

10.2 Tunnel Virtual IP

10.3 Tunnel MTU

10.4 Tunnel Key

10.5 Remote Subnet Route

10.6 NAT & Global Forwarding

10.7 Enable/Disable Tunnel

11. IPSec VPN

- 11.1 Enter IPSec Configuration
- 11.2 IPSec Encapsulation Mode
- 11.3 XAuth User Authentication
- 11.4 IKE Phase 1 Parameters
- 11.5 ESP Phase 2 Parameters
- 11.6 Enable/Disable IPSec

12. L2TP VPN

- 12.1 L2TP Server Address
- 12.2 L2TP Authentication Configuration
- 12.3 Pre-Shared Key
- 12.4 NAT Traversal
- 12.5 Enable/Disable L2TP

13. PPTP VPN

- 13.1 PPTP Server Address
- 13.2 PPTP Authentication Configuration
- 13.3 MPPE Encryption
- 13.4 Enable/Disable PPTP

14. OpenVPN Server

- 14.1 Enter OpenVPN Server Configuration
- 14.2 Transport Protocol & Port
- 14.3 Authentication Method
- 14.4 VPN Address Pool
- 14.5 Push Route
- 14.6 Encryption Algorithm
- 14.7 User Account Management
- 14.8 Client-to-Client
- 14.9 Renegotiation Time
- 14.10 CRL Certificate Revocation
- 14.11 Enable/Disable OpenVPN Server

15. OpenVPN Client

- 15.1 Enter OpenVPN Client Configuration
- 15.2 Server Address & Port
- 15.3 Client Authentication
- 15.4 TLS Configuration
- 15.5 Enable/Disable OpenVPN Client

16. Firewall Rules (ACL)

- 16.1 Standard ACL (1-99)
- 16.2 Extended ACL (100-199) — TCP/UDP
- 16.3 Extended ACL — ICMP
- 16.4 Extended ACL — Other Protocols
- 16.5 ACL Description
- 16.6 Delete ACL

17. Firewall DMZ

- 17.1 Configure DMZ Host
- 17.2 Enable/Disable DMZ

18. Firewall Port Mapping

- 18.1 Add Port Mapping Rule
- 18.2 Delete Port Mapping Rule
- 18.3 Enable/Disable Port Mapping

19. Firewall SPI

- 19.1 SPI Content Filtering
- 19.2 WAN Side Access Blocking

19.3 Enable/Disable SPI

20. Firewall MAC-IP Binding

20.1 Add MAC-IP Binding

20.2 Delete MAC-IP Binding

20.3 Enable/Disable MAC-IP Binding

21. Firewall Interface ACL

21.1 Register Interface ACL

22. Firewall Security Policy

22.1 Connection Rate Limiting

22.2 Max Connections

22.3 Port Scan Protection

23. QoS Traffic Control

23.1 Enter QoS Configuration

23.2 Total Bandwidth Setting

23.3 Default Traffic Class

23.4 Traffic Class Configuration

23.5 Traffic Matching Rules

23.6 Enable/Disable QoS

24. Policy-Based Routing

24.1 Add Policy Route Rule

24.2 Delete Policy Route Rule

25. VRRP High Availability

25.1 Configure VRRP Virtual IP

25.2 VRRP Priority

25.3 VRRP Advertisement Interval

25.4 VRRP Preempt Mode

25.5 VRRP ICMP Link Detection

25.6 VRRP Tracking

26. PoE Management

26.1 Enter PoE Configuration

26.2 Port Power Configuration

26.3 PoE ICMP Detection

26.4 Power-Cut Reboot Configuration

27. Low Power Management

27.1 Enter Low Power Configuration

27.2 Enable/Disable Low Power

27.3 Wake-up Source Configuration

27.4 Scheduled Wake-up Configuration

27.5 DI Wake-up Configuration

27.6 Low Power Action Configuration

28. MQTT Client

28.1 Enter MQTT Client Configuration

28.2 Enable MQTT Client

28.3 Server Connection Configuration

28.4 Authentication Configuration

28.5 TLS Encryption

28.6 Last Will Message

28.7 System Info Publishing

28.8 Log level

29. TR-069 Management

29.1 Enter TR-069 Configuration

29.2 ACS Server Configuration

29.3 CPE Authentication Configuration

29.4 Periodic Notification Configuration

29.5 Enable/Disable TR-069

30. GPS Positioning

30.1 Enter GPS Configuration

30.2 GPS Signal Source

30.3 GPS Coordinate System

30.4 GPS Debug Logging

30.5 Enable GPS

31. Cloud Management Platform

31.1 Cloud Platform Server Configuration

31.2 Cloud Platform Connection Protocol

31.3 Enable/Disable Cloud Management

32. Alarms & Events

32.1 Alarm Recording & Notification

32.2 Alarm SMS Phone Group

32.3 Alarm Email Group

32.4 Alarm MQTT Publishing

33. Email Groups

33.1 Create Email Group

33.2 Add Email Address

33.3 Delete Email Group

33.4 SMTP Server Configuration

34. Modbus RTU

34.1 Enter Modbus RTU Configuration

34.2 Slave ID

34.3 Serial Port Mode

34.4 DI/DO Address Mapping

34.5 Transmit/Receive Delay

34.6 Enable/Disable Modbus RTU

35. Modbus TCP

35.1 Enter Modbus TCP Configuration

35.2 Listening Port

35.3 DI/DO Address Mapping

35.4 Enable/Disable Modbus TCP

36. Modbus Master

36.1 Enter Modbus Master Configuration

36.2 Add Slave

36.3 Add Collection Instruction

37. USB Management

37.1 USB Link Control

38. Storage Management

38.1 Format Storage Media

38.2 Detect Storage Media

39. Python Applications

39.1 Python SDK Configuration

39.2 Application Management

39.3 Enable/Disable Python Runtime

40. Network Interface Basic Configuration

40.1 Set Interface Properties

40.2 Configure IPv4 Address

40.3 Configure IPv6 Address

40.4 Interface Description

40.5 Interface Bandwidth

- 40.6 Enable/Disable Interface
- 40.7 Link Detection
- 40.8 Multicast Support
- 40.9 Interface Monitor Interval

41. DHCP Client

- 41.1 Enable DHCP Client
- 41.2 DHCP Client ID
- 41.3 DHCP Hostname
- 41.4 Use DHCP Provided DNS
- 41.5 Release/Renew DHCP Lease
- 41.6 IPv6 DHCP Client

42. DHCP Server

- 42.1 Enable DHCP Service
- 42.2 Enter DHCP Server Configuration
- 42.3 Declare DHCP Subnet
- 42.4 Address Pool Range
- 42.5 Bind Interface
- 42.6 Default Gateway
- 42.7 DNS Server
- 42.8 Lease Time
- 42.9 Static Address Binding
- 42.10 Authoritative Mode
- 42.11 Enable/Disable Subnet

43. DHCP Relay

- 43.1 DHCP Relay Helper Address
- 43.2 Relay Listening Port
- 43.3 Relay Information Option

44. DNS Configuration

- 44.1 DNS Server Address
- 44.2 DNS Domain Name
- 44.3 DNS Forwarding

45. Static Routing

- 45.1 Add Static Route (CIDR Format)
- 45.2 Delete Static Route

46. VLAN Configuration

- 46.1 Create/Delete VLAN
- 46.2 Interface VLAN Mode
- 46.3 Access Interface VLAN
- 46.4 Trunk Interface Allowed VLAN
- 46.5 VLAN Interface (SVI)

47. Switch Configuration

- 47.1 Switch WAN Port VLAN
- 47.2 Port Join VLAN
- 47.3 Apply Switch Configuration

48. WiFi (WLAN) Configuration

- 48.1 Show WiFi Information
- 48.2 Configure SSID
- 48.3 WiFi Authentication Method
- 48.4 WiFi Encryption Method
- 48.5 WiFi Password
- 48.6 WiFi Channel
- 48.7 WiFi Transmit Power
- 48.8 Hide SSID

48.9 WiFi Max Clients

48.10 Enable/Disable WiFi

49. Bridge Configuration

49.1 Create Bridge Interface

49.2 Add Interface to Bridge

49.3 STP Spanning Tree Protocol

1. System & Management

1.1 Web Access Timeout

Function: Set the session timeout for the Web management interface

Syntax

```
1 ip web-access timeout <100-3600>
```

Parameters

Parameter	Description
<100-3600>	Timeout in seconds, range 100–3600

Notes

- After timeout, the user must log in to the Web interface again

Example

```
1 configure terminal
2 ip web-access timeout 600
```

1.2 HTTP Access Control

Function: Enable or disable HTTP access to the router management interface, with configurable port

Syntax

```
1 ip http access
2 no ip http access
3 ip http server port <1-65535>
```

Parameters

Parameter	Description
<1-65535>	HTTP service listening port, default: 80

Notes

- After disabling HTTP, the device can only be managed via HTTPS, SSH, or Telnet
- After changing the port, use the new port to access, e.g., <http://192.168.1.1:8080>

Example

```
1 configure terminal
2 ip http access
3 ip http server port 8080
```

1.3 HTTPS Access Control

Function: Enable or disable HTTPS access to the router management interface, with configurable port

Syntax

```
1 ip https access
2 no ip https access
3 ip https server port <1-65535>
```

Parameters

Parameter	Description
<1-65535>	HTTPS service listening port, default: 443

Notes

- It is recommended to use HTTPS instead of HTTP in production environments

Example

```
1 configure terminal
2 ip https access
3 ip https server port 443
```

1.4 Telnet Access Control

Function: Enable or disable Telnet access to the router, with configurable port

Syntax

```
1 ip telnet access
2 no ip telnet access
3 ip telnet server port <1-65535>
```

Parameters

Parameter	Description
<1-65535>	Telnet service listening port, default: 23

Notes

- Telnet is a plaintext protocol; SSH is recommended for production environments

Example

```
1 configure terminal
2 ip telnet access
3 ip telnet server port 23
```

1.5 SSH Access Control

Function: Enable or disable SSH access to the router, with configurable port

Syntax

```
1 ip ssh access
2 no ip ssh access
3 ip ssh server port <1-65535>
```

Parameters

Parameter	Description
<1-65535>	SSH service listening port, default: 22

Notes

- SSH is an encrypted protocol, recommended for remote management

Example

```
1 configure terminal
2 ip ssh access
3 ip ssh server port 22
```

1.6 Remote Access Control

Function: Control whether each management protocol allows access from the WAN side (remote)

Syntax

```
1 ip (http|https|telnet|ssh) remote access
2 no ip (http|https|telnet|ssh) remote access
```

Parameters

Parameter	Description
http	https

Notes

- By default, only LAN-side access is allowed. Carefully evaluate security risks before enabling remote access.

Example

```
1 configure terminal
2 ip ssh remote access
3 no ip http remote access
```

2. Network Status Query

This chapter covers network status query commands, including WAN/LAN port configuration, Ethernet port information, VLAN/Bridge/Wi-Fi interfaces, switch configuration, DHCP service, and routing table display commands.

2.1 Show WAN Port Running Info

Function: Display WAN port running status information (link status, IP, MAC, etc.)

Syntax

```
1 show wan port info [WORD]
```

Parameters

Parameter	Description
WORD (optional)	WAN port name, e.g., wan, sim1, sim2. When omitted, displays all WAN port information.

Usage Notes

- Execute under the configure terminal (CONFIG_NODE) view.
- Displays the port physical link status, assigned IP address, subnet mask, gateway, MTU, traffic statistics, etc.

Example

```
1 Router# configure terminal
2 Router(config)# show wan port info
```

2.2 Show WAN Port Configuration

Function: Display WAN port configuration information (static/dynamic assignment method, protocol type, etc.)

Syntax

```
1 show wan port config [WORD]
```

Parameters

Parameter	Description
WORD (optional)	WAN port name. When omitted, displays all WAN port configurations.

Example

```
1 Router(config)# show wan port config wan
```

2.3 Show WAN Port Name List

Function: Display the name list of all WAN ports in the system

Syntax

```
1 show wan port name
```

Example

```
1 Router(config)# show wan port name
```

2.4 Show LAN Port Configuration

Function: Display LAN port configuration information (IP address, subnet mask, DHCP mode, etc.)

Syntax

```
1 show lan port config [WORD]
```

Parameters

Parameter	Description
WORD (optional)	LAN port name, e.g., lan, lan0. When omitted, displays all LAN port configurations.

Example

```
1 Router(config)# show lan port config
```

2.5 Show Ethernet Port Info

Function: Display detailed running information of Ethernet ports

Syntax

```
1 show ethernet port info [WORD]
```

Parameters

Parameter	Description
WORD (optional)	Ethernet port name (e.g., eth0, eth1). When omitted, displays all Ethernet ports.

Example

```
1 Router(config)# show ethernet port info eth0
```

2.6 Show Ethernet Port Status

Function: Display current link status of Ethernet ports (Up/Down, speed, duplex mode, etc.)

Syntax

```
1 show ethernet port status [WORD]
```

Parameters

Parameter	Description
WORD (optional)	Port name. When omitted, displays all port statuses.

Example

```
1 Router(config)# show ethernet port status
```

2.7 Show Unclassified Interface Info

Function: Display information for unclassified (unspec) interfaces

Syntax

```
1 show unspec interface
```

Example

```
1 Router(config)# show unspec interface
```

2.8 Show Network Connection Status

Function: Display overall network connection status, including summary of interface IPs, DNS, default route, etc.

Syntax

```
1 show network status
```

Example

```
1 Router(config)# show network status
```

2.9 Show Interface Name List

Function: Display the name list of all interfaces in the system

Syntax

```
1 show interface name
```

Example

```
1 Router(config)# show interface name
```

2.10 Show Interface Detailed Info

Function: Display detailed interface configuration and running status (IP, MAC, MTU, packet statistics, etc.)

Syntax

```
1 show interface [IFNAME]
2 show interface vrf NAME
3 show interface description
```

Parameters

Parameter	Description
IFNAME (optional)	Interface name, e.g., eth0, br0, tun0. When omitted, displays all interfaces.
vrf NAME	Display interface information within the specified VRF.

Parameter	Description
description	Only display the interface description field.

Example

```
1 Router(config)# show interface
2 Router(config)# show interface eth0
3 Router(config)# show interface description
```

2.11 Show VLAN Interface Info

Function: Display VLAN interface configuration information (VLAN ID, parent physical interface, IP address, etc.)

Syntax

```
1 show vlan interface
```

Example

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

2.12 Show Switch Configuration

Function: Display global configuration information of the switch (Layer 2 switching), including port VLAN assignment, STP, etc.

Syntax

```
1 show switch config
```

Example

```
1 Router(config)# show switch config
```

2.13 Show Switch Running Status

Function: Display switch running status (port link status, traffic statistics, etc.)

Syntax

```
1 show switch status
```

Example

```
1 Router(config)# show switch status
```

2.14 Show Switch Port Speed

Function: Display the speed configuration of a specified switch port

Syntax

```
1 show switchport port speed WORD
```

Parameters

Parameter	Description
WORD	Port name, e.g., lan1, lan2.

Example

```
1 Router(config)# show switchport port speed lan1
```

2.15 Show Switch Port Duplex Mode

Function: Display the duplex mode of a specified switch port (full-duplex/half-duplex)

Syntax

```
1 show switchport port duplex WORD
```

Parameters

Parameter	Description
WORD	Port name.

Example

```
1 Router(config)# show switchport port duplex lan1
```

2.16 Show Switch Port Operating Mode

Function: Display the operating mode of a specified switch port (Access/Trunk, etc.)

Syntax

```
1 show switchport port mode WORD
```

Parameters

Parameter	Description
WORD	Port name.

Example

```
1 Router(config)# show switchport port mode lan1
```

2.17 Show Bridge Member Ports

Function: Display the member port list of Bridge interfaces

Syntax

```
1 show bridge members
```

Example

```
1 Router(config)# show bridge members
```

2.18 Show Bridge Configuration

Function: Display Bridge configuration information (STP status, forward delay, Hello time, etc.)

Syntax

```
1 show bridge config
```

Example

```
1 Router(config)# show bridge config
```

2.19 Show Wi-Fi Channel List

Function: Display the channel list supported by Wi-Fi wireless interfaces (2.4 GHz / 5 GHz)

Syntax

```
1 show dot11 channel-list
```

Example

```
1 Router(config)# show dot11 channel-list
```

2.20 Show Wi-Fi Interface Configuration

Function: Display Wi-Fi interface configuration information (SSID, band, channel, encryption method, etc.)

Syntax

```
1 show dot11 config
```

Example

```
1 Router(config)# show dot11 config
```

2.21 Show Wireless Client Association List

Function: Display the list of wireless clients currently connected to the AP

Syntax

```
1 show dot11 associations  
2 show dot11 sta associations
```

Description

show dot11 associations :Display associated clients of all wireless interfaces.

show dot11 sta associations :Display association information from the STA (Station) perspective.

Example

```
1 Router(config)# show dot11 associations  
2 Router(config)# show dot11 sta associations
```

2.22 Show Wireless Access Point Info

Function: Display wireless Access Point (AP) information configured in the system

Syntax

```
1 show dot11 access-points
```

Example

```
1 Router(config)# show dot11 access-points
```

2.23 Show DHCP Server Configuration

Function: Display DHCP server configuration information (address pool, lease time, options, etc.)

Syntax

```
1 show ip dhcp server config
```

Example

```
1 Router(config)# show ip dhcp server config
```

2.24 Show DHCP Address Binding Table

Function: Display the current DHCP server address binding table (IP-to-MAC mappings)

Syntax

```
1 show ip dhcp binding
```

Example

```
1 Router(config)# show ip dhcp binding
```

2.25 Show DHCP Server Running Status

Function: Display DHCP server running status (enabled/disabled, allocated leases, conflict statistics, etc.)

Syntax

```
1 show ip dhcp server status
```

Example

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

2.26 Show DHCP Relay Information

Function: Display DHCP Relay configuration and statistics

Syntax

```
1 show ip dhcp relay information
```

Example

```
1 Router(config)# show ip dhcp relay information
```

2.27 Show Routing Table

Function: Display routing table entries

Syntax

```
1 show ip route
2 show ip route A.B.C.D
3 show ip route A.B.C.D validity
```

Parameters

Parameter	Description
A.B.C.D (optional)	Destination network address, used to query a specific route entry.
validity (optional)	Used with destination address to display route validity information.

Usage Notes

- Display all routes in the kernel routing table, including directly connected routes, static routes, and routes learned via dynamic routing protocols (RIP/OSPF/BGP).
- Each route displays destination network, next hop, egress interface, metric, source protocol, etc.

Example

```
1 Router(config)# show ip route
2 Router(config)# show ip route 192.168.1.0
3 Router(config)# show ip route 10.0.0.0 validity
```

3. Time & Synchronization

3.1 Set System Time Manually

Function: Manually set the device system time

Syntax

```
1 clock set TIME
```

Parameters

Parameter	Description
TIME	Time string, format: YYYY.MM.DD-hh:mm:ss

Notes

- After manually setting the time, if NTP is enabled, it will be overwritten on the next sync

Example

```
1 configure terminal
2 clock set 2024.03.20-10:30:00
```

3.2 Set Timezone Offset

Function: Set the system timezone offset, e.g., UTC+8

Syntax

```
1 clock timezone WORD
```

Parameters

Parameter	Description
WORD	Timezone offset, format: UTC-8, UTC+5:30

Example

```
1 configure terminal
2 clock timezone UTC-8
```

3.3 Set Timezone Name

Function: Set the system timezone name (IANA timezone database name)

Syntax

```
1 clock zonename .LINE
```

Parameters

Parameter	Description
.LINE	Timezone name, e.g., Asia/Shanghai

Example

```
1 configure terminal
2 clock zonename Asia/Shanghai
```

3.4 Set Timezone Type

Function: Set the timezone type identifier

Syntax

```
1 clock timezone type WORD
```

Parameters

Parameter	Description
WORD	Timezone type string

Example

```
1 configure terminal
2 clock timezone type CST
```

3.5 NTP Immediate Sync

Function: Immediately trigger an NTP time synchronization

Syntax

```
1 ntp sync
```

Notes

- NTP server address must be configured first

Example

```
1 configure terminal
2 ntp sync
```

3.6 Configure NTP Primary Server

Function: Set the NTP primary server address

Syntax

```
1 ntp server ADDR
```

Parameters

Parameter	Description
ADDR	NTP server IP address or domain name

Example

```
1 configure terminal
2 ntp server pool.ntp.org
```

3.7 Configure NTP Secondary Server

Function: Set the NTP secondary server address, used when the primary server is unreachable

Syntax

```
1 ntp secondary-server ADDR
2 no ntp secondary-server
```

Parameters

Parameter	Description
ADDR	Secondary NTP server IP address or domain name

Example

```
1 configure terminal
2 ntp secondary-server time.cloudflare.com
```

3.8 NTP Sync Interval

Function: Set the NTP automatic synchronization interval

Syntax

```
1 ntp update-interval <0-1440>
```

Parameters

Parameter	Description
<0-1440>	Sync interval in minutes; 0 disables automatic sync

Example

```
1 configure terminal
2 ntp update-interval 60
```

3.9 GPS Time Sync Interval

Function: Set the GPS time synchronization interval

Syntax

```
1 gps sync interval <60-2678400>
```

Parameters

Parameter	Description
<60-2678400>	Sync interval in seconds, range: 60 seconds to 31 days

Example

```
1 configure terminal
2 gps sync interval 3600
```

4. Log Management

4.1 Remote Log Server

Function: Configure sending system logs to a remote Syslog server

Syntax

```
1 log server HOST port <1-65535>
2 no log server
```

Parameters

Parameter	Description
HOST	Remote log server IP address or domain name
<1-65535>	Syslog service port, default: 514

Notes

- Uses standard Syslog protocol (UDP)

Example

```
1 configure terminal
2 log server 192.168.1.100 port 514
```

4.2 Console Logging

Function: Enable or disable logging output to the console

Syntax

```
1 log console
2 no log console
```

Example

```
1 configure terminal
2 log console
```

4.3 Local Storage Logging

Function: Configure log storage to local Flash, and set the maximum space usage

Syntax

```
1 log storage local size <1-5120>
```

Parameters

Parameter	Description
<1-5120>	Maximum storage space in KB

Example

```
1 configure terminal
2 log storage local size 1024
```

4.4 External Storage Logging

Function: Configure log storage to TF card or SSD, and set the maximum space usage

Syntax

```
1 log storage (tfcardssd) size <1-512000>
```

Parameters

Parameter	Description
tfcardssd	Storage media types
<1-512000>	Maximum storage space in KB

Example

```
1 configure terminal
2 log storage tfcard size 102400
```

4.5 Global Log Level

Function: Set the system global log output level (follows Syslog standard levels)

Syntax

```
1 log global loglevel <0-7>
```

Parameters

Parameter	Description
<0-7>	Log level
0 = Emergency	
1 = Alert	
2 = Critical	
3 = Error	
4 = Warning	
5 = Notice	
6 = Informational	
7 = Debug	

Example

```
1 configure terminal
2 log global loglevel 6
```

5. SNMP Management

5.1 SNMP Community string

Function: Configure SNMPv1/v2c read-only or read-write community string

Syntax

```
1 snmp-server community WORD (ro|rw)
2 no snmp-server community WORD
```

Parameters

Parameter	Description
WORD	Community String

Parameter	Description
ro	Read-only permission
rw	Read-write permission

Notes

- It is recommended to change the default public/private community strings for better security

Example

```
1 configure terminal
2 snmp-server community mySecret ro
```

5.2 SNMP Trap Destination

Function: Configure the destination host for receiving SNMP Trap messages

Syntax

```
1 snmp-server host HOST (traps|informs) version (1|2c|3) COMMUNITY
2 no snmp-server host HOST
```

Parameters

Parameter	Description
HOST	Trap receiving server address
traps informs	Message type
version	SNMP version
COMMUNITY	Community string

Example

```
1 configure terminal
2 snmp-server host 192.168.1.200 traps version 2c public
```

5.3 SNMP Contact & Location

Function: Set the device management contact and physical location information (MIB-II sysContact/sysLocation)

Syntax

```
1 snmp-server contact .LINE
2 snmp-server location .LINE
```

Parameters

Parameter	Description
.LINE	Contact or location description string

Example

```
1 configure terminal
2 snmp-server contact admin@example.com
3 snmp-server location Server-Room-A
```

5.4 Enable/Disable SNMP

Function: Globally enable or disable the SNMP service

Syntax

```
1 snmp-server enable
2 no snmp-server enable
```

Example

```
1 configure terminal
2 snmp-server enable
```

6. User & Authentication (AAA)

6.1 Local User Management

Function: Create or delete local login users and passwords

Syntax

```
1 username USER password PASSWORD
2 no username USER password PASSWORD
```

Parameters

Parameter	Description
USER	Username
PASSWORD	Password

Notes

- Strong passwords are recommended (containing upper/lowercase letters, numbers, and special characters)

- When deleting a user, both username and password must be provided

Example

```
1 configure terminal
2 username admin password Admin@123
```

6.2 RADIUS Server Configuration

Function: Configure RADIUS authentication server address, port, and key

Syntax

```
1 radius-server host HOST
2 radius-server port <1-65535>
3 radius-server key WORD
```

Parameters

Parameter	Description
HOST	RADIUS server IP address
<1-65535>	Authentication port, default: 1812
WORD	Shared secret key

Example

```
configure terminal
radius-server host 192.168.1.10
radius-server port 1812
radius-server key myRadiuskey
```

6.3 TACACS+ Server Configuration

Function: Configure TACACS+ authentication server

Syntax

```
1 tacacs-server host HOST
2 tacacs-server port <1-65535>
3 tacacs-server key WORD
```

Parameters

Parameter	Description
HOST	TACACS+ server IP address
<1-65535>	Port, default: 49

Parameter	Description
WORD	Shared secret key

Example

```
configure terminal
tacacs-server host 192.168.1.11
tacacs-server port 49
tacacs-server key myTacacsKey
```

6.4 LDAP Server Configuration

Function: Configure LDAP authentication server address, port, and bind account

Syntax

```
1 ldap server host HOST
2 ldap server transport port <1-65535>
3 ldap server bind authenticate root-dn NAME password WORD
```

Parameters

Parameter	Description
HOST	LDAP server address
<1-65535>	Port, default: 389 (LDAPS: 636)
NAME	Bind DN (Distinguished Name)
WORD	Bind password

Example

```
configure terminal
ldap server host 192.168.1.12
ldap server transport port 389
ldap server bind authenticate root-dn cn=admin,dc=example,dc=com password ldapPass
```

6.5 AAA Authentication Policy

Function: Configure authentication method chains for different access methods (console, HTTP, SSH, Telnet), supporting up to three fallback levels

Syntax

```
1 aaa authentication (console|http|ssh|telnet) default (local|radius|tacacs+|ldap)
2 aaa authentication (console|http|ssh|telnet) default (local|radius|tacacs+|ldap)
3 (local |radius|tacacs+|ldap)
4 aaa authentication (console|http|ssh|telnet) default (local|radius|tacacs+|ldap)
5 (local |radius|tacacs+|ldap) (local |radius|tacacs+|ldap)
6 no aaa authentication (console|http|ssh|telnet) default
```

Parameters

Parameter	Description
console http ssh telnet	access methods
local radius tacacs+ ldap	Authentication methods, tried in order

Notes

- It is recommended to keep at least "local" as the final fallback to prevent login failures when remote authentication servers are unavailable

Example

```
1 configure terminal
2 aaa authentication ssh default radius local
3 aaa authentication http default ldap radius local
```

6.6 Apply AAA Configuration

Function: Apply AAA configuration changes immediately

Syntax

```
1 aaa apply
```

Example

```
1 configure terminal
2 aaa apply
```

7. Cellular Network

7.1 SMS Mode

Function: Set SMS send/receive mode to PDU or TEXT

Syntax

```
1 cellular sms mode (pdu|text)
```

Parameters

Parameter	Description
pdu	PDU encoding mode, supports multi-language characters
text	Text mode, ASCII only

Notes

- PDU mode is required for Chinese SMS messages

Example

```
1 configure terminal
2 cellular sms mode pdu
```

7.2 SMS Polling Interval

Function: Set SMS inbox polling interval

Syntax

```
1 cellular sms poll <0-3600>
```

Parameters

Parameter	Description
<0-3600>	Polling interval in seconds; 0 disables polling

Example

```
1 configure terminal
2 cellular sms poll 60
```

7.3 Dial Redial Interval

Function: Set the redial wait time after cellular dial failure

Syntax

```
1 cellular dial interval <0-3600>
```

Parameters

Parameter	Description
<0-3600>	Redial interval in seconds

Example

```
1 configure terminal
2 cellular dial interval 30
```

7.4 Dial Max Retries

Function: Set the maximum retry count after cellular dial failure

Syntax

```
1 cellular dial retries <1-3>
```

Parameters

Parameter	Description
<1-3>	Maximum retry count

Example

```
1 configure terminal
2 cellular dial retries 3
```

7.5 APN Configuration

Function: Configure the APN access point name for a specified SIM card slot

Syntax

```
1 cellular <1-2> networks apn WORD
```

Parameters

Parameter	Description
<1-2>	SIM card slot number
WORD	APN name, e.g., internet, cmnet

Example

```
1 configure terminal
2 cellular 1 networks apn cmnet
```

7.6 Authentication Method

Function: Set the cellular network PPP authentication method

Syntax

```
1 cellular <1-2> networks auth (none|pap|chap|mschapv2)
```

Parameters

Parameter	Description
<1-2>	SIM card slot number
none pap chap mschapv2	Authentication protocol

Example

```
1 configure terminal
2 cellular 1 networks auth chap
```

7.7 Dial Username/Password

Function: Set the username and password for cellular network dial-up authentication

Syntax

```
1 cellular <1-2> networks user WORD
2 cellular <1-2> networks password WORD
```

Parameters

Parameter	Description
<1-2>	SIM card slot number
WORD	Username or password

Example

```
1 configure terminal
2 cellular 1 networks user card
3 cellular 1 networks password card
```

7.8 PLMN Selection

Function: Manually specify the operator PLMN (Public Land Mobile Network) number

Syntax

```
1 cellular <1-2> plmn <0-999999>
```

Parameters

Parameter	Description
<1-2>	SIM card slot number
<0-999999>	PLMN number; 0 means automatic selection

Example

```
1 configure terminal
2 cellular 1 plmn 46000
```

7.9 LTE Band Configuration

Function: Restrict the LTE frequency bands used

Syntax

```
1 cellular <1-2> lte_band WORD
```

Parameters

Parameter	Description
<1-2>	SIM card slot number
WORD	Band mask string (hexadecimal)

Example

```
1 configure terminal
2 cellular 1 lte_band 80000
```

7.10 SIM PIN Code

Function: Configure SIM card PIN code

Syntax

```
1 cellular <1-2> pincod WORD
```

Parameters

Parameter	Description
<1-2>	SIM card slot number
WORD	4-8 digit PIN code

Notes

- After 3 incorrect PIN attempts, the card will be locked and require a PUK code to unlock

Example

```
1 configure terminal
2 cellular 1 pincode 1234
```

7.11 Data Usage Limit

Function: Set monthly data usage limit for cellular network

Syntax

```
1 cellular <1-2> flow limit <0-999999>
```

Parameters

Parameter	Description
<1-2>	SIM card slot number
<0-999999>	Data limit in MB; 0 means unlimited

Example

```
1 configure terminal
2 cellular 1 flow limit 10240
```

7.12 Data Statistics Reset Day

Function: Set the monthly data statistics reset date

Syntax

```
1 cellular <1-2> billing day <1-31>
```

Parameters

Parameter	Description
<1-2>	SIM card slot number
<1-31>	Monthly reset day

Example

```
1 configure terminal
2 cellular 1 billing day 1
```

7.13 ICMP Link Detection

Function: Configure ICMP ping-based detection of cellular link connectivity

Syntax

```
1 cellular <1-2> failover icmp
2 cellular <1-2> icmp server ADDR
3 cellular <1-2> icmp count <1-100>
4 cellular <1-2> icmp loss <1-100>
5 cellular <1-2> icmp intval <1-3600>
6 cellular <1-2> icmp timeout <1-60>
```

Parameters

Parameter	Description
ADDR	ICMP detection target IP
count	Number of packets sent
loss	Allowed packet loss percentage
intval	Detection interval (seconds)
timeout	Timeout (seconds)

Example

```
configure terminal
cellular 1 failover icmp
cellular 1 icmp server 8.8.8.8 cellular 1 icmp count 3
cellular 1 icmp loss 50
cellular 1 icmp intval 30 cellular 1 icmp timeout 5
```

7.14 Force Reload Module

Function: Force reload the cellular module

Syntax

```
1 cellular reload force
```

Notes

- This operation will interrupt the current cellular connection

Example

```
1 configure terminal
2 cellular reload force
```

8. PPP Dial-up

8.1 Create Dialer Interface

Function: Enter the configuration view for the specified dialer interface number

Syntax

```
1 interface-dialer INDEX
```

Parameters

Parameter	Description
INDEX	Dialer interface number

Example

```
1 configure terminal
2 interface-dialer 1
```

8.2 PPP Protocol type

Function: Set the PPP encapsulation protocol type

Syntax

```
1 protocol (pptp|l2tp|pppoe)
```

Parameters

Parameter	Description
pptp	Point-to-Point Tunneling Protocol
l2tp	Layer 2 Tunneling Protocol
pppoe	PPP over Ethernet

Example

```
1 configure terminal
2 interface-dialer 1
3 protocol pppoe
```

8.3 PPP Authentication Configuration

Function: Set PPP authentication method, username, and password

Syntax

```
1 authentication (pap|chap|mschapv2)
2 username USER
3 password PASSWORD
```

Parameters

Parameter	Description
pap chap mschapv2	Authentication
USER	Username
PASSWORD	Password

Example

```
configure terminal interface-dialer 1 authentication chap username broadband password
mypassword
```

8.4 PPP MTU/MRU

Function: Set PPP link MTU and MRU values

Syntax

```
1 mtu <64-1500>
2 mru <64-1500>
```

Parameters

Parameter	Description
<64-1500>	MTU/MRU in bytes

Notes

- For PPPoE, MTU is typically set to 1492

Example

```
configure terminal interface-dialer 1 mtu 1492
mru 1492
```

8.5 PPP Heartbeat Detection

Function: Configure PPP LCP Echo heartbeat detection parameters

Syntax

```
1 echo interval <1-3600>
2 echo max-retries <1-100>
```

Parameters

Parameter	Description
interval	Heartbeat send interval (seconds)
max-retries	Maximum failure count; connection is re-established after exceeding

Example

```
configure terminal interface-dialer 1 echo interval 30
echo max-retries 3
```

8.6 NAT & Global Traffic Forwarding

Function: Enable NAT or global traffic forwarding on the PPP interface

Syntax

```
1 nat
2 no nat
3 global traffic forwarding
4 no global traffic forwarding
```

Example

```
1 configure terminal
2 interface-dialer 1
3 nat
```

9. WireGuard VPN

9.1 Enter WireGuard Interface Configuration

Function: Enter the configuration view for a specified WireGuard interface

Syntax

```
1 wireguard (wg0|wg1|wg2)
```

Parameters

Parameter	Description
wg0 wg1 wg2	WireGuard interface names; up to 3 instances are supported

Example

```
1 configure terminal
2 wireguard wg0
```

9.2 Interface IP Address

Function: Set the local IP address for the WireGuard interface

Syntax

```
1 ip A.B.C.D/M
```

Parameters

Parameter	Description
A.B.C.D/M	IP address and mask in CIDR format

Example

```
1 wireguard wg0
2 ip 10.0.0.1/24
```

9.3 Listening Port

Function: Set the UDP port for WireGuard to listen on

Syntax

```
1 port <1-65535>
```

Parameters

Parameter	Description
<1-65535>	UDP listening port, default: 51820

Example

```
1 wireguard wg0
2 port 51820
```

9.4 Private Key Configuration

Function: Configure the private key for the WireGuard interface

Syntax

```
1 private-key enable
2 private-key disable
3 private-key KEY
4 no private-key
```

Parameters

Parameter	Description
enable	Enable private key (use stored private key)
disable	Disable private key
KEY	Base64-encoded private key string

Notes

- Private keys must be kept secure and should not be stored in plaintext in configuration files

Example

```
1 wireguard wg0
2 private-key enable
```

9.5 DNS Configuration

Function: Configure DNS server for the WireGuard interface

Syntax

```
1 dns A.B.C.D
2 wireguard dns apply
```

Parameters

Parameter	Description
A.B.C.D	DNS server IP address

Example

```
1 wireguard wg0
2 dns 8.8.8.8
3 wireguard dns apply
```

9.6 MTU Setting

Function: Set the WireGuard interface MTU

Syntax

```
1 mtu <576-1500>
```

Parameters

Parameter	Description
<576-1500>	MTU in bytes; WireGuard recommends 1420

Example

```
1 wireguard wg0 2 mtu 1420
```

9.7 Peer Configuration

Function: Add and configure a WireGuard peer

Syntax

```
1 peer NAME
2 public-key KEY
3 allowed-ips A.B.C.D/M
4 endpoint A.B.C.D
5 port <1-65535>
6 keepalive <0-65535>
7 psk KEY
8 route A.B.C.D/M
```

Parameters

Parameter	Description
NAME	Peer name identifier
public-key KEY	Peer Base64 public key
allowed-ips	Networks allowed to be routed through this peer
endpoint	Peer public IP address
port	Peer listening port
keepalive	Keepalive interval (seconds); 0 disables
psk	Pre-shared key (optional, enhances security)
route	Route added to the peer

Example

```
wireguard wg0
peer server1
public-key abc123...== endpoint 203.0.113.1
port 51820
allowed-ips 10.0.0.0/24 keepalive 25
```

9.8 Enable/Disable Interface

Function: Enable or disable the WireGuard interface

Syntax

```
1 no shutdown
2 shutdown
3 enable start
```

Example

10. GRE Tunnel

10.1 Enter GRE Tunnel Configuration

Function: Enter GRE tunnel configuration view (typically within interface configuration)

Syntax

```
1 tunnel source A.B.C.D
2 tunnel destination IP
```

Parameters

Parameter	Description
A.B.C.D	Local tunnel source IP address
IP	Remote tunnel destination IP address

Example

```
1 configure terminal
2 tunnel source 203.0.113.1
3 tunnel destination 203.0.113.2
```

10.2 Tunnel Virtual IP

Function: Set the virtual IP addresses at both ends of the GRE tunnel

Syntax

```
1 ip address local A.B.C.D A.B.C.D
2 ip address peer A.B.C.D
```

Parameters

Parameter	Description
First A.B.C.D	Local virtual IP
Second A.B.C.D	Subnet mask
peer A.B.C.D	Remote virtual IP

Example

```
1 ip address local 172.16.0.1 255.255.255.0
2 ip address peer 172.16.0.2
```

10.3 Tunnel MTU

Function: Set the GRE tunnel MTU value

Syntax

```
1 tunnel mtu <64-1500>
```

Parameters

Parameter	Description
<64-1500>	MTU in bytes; GRE encapsulation overhead is approximately 24 bytes, recommended setting: 1476

Example

```
1 tunnel mtu 1476
```

10.4 Tunnel Key

Function: Set the authentication key for the GRE tunnel

Syntax

```
1 tunnel key SECRET
2 no tunnel key
```

Parameters

Parameter	Description
SECRET	Tunnel key string

Notes

- The key must be identical on both ends

Example

```
1 tunnel key myGREkey123
```

10.5 Remote Subnet Route

Function: Add a remote subnet route reachable via the GRE tunnel

Syntax

```
1 remote subnet A.B.C.D A.B.C.D
2 no remote subnet
```

Parameters

Parameter	Description
First A.B.C.D	Remote network address
Second A.B.C.D	Subnet mask

Example

```
1 remote subnet 192.168.2.0 255.255.255.0
```

10.6 NAT & Global Forwarding

Function: Enable NAT or global traffic forwarding on the GRE tunnel

Syntax

```
1 nat
2 no nat
3 global traffic forwarding
4 no global traffic forwarding
```

Example

```
1 nat
2 global traffic forwarding
```

10.7 Enable/Disable Tunnel

Function: Enable or disable the GRE tunnel

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 no shutdown
2 enable startup
```

11. IPsec VPN

11.1 Enter IPsec Configuration

Function: Enter the configuration view for the specified IPsec crypto map number

Syntax

```
1 set crypto map <1-10>
```

Parameters

Parameter	Description
<1-10>	Crypto map number

Example

```
1 configure terminal
2 set crypto map 1
```

11.2 IPsec Encapsulation Mode

Function: Set the upper-layer encapsulation protocol for IPsec (can stack GRE or L2TP)

Syntax

```
1 over ipsec type (none|gre|l2tp)
```

Parameters

Parameter	Description
none	Pure IPsec
gre	GRE over IPsec
l2tp	L2TP over IPsec

Example

```
1 over ipsec type l2tp
```

11.3 XAuth User Authentication

Function: Configure IPsec XAuth extended authentication username and password

Syntax

```
1 ipsec-server xauth USERNAME PASSWORD
```

Parameters

Parameter	Description
USERNAME	XAuth Username
PASSWORD	XAuth Password

Example

```
1 ipsec-server xauth vpnuser vpnpass123
```

11.4 IKE Phase 1 Parameters

Function: Configure IKE Phase 1 (Main Mode/Aggressive Mode) parameters

Syntax

```
1 ike version (1|2)
2 ike mode (main|aggressive)
3 ike encryption (des|3des|aes128|aes256)
4 ike hash (md5 |sha1|sha256)
5 ike dh-group (1|2 |5 |14)
6 ike lifetime <60-86400>
```

Parameters

Parameter	Description
version	IKE version

Parameter	Description
mode	Negotiation mode
encryption	Encryption Algorithm
hash	Hash algorithm
dh-group	DH key exchange group
lifetime	SA lifetime (seconds)

Example

```
ike version 1
ike mode main
ike encryption aes256
ike hash sha256
ike dh-group 14
ike lifetime 86400
```

11.5 ESP Phase 2 Parameters

Function: Configure IPsec ESP Phase 2 parameters

Syntax

```
1 esp encryption (des|3des|aes128|aes256)
2 esp hash (md5 |sha1|sha256)
3 esp lifetime <60-86400>
```

Example

```
1 esp encryption aes256
2 esp hash sha256
3 esp lifetime 3600
```

11.6 Enable/Disable IPsec

Function: Enable or disable IPsec VPN

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 no shutdown
2 enable startup
```

12. L2TP VPN

12.1 L2TP Server Address

Function: Set the L2TP server IP address

Syntax

```
1 server A.B.C.D
```

Parameters

Parameter	Description
A.B.C.D	L2TP server IP address

Example

```
1 configure terminal
2 server 203.0.113.10
```

12.2 L2TP Authentication Configuration

Function: Set the username and password for the L2TP connection

Syntax

```
1 username USER
2 password PASSWORD
```

Parameters

Parameter	Description
USER	L2TP Username
PASSWORD	L2TP Password

Example

```
1 username l2tpuser
2 password l2tppass
```

12.3 Pre-Shared Key

Function: Set L2TP/IPSec Pre-Shared Key(PSK)

Syntax

```
1 preshared-key KEY
```

Parameters

Parameter	Description
KEY	Pre-shared key string

Notes

- The PSK must be identical on both ends

Example

```
1 preshared-key myL2TPsecret
```

12.4 NAT Traversal

Function: Enable L2TP NAT Traversal (NAT-T)

Syntax

```
1 nat-traversal  
2 no nat-traversal
```

Example

```
1 nat-traversal
```

12.5 Enable/Disable L2TP

Function: Enable or disable the L2TP VPN connection

Syntax

```
1 no shutdown  
2 shutdown  
3 enable startup  
4 no enable startup
```

Example

```
1 no shutdown  
2 enable startup
```

13. PPTP VPN

13.1 PPTP Server Address

Function: Set the PPTP server IP address

Syntax

```
1 server A.B.C.D
```

Parameters

Parameter	Description
A.B.C.D	PPTP server IP address

Example

```
1 configure terminal
2 server 203.0.113.20
```

13.2 PPTP Authentication Configuration

Function: Set the PPTP connection username and password

Syntax

```
1 username USER
2 password PASSWORD
```

Example

```
1 username pptpuser
2 password pptppass
```

13.3 MPPE Encryption

Function: Enable or disable MPPE data encryption for PPTP

Syntax

```
1 mppe
2 no mppe
```

Notes

- MPPE requires MS-CHAPv2 authentication

Example

```
1 mppe
```

13.4 Enable/Disable PPTP

Function: Enable or disable the PPTP VPN connection

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 no shutdown
2 enable startup
```

14. OpenVPN Server

14.1 Enter OpenVPN Server Configuration

Function: Enter the OpenVPN server configuration view.

Syntax

```
1 openvpn server
```

Example

```
1 configure terminal
2 openvpn server
```

14.2 Transport Protocol & Port

Function: Set the transport protocol and listening port for OpenVPN

Syntax

```
1 protocol (tcp|udp)
2 port <1-65535>
```

Parameters

Parameter	Description
tcp udp	Transport protocols, UDP offers better performance, whilst TCP provides greater penetration.

Parameter	Description
<1-65535>	Listening port, default: 1194

Example

```
1 protocol udp
2 port 1194
```

14.3 Authentication Method

Function: Set the OpenVPN client authentication method

Syntax

```
1 authentication (none|password|certificate)
```

Parameters

Parameter	Description
none	No authentication
password	Username/password authentication
certificate	Certificate authentication

Example

```
1 authentication certificate
```

14.4 VPN Address Pool

Function: Set the IP address pool assigned to OpenVPN clients

Syntax

```
1 server A.B.C.D A.B.C.D
```

Parameters

Parameter	Description
First A.B.C.D	Address pool network address
Second A.B.C.D	Subnet mask

Example

```
1 server 10.8.0.0 255.255.255.0
```

14.5 Push Route

Function: Push routes to clients, directing client traffic through the VPN

Syntax

```
1 push route A.B.C.D A.B.C.D
```

Parameters

Parameter	Description
First A.B.C.D	Destination network address
Second A.B.C.D	Subnet mask

Example

```
1 push route 192.168.1.0 255.255.255.0
```

14.6 Encryption Algorithm

Function: Set the OpenVPN data channel encryption algorithm

Syntax

```
1 cipher (AES-128-CBC|AES-256-CBC|DES-CBC|3DES-CBC)
```

Example

```
1 cipher AES-256-CBC
```

14.7 User Account Management

Function: Add or delete OpenVPN user accounts (password authentication mode)

Syntax

```
1 username USER password PASSWORD  
2 no username USER password PASSWORD
```

Parameters

Parameter	Description
USER	Username

Parameter	Description
PASSWORD	Password

Example

```
1 username vpnclient1 password Client@123
```

14.8 Client-to-Client

Function: Allow or deny communication between OpenVPN clients

Syntax

```
1 client-to-client  
2 no client-to-client
```

Example

```
1 client-to-client
```

14.9 Renegotiation Time

Function: Set the OpenVPN key renegotiation interval

Syntax

```
1 renegotiation time <0-86400>
```

Parameters

Parameter	Description
<0-86400>	Renegotiation interval (seconds); 0 disables

Example

```
1 renegotiation time 3600
```

14.10 CRL Certificate Revocation

Function: Enable or disable Certificate Revocation List (CRL) checking

Syntax

```
1 CRL  
2 no CRL
```

Example

```
1 CRL
```

14.11 Enable/Disable OpenVPN Server

Function: Enable or disable the OpenVPN server.

Syntax

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 no shutdown
2 enable startup
```

15. OpenVPN Client

15.1 Enter OpenVPN Client Configuration

Function: Enter the OpenVPN client configuration view.

Syntax

```
1 openvpn client
```

Example

```
1 configure terminal
2 openvpn client
```

15.2 Server Address & Port

Function: Set the OpenVPN server address and port to connect to

Syntax

```
1 remote A.B.C.D
2 port <1-65535>
3 protocol (tcp|udp)
```

Parameters

Parameter	Description
A.B.C.D	OpenVPN server IP address
<1-65535>	Server port
tcp udp	Transport protocol

Example

```
1 remote 203.0.113.50
2 port 1194
3 protocol udp
```

15.3 Client Authentication

Function: Set OpenVPN ClientUsernamePassword

Syntax

```
1 username USER
2 password PASSWORD
```

Example

```
1 username vpnclient
2 password myVPNpass
```

15.4 TLS Configuration

Function: Configure the OpenVPN TLS encryption mode

Syntax

```
1 tls-mode (tls|tls-auth|tls-crypt)
```

Parameters

Parameter	Description
tls	Standard TLS
tls-auth	TLS + HMAC authentication
tls-crypt	TLS + encryption authentication (more secure)

Example

```
1 tls-mode tls-crypt
```

15.5 Enable/Disable OpenVPN Client

Function: Enable or disable the OpenVPN client connection.

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 no shutdown
2 enable startup
```

16. Firewall Rules (ACL)

16.1 Standard ACL (1-99)

Function: Create a standard ACL rule, filtering based on source IP address

Syntax

```
1 firewall-acl <1-99> (permit|deny) A.B.C.D A.B.C.D
2 firewall-acl <1-99> (permit|deny) any
```

Parameters

Parameter	Description
<1-99>	ACL group number (standard ACL)
permit deny	Permit or deny
A.B.C.D A.B.C.D	Source IP address and wildcard mask
any	Match all source addresses

Notes

- Standard ACLs only match source IP; extended ACLs (100-199) support more matching conditions
- ACL rules are matched in order, with an implicit deny all at the end

Example

```
1 configure terminal
2 firewall-acl 10 permit 192.168.1.0 0.0.0.255
3 firewall-acl 10 deny any
```

16.2 Extended ACL (100-199) — TCP/UDP

Function: Create an extended ACL rule, filtering based on protocol, source/destination IP, and port

Syntax

```
1 firewall-acl <100-199> (permit|deny) (tcp|udp) A.B.C.D A.B.C.D eq <1-65535>
2 A.B.C.D A.B.C.D eq <1-65535>
3 firewall-acl <100-199> (permit|deny) (tcp|udp) any eq <1-65535> any eq <1-65535>
4 firewall-acl <100-199> (permit|deny) (tcp|udp) A.B.C.D A.B.C.D A.B.C.D A.B.C.D
```

Parameters

Parameter	Description
<100-199>	ACL group number (extended ACL)
permit deny	Permit or deny
tcp udp	Transport protocol
A.B.C.D A.B.C.D	IP address and wildcard mask
eq <1-65535>	Exact port number match
any	Match any address

Example

```
1 configure terminal
2 firewall-acl 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
3 firewall-acl 100 deny tcp any any eq 23
```

16.3 Extended ACL — ICMP

Function: Create an extended ACL rule based on ICMP protocol

Syntax

```
1 firewall-acl <100-199> (permit|deny) icmp A.B.C.D A.B.C.D A.B.C.D A.B.C.D
2 firewall-acl <100-199> (permit|deny) icmp any any
```

Example

```
1 configure terminal
2 firewall-acl 101 permit icmp 192.168.1.0 0.0.0.255 any
3 firewall-acl 101 deny icmp any any
```

16.4 Extended ACL — Other Protocols

Function: Create an extended ACL rule based on protocol number

Syntax

```
1 firewall-acl <100-199> (permit|deny) <0-255> A.B.C.D A.B.C.D A.B.C.D A.B.C.D
2 firewall-acl <100-199> (permit|deny) <0-255> any any
```

Parameters

Parameter	Description
<0-255>	IP protocol number (e.g., 6=TCP, 17=UDP, 1=ICMP, 47=GRE)

Example

```
1 configure terminal
2 firewall-acl 102 permit 47 any any
```

16.5 ACL Description

Function: Add a description to an ACL group

Syntax

```
1 firewall-acl <1-99> remark DESC
2 firewall-acl <100-199> remark DESC
3 no firewall-acl <1-199> remark
```

Parameters

Parameter	Description
DESC	Description string

Example

```
1 configure terminal
2 firewall-acl 100 remark Allow-HTTP-from-LAN
```

16.6 Delete ACL

Function: Delete an entire ACL group or a specific rule within a group

Syntax

```
1 no firewall-acl <1-199>
2 no firewall-acl id <1-199> index <1-127>
```

Parameters

Parameter	Description
id	ACL group number
index	Rule index within the group

Example

```
1 configure terminal
2 no firewall-acl 100
3 no firewall-acl id 101 index 3
```

17. Firewall DMZ

17.1 Configure DMZ Host

Function: Forward all inbound traffic that does not match port mapping rules to the specified DMZ host

Syntax

```
1 firewall dmz SRC A.B.C.D
2 no firewall dmz
```

Parameters

Parameter	Description
SRC	WAN interface name or "any"
A.B.C.D	DMZ host IP address

Notes

- The DMZ host will be exposed to all inbound traffic not handled by port mapping rules; ensure the host is properly secured
- Only one DMZ host can be configured at a time

Example

```
1 configure terminal
2 firewall dmz any 192.168.1.100
```

17.2 Enable/Disable DMZ

Function: Enable or disable the DMZ function

Syntax

```
1 firewall dmz no shutdown
2 firewall dmz shutdown
3 firewall dmz startup
4 firewall dmz no startup
```

Example

```
1 configure terminal
2 firewall dmz no shutdown
3 firewall dmz startup
```

18. Firewall Port Mapping

18.1 Add Port Mapping Rule

Function: Forward traffic from a specific external port to an internal host (DNAT/port forwarding)

Syntax

```
1 firewall port-mapping NAME protocol (tcp|udp|tcp-udp) external-port <1-65535>
2 internal-ip A.B.C.D internal-port <1-65535>
```

Parameters

Parameter	Description
NAME	Rule name
tcp udp tcp-udp	Protocol type
external-port	External listening port
internal-ip	Internal destination host IP
internal-port	Internal destination port

Notes

- External port must not conflict with system management ports (e.g., 22, 80, 443)

Example

```
1 configure terminal
2 firewall port-mapping web-server protocol tcp external-port 8080 internal-ip
3 192.168.1.10 internal-port 80
```

18.2 Delete Port Mapping Rule

Function: Delete the port mapping rule with the specified name

Syntax

```
1 no firewall port-mapping NAME
```

Example

```
1 configure terminal
2 no firewall port-mapping web-server
```

18.3 Enable/Disable Port Mapping

Function: Enable or disable the port mapping function

Syntax

```
1 firewall port-mapping startup
2 firewall port-mapping no startup
```

Example

```
1 configure terminal
2 firewall port-mapping startup
```

19. Firewall SPI

19.1 SPI Content Filtering

Function: Enable SPI deep packet inspection content filtering to block specific types of traffic

Syntax

```
1 firewall spi filter (proxy|cookies|java|activex)
2 no firewall spi filter (proxy|cookies|java|activex)
```

Parameters

Parameter	Description
proxy	Filter proxy traffic
cookies	Filter Cookies
java	Filter Java Applets
activex	Filter ActiveX controls

Example

```
1 configure terminal
2 firewall spi filter java
3 firewall spi filter activex
```

19.2 WAN Side Access Blocking

Function: Block specific types of access from the WAN side

Syntax

```
1 firewall spi block (wan-ping|wan-nat|wan-snmp|wan-multicast|wan-ident|wan- 2 ipsec|wan-  
openvpn)  
3 no firewall spi block (wan-ping|wan-nat|wan-snmp|wan-multicast|wan-ident|wan- 4 ipsec|wan-  
openvpn)
```

Parameters

Parameter	Description
wan-ping	Block WAN-side Ping
wan-net	Block WAN-side NAT traversal
wan-snmp	Block WAN-side SNMP access
wan-multicast	Block WAN-side multicast
wan-ident	Block Ident protocol
wan-ipsec	Block WAN-side IPSec
wan-openvpn	Block WAN-side OpenVPN

Example

```
1 configure terminal  
2 firewall spi block wan-ping  
3 firewall spi block wan-snmp
```

19.3 Enable/Disable SPI

Function: Globally enable or disable the SPI firewall

Syntax

```
1 firewall spi (enable|disable)  
2 firewall spi startup  
3 no firewall spi startup
```

Example

```
1 configure terminal  
2 firewall spi enable  
3 firewall spi startup
```

20. Firewall MAC-IP Binding

20.1 Add MAC-IP Binding

Function: Bind a specified MAC address to an IP address to prevent IP spoofing

Syntax

```
1 firewall mac-ip bind MAC A.B.C.D
```

Parameters

Parameter	Description
MAC	MAC address, format: XX:XX:XX:XX:XX:XX
A.B.C.D	Bound IP address

Notes

- After binding, this MAC address can only use the specified IP; traffic with other IPs will be dropped

Example

```
1 configure terminal
2 firewall mac-ip bind 00:11:22:33:44:55 192.168.1.50
```

20.2 Delete MAC-IP Binding

Function: Delete the specified MAC-IP binding rule

Syntax

```
1 no firewall mac-ip bind MAC
```

Example

```
1 configure terminal
2 no firewall mac-ip bind 00:11:22:33:44:55
```

20.3 Enable/Disable MAC-IP Binding

Function: Globally enable or disable the MAC-IP binding function

Syntax

```
1 firewall mac-ip startup
2 no firewall mac-ip startup
```

Example

```
1 configure terminal
2 firewall mac-ip startup
```

21. Firewall Interface ACL

21.1 Register Interface ACL

Function: Apply an ACL to the inbound or outbound direction of a specified interface

Syntax

```
1 firewall-acl register interface IFNAME
2 ip access-group <1-199> (in|out)
3 no ip access-group (in|out)
```

Parameters

Parameter	Description
IFNAME	Interface name, e.g., eth0, ppp0
<1-199>	ACL group number
in out	Apply direction

Example

```
1 configure terminal
2 firewall-acl register interface eth0
3 ip access-group 100 in
```

22. Firewall Security Policy

22.1 Connection Rate Limiting

Function: Limit the number of new connections per second to prevent DoS attacks

Syntax

```
1 firewall security connection-rate-limit <1-65535>
2 no firewall security connection-rate-limit
```

Parameters

Parameter	Description
<1-65535>	Maximum new connections per second

Example

```
1 configure terminal
2 firewall security connection-rate-limit 1000
```

22.2 Max Connections

Function: Limit the maximum number of concurrent connections

Syntax

```
1 firewall security max-connections <1-65535>
2 no firewall security max-connections
```

Example

```
1 configure terminal
2 firewall security max-connections 10000
```

22.3 Port Scan Protection

Function: Enable port scan detection and protection

Syntax

```
1 firewall security port-scan (enable|disable)
```

Example

```
1 configure terminal
2 firewall security port-scan enable
```

23. QoS Traffic Control

23.1 Enter QoS Configuration

Function: Enter the uplink or downlink QoS configuration view

Syntax

```
1 qos (upload|download)
```

Parameters

Parameter	Description
upload	Uplink traffic QoS
download	Downlink traffic QoS

Example

```
1 configure terminal
2 qos upload
```

23.2 Total Bandwidth Setting

Function: Set the total bandwidth cap for QoS control

Syntax

```
1 total-bandwidth <0-8000000>
```

Parameters

Parameter	Description
<0-8000000>	Bandwidth value in Kbps; 0 means unlimited

Example

```
1 qos upload
2 total-bandwidth 100000
```

23.3 Default Traffic Class

Function: Set the default class for traffic that does not match any rules

Syntax

```
1 default-class NAME
```

Parameters

Parameter	Description
NAME	Default traffic class name

Example

```
1 qos upload
2 default-class default
```

23.4 Traffic Class Configuration

Function: Define a QoS traffic class with its bandwidth guarantee and ceiling

Syntax

```
1 class NAME
2 bandwidth <0-8000000>
3 ceiling <0-8000000>
4 priority <0-7>
```

Parameters

Parameter	Description
NAME	Traffic class name
bandwidth	Guaranteed bandwidth (Kbps)
ceiling	Maximum bandwidth (Kbps)
priority	Priority; 0 is lowest, 7 is highest

Example

```
qos upload
class voip
bandwidth 2000 ceiling 5000
priority 7
```

23.5 Traffic Matching Rules

Function: Add matching conditions for a traffic class (IP, port, protocol, etc.)

Syntax

```
1 match NAME (src-ip|dst-ip) A.B.C.D/M
2 match NAME (src-port|dst-port) <1-65535>
3 match NAME protocol (tcp|udp|icmp)
```

Parameters

Parameter	Description
NAME	Match rule name
A.B.C.D/M	IP address/mask (CIDR)
<1-65535>	Port number

Example

```
qos upload class voip
match voip-match dst-port 5060
match voip-rtsp protocol udp
```

23.6 Enable/Disable QoS

Function: Enable or disable QoS traffic control

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 qos upload
2 no shutdown
3 enable startup
```

24. Policy-Based Routing

24.1 Add Policy Route Rule

Function: Add a policy routing rule based on source IP, destination IP, or ingress interface to direct traffic to a specified routing table

Syntax

```
1 policy_route priority <1-255> source A.B.C.D/M
2 policy_route priority <1-255> dest A.B.C.D/M
3 policy_route priority <1-255> ifname IFNAME
```

Parameters

Parameter	Description
<1-255>	Rule priority; lower values have higher priority
source A.B.C.D/M	Match source IP network
dest A.B.C.D/M	Match destination IP network
ifname IFNAME	Match ingress interface name

Notes

- Policy routing takes precedence over the regular routing table
- Only one rule is allowed per priority level

Example

```
1 configure terminal
2 policy_route priority 10 source 192.168.2.0/24
3 policy_route priority 20 ifname eth1
```

24.2 Delete Policy Route Rule

Function: Delete the policy route rule with the specified priority

Syntax

```
1 no policy_route priority INDEX
```

Parameters

Parameter	Description
INDEX	Rule priority number

Example

```
1 configure terminal
2 no policy_route priority 10
```

25. VRRP High Availability

25.1 Configure VRRP Virtual IP

Function: Configure a virtual IP address for the specified VRRP group

Syntax

```
1 vrrp <1-255> ip A.B.C.D
```

Parameters

Parameter	Description
<1-255>	VRRP group ID
A.B.C.D	Virtual IP address

Notes

- All routers in the same VRRP group must have the same virtual IP
- The virtual IP must not be the same as the interface real IP

Example

```
1 configure terminal
2 vrrp 1 ip 192.168.1.254
```

25.2 VRRP Priority

Function: Set the priority of this router in the VRRP group; the highest priority becomes Master

Syntax

```
1 vrrp <1-255> priority <1-254>
```

Parameters

Parameter	Description
<1-255>	VRRP group ID
<1-254>	Priority, default: 100; 254 is the highest

Example

```
1 configure terminal
2 vrrp 1 priority 150
```

25.3 VRRP Advertisement Interval

Function: Set the interval at which the VRRP Master sends advertisement messages

Syntax

```
1 vrrp <1-255> advertise <1-255>
```

Parameters

Parameter	Description
<1-255> (second)	Advertisement interval in seconds, default: 1

Example

```
1 configure terminal
2 vrrp 1 advertise 1
```

25.4 VRRP Preempt Mode

Function: Enable or disable VRRP preempt mode. When enabled, a higher-priority router will re-preempt the Master role upon recovery

Syntax

```
1 vrrp <1-255> preempt
2 no vrrp <1-255> preempt
```

Example

```
1 configure terminal
2 vrrp 1 preempt
```

25.5 VRRP ICMP Link Detection

Function: Configure VRRP to detect uplink status via ICMP; on link failure, priority is automatically lowered to trigger a switchover

Syntax

```
1 icmp main-server A.B.C.D
2 icmp secondary-server A.B.C.D 3 icmp period <1-3600>
4 icmp interval <1-60>
5 icmp timeout <1-60>
6 icmp times <1-100>
```

Parameters

Parameter	Description
main-server	Primary detection target IP
secondary-server	Secondary detection target IP
period	Detection period (seconds)
interval	Packet send interval (seconds)
timeout	Timeout (seconds)
times	Failure count threshold

Example

```
configure terminal
icmp main-server 8.8.8.8
icmp period 30
icmp interval 3
icmp timeout 2
icmp times 3
```

25.6 VRRP Tracking

Function: Configure VRRP tracking objects; on tracked object failure, VRRP priority is automatically lowered

Syntax

```
1 track id <1-255>
2 no track
```

Parameters

Parameter	Description
<1-255>	Tracking object ID

Example

```
1 configure terminal
2 track id 1
```

26. PoE Management

26.1 Enter PoE Configuration

Function: Enter the PoE (Power over Ethernet) configuration view

Syntax

```
1 poe
```

Example

```
1 configure terminal
2 poe
```

26.2 Port Power Configuration

Function: Set PoE port power switch, priority, and maximum power

Syntax

```
1 set power conf (enable|disable)
2 set priority conf (low|high|critical)
3 set max power <1-30>
```

Parameters

Parameter	Description
enable disable	Enable or disable power supply
low high critical	Power supply priority
<1-30>	Maximum power supply (Watts)

Example

```
set power conf enable
set priority conf high
set max power 15
```

26.3 PoE ICMP Detection

Function: Configure PoE port ICMP detection of powered device status; auto power-cycle on device unresponsiveness

Syntax

```
1 set icmp enable
2 set icmp dest A.B.C.D
3 set icmp interval <1-3600>
4 set icmp retry interval <1-3600>
5 set icmp timeout <1-60>
6 set icmp times <1-100>
```

Parameters

Parameter	Description
dest	Powered device IP address
interval	Detection interval (seconds)
retry interval	Retry interval (seconds)
timeout	Timeout (seconds)
times	Failure count threshold

Example

```
set icmp enable
set icmp dest 192.168.1.200
set icmp interval 30
set icmp timeout 5
set icmp times 3
```

26.4 Power-Cut Reboot Configuration

Function: Configure PoE port power-cut reboot interval and maximum reboot count

Syntax

```
1 set power cut interval <1-3600>
2 set reboot times <0-100>
```

Parameters

Parameter	Description
power cut interval	Power-cut duration (seconds)
reboot times	Maximum reboot count; 0 means unlimited

Example

```
1 poe
```

27. Low Power Management

27.1 Enter Low Power Configuration

Function: Enter the low power mode configuration view

Syntax

```
1 power management
```

Example

```
1 configure terminal
2 power management
```

27.2 Enable/Disable Low Power

Function: Globally enable or disable low power mode

Syntax

```
1 enable low-power
2 no enable low-power
```

Example

```
1 power management
2 enable low-power
```

27.3 Wake-up Source Configuration

Function: Configure wake-up triggers for the device from low power state

Syntax

```
1 wakeup by (time|di |cellular|serial |ethernet)
```

Parameters

Parameter	Description
time	Scheduled wake-up
di	Digital Input (DI) signal wake-up
cellular	Cellular network event wake-up
serial	Serial port data wake-up
ethernet	Ethernet data wake-up

Example

```
1 power management
2 wakeup by time
3 wakeup by di
```

27.4 Scheduled Wake-up Configuration

Function: Configure Scheduled wake-up

Syntax

```
1 time mode (interval |schedule)
2 wakeup time HH:MM:SS
3 standby time HH:MM:SS
```

Parameters

Parameter	Description
interval	Wake up at periodic intervals
schedule	Wake up at a scheduled time
HH:MM:SS	Time format

Example

```
power management
time mode schedule
wakeup time 08:00:00
standby time 18:00:00
```

27.5 DI Wake-up Configuration

Function: Configure the level and duration for Digital Input (DI) triggered wake-up

Syntax

```
1 di level (high|low)
2 di duration <1-3600>
3 di mode (wakeup|standby|both)
```

Parameters

Parameter	Description
high low	Trigger level
<1-3600>	Trigger duration (seconds)
wakeup standby both	Trigger mode

Example

```
power management di level high
di duration 5
di mode wakeup
```

27.6 Low Power Action Configuration

Function: Configure actions triggered when entering standby or waking up (SMS/Email/DO output)

Syntax

```
1 action (standby|wakeup) (sms|email |do)
```

Parameters

Parameter	Description
standby wakeup	Trigger conditions
sms	Send SMS notification
email	Send email notification
do	Trigger Digital Output (DO)

Example

```
1 power management
2 action wakeup sms
3 action standby email
```

28. MQTT Client

28.1 Enter MQTT Client Configuration

Function: Enter the MQTT client configuration view.

Syntax

Syntax

```
1 mqtt-client
```

Example

```
1 configure terminal
2 mqtt-client
```

28.2 Enable MQTT Client

Function: Enable the MQTT client instance with the specified name

Syntax

```
1 enable client-name NAME
```

Parameters

Parameter	Description
NAME	MQTT client instance name

Example

```
1 mqtt-client
2 enable client-name myBroker
```

28.3 Server Connection Configuration

Function: Configure MQTT Broker server address, port, and connection parameters

Syntax

```
1 server-ip A.B.C.D
2 port <1-65535>
3 clientid NAME
4 timeout <1-3600>
5 keep-alive <10-3600>
6 auto-reconnect (enable|disable)
```

Parameters

Parameter	Description
server-ip	Broker IP address
port	Broker port, default: 1883 (8883 for TLS)
clientid	Client ID, must be unique
timeout	Connection timeout (seconds)
keep-alive	Keepalive interval (seconds)
auto-reconnect	Auto-reconnect on disconnect

Example

```
mqtt-client
server-ip 192.168.1.50 port 1883
clientid router-001 keep-alive 60
auto-reconnect enable
```

28.4 Authentication Configuration

Function: Configure MQTT connection username and password authentication

Syntax

```
1 username USER
2 password PASSWORD
```

Example

```
1 mqtt-client
2 username mqttuser
3 password mqttpass
```

28.5 TLS Encryption

Function: Enable MQTT TLS encrypted connection

Syntax

```
1 tls (enable|disable)
2 tls-mode (one-way|two-way)
```

Parameters

Parameter	Description
one-way	One-way authentication (only verify server certificate)

Parameter	Description
two-way	Two-way authentication (mutual certificate verification)

Example

```
1 mqtt-client
2 tls enable
3 tls-mode one-way
```

28.6 Last Will Message

Function: Configure MQTT Last Will message, automatically published on abnormal disconnection

Syntax

```
1 will-msg topic WORD
2 will-msg qos <0-2>
3 will-msg retain-flag (enable|disable)
```

Parameters

Parameter	Description
topic	Last Will message topic
qos	Quality of Service level (0/1/2)
retain-flag	Whether to retain the message

Example

```
mqtt-client
will-msg topic device/status
will-msg qos 1
will-msg retain-flag enable
```

28.7 System Info Publishing

Function: Configure periodic publishing of system information (CPU, memory, temperature, etc.) to a specified topic

Syntax

```
1 pub-sysinfo topic WORD interval <1-3600>
2 pub-sysstatus topic WORD interval <1-3600>
3 pub-cell topic WORD interval <1-3600>
4 pub-ethernet topic WORD interval <1-3600>
5 pub-gps topic WORD interval <1-3600>
```

Parameters

Parameter	Description
topic	Publish topic
interval	Publish interval (seconds)

Example

```
mqtt-client
pub-sysinfo topic device/sysinfo interval 60 pub-cell topic device/cellular interval 30
pub-gps topic device/gps interval 10
```

28.8 Log level

Function: Set the MQTT client log output level

Syntax

```
1 set log-level <0-2>
```

Parameters

Parameter	Description
0	Errors only
1	Normal information
2	Debug information

Example

```
1 mqtt-client
2 set log-level 1
```

29. TR-069 Management

29.1 Enter TR-069 Configuration

Function: Enter the TR-069 (CPE WAN Management Protocol) configuration view

Syntax

```
1 tr069 management
```

Example

```
1 configure terminal
2 tr069 management
```

29.2 ACS Server Configuration

Function: Configure TR-069 ACS (Auto Configuration Server) URL and authentication information

Syntax

```
1 acs url URL
2 acs username USER
3 acs password PASSWORD
4 no acs url
5 no acs username
6 no acs password
```

Parameters

Parameter	Description
URL	ACS server URL, e.g., http://acs.example.com:7547/
USER	ACS authentication username
PASSWORD	ACS authentication password

Example

```
tr069 management
acs url http://acs.example.com:7547/
acs username acsuser
acs password acspass
```

29.3 CPE Authentication Configuration

Function: Configure the username and password for CPE (Customer Premises Equipment) authentication to ACS

Syntax

```
1 cpe username USER
2 cpe password PASSWORD
3 no cpe username
4 no cpe password
```

Example

```
1 tr069 management
2 cpe username cpeuser
3 cpe password cpepass
```

29.4 Periodic Notification Configuration

Function: Configure CPE to send periodic Inform notifications to ACS

Syntax

```
1 cpe inform (enable|disable)
2 cpe inform interval <1-86400>
```

Parameters

Parameter	Description
enable disable	Enable or disable periodic inform notifications
<1-86400>	Notification interval (seconds)

Example

```
1 tr069 management
2 cpe inform enable
3 cpe inform interval 3600
```

29.5 Enable/Disable TR-069

Function: Enable or disable the TR-069 service

Syntax

```
1 no shutdown
2 shutdown
```

Example

```
1 tr069 management
2 no shutdown
```

30. GPS Positioning

30.1 Enter GPS Configuration

Function: Enter the GPS configuration view

Syntax

```
1 gps config
```

Example

```
1 configure terminal
2 gps config
```

30.2 GPS Signal Source

Function: Select the GPS signal source (built-in cellular module or external GPS module)

Syntax

```
1 gps module (cellular|extern)
```

Parameters

Parameter	Description
cellular	Use cellular module built-in GPS
extern	Use external GPS module

Example

```
1 gps config
2 gps module cellular
```

30.3 GPS Coordinate System

Function: Set the GPS coordinate system type (GCJ-02 coordinate system required within China)

Syntax

```
1 gps location (china|other)
2 no gps location
```

Parameters

Parameter	Description
china	GCJ-02 coordinate system (China offset coordinates)
other	WGS-84 standard coordinate system

Notes

- When using map services in mainland China, select "china"; otherwise, coordinates will be offset

Example

```
1 gps config
2 gps location china
```

30.4 GPS Debug Logging

Function: Enable GPS debug log output

Syntax

```
1 gps debug (syslog|filelog)
2 no gps debug
```

Parameters

Parameter	Description
syslog	Output to system log
filelog	Output to file

Example

```
1 gps config
2 gps debug syslog
```

30.5 Enable GPS

Function: Enable GPS function (auto-start on boot)

Syntax

```
1 enable startup
```

Example

```
1 gps config
2 enable startup
```

31. Cloud Management Platform

31.1 Cloud Platform Server Configuration

Function: Configure the server address and authentication information for connecting the device to the cloud management platform

Syntax

```
1 cloud server A.B.C.D
2 cloud server port <1-65535>
3 cloud username USER
4 cloud password PASSWORD
5 cloud device-id ID
```

Parameters

Parameter	Description
A.B.C.D	Cloud platform server IP or domain name
<1-65535>	Service port
USER	Authentication username
PASSWORD	Authentication password
ID	Device unique identifier

Example

```
configure terminal
cloud server cloud.example.com
cloud server port 8883
cloud username devuser
cloud password devpass
cloud device-id SN123456
```

31.2 Cloud Platform Connection Protocol

Function: Set the protocol type for communication with the cloud platform

Syntax

```
1 cloud protocol (mqtt|http|https)
```

Parameters

Parameter	Description
mqtt	MQTT protocol
http	HTTP protocol
https	HTTPS encrypted protocol

Example

```
1 configure terminal
2 cloud protocol mqtt
```

31.3 Enable/Disable Cloud Management

Function: Enable or disable cloud management platform connection

Syntax

```
1 cloud enable
2 no cloud enable
3 cloud startup
4 no cloud startup
```

Example

```
1 configure terminal
2 cloud enable
3 cloud startup
```

32. Alarms & Events

32.1 Alarm Recording & Notification

Function: Configure alarm recording and notification methods (Email/SMS/SNMP Trap) when specific events occur

Syntax

```
1 alarm (record|email |sms|snmp) (system-boot|link-up|link-down|cellular- 2 up|cellular-
down|vpn-up|vpn-down|temperature|power)
3 no alarm (record|email |sms|snmp) (system-boot|...)
```

Parameters

Parameter	Description
record	Record to log
email	Send email notification
sms	Send SMS notification
snmp	Send SNMP Trap
Event type	
System-boot	System boot
link-up/down	Link up/down
cellular-up/down	Cellular up/down
vpn-up/down	VPN connection up/down

Parameter	Description
temperature	Temperature alarm
power	Power alarm

Example

```
configure terminal
alarm email system-boot
alarm sms cellular-down
alarm snmp link-down
```

32.2 Alarm SMS Phone Group

Function: Set the phone number group for receiving alarm SMS

Syntax

```
1 alarm sms phone group id <1-100>
2 no alarm sms phone group
```

Parameters

Parameter	Description
<1-100>	Phone number group ID

Example

```
1 configure terminal
2 alarm sms phone group id 1
```

32.3 Alarm Email Group

Function: Set the email address group for receiving alarm emails

Syntax

```
1 alarm email group id <1-100>
2 no alarm email group
```

Parameters

Parameter	Description
<1-100>	Email address group ID

Example

```
1 configure terminal
2 alarm email group id 1
```

32.4 Alarm MQTT Publishing

Function: Configure publishing alarm events to a specified topic via MQTT

Syntax

```
1 alarm mqtt publish (enable|disable)
2 alarm mqtt add event ARRAY topic WORD qos <0-2> flag <0-1> mqtt name .LINE
3 alarm mqtt delete all
```

Parameters

Parameter	Description
ARRAY	Event type array
topic	MQTT Publish topic
qos	Quality of Service (0/1/2)
flag	Retain flag
mqtt name	MQTT client name

Example

```
1 configure terminal
2 alarm mqtt publish enable
3 alarm mqtt add event link-down topic alarm/link qos 1 flag 0 mqtt name myBroker
```

33. Email Groups

33.1 Create Email Group

Function: Create an email address group for alarm notifications and other functions

Syntax

```
1 email-group id <1-100> name NAME
```

Parameters

Parameter	Description
<1-100>	Email group ID
NAME	Email group name

Example

```
1 configure terminal
2 email-group id 1 name ops-team
```

33.2 Add Email Address

Function: Add a recipient address to the email group

Syntax

```
1 email-group id <1-100> add EMAIL
```

Parameters

Parameter	Description
EMAIL	Email address

Example

```
1 configure terminal
2 email-group id 1 add admin@example.com
```

33.3 Delete Email Group

Function: Delete the specified email group

Syntax

```
1 no email-group id <1-100>
```

Example

```
1 configure terminal
2 no email-group id 1
```

33.4 SMTP Server Configuration

Function: Configure the SMTP server for sending alarm emails

Syntax

```
1 smtp server HOST
2 smtp port <1-65535>
3 smtp username USER
4 smtp password PASSWORD
5 smtp from EMAIL
6 smtp ssl (enable|disable)
```

Parameters

Parameter	Description
HOST	SMTP server address
port	SMTP port (default: 25, SSL: 465, STARTTLS: 587)
from	Sender address

Example

```
1 smtp server HOST
2 smtp server smtp.example.com
3 smtp port 587
4 smtp username sender@example.com
5 smtp password smtppass
6 smtp from noreply@example.com
7 smtp ssl enable
```

34. Modbus RTU

34.1 Enter Modbus RTU Configuration

Function: Enter the Modbus RTU slave configuration view

Syntax

```
1 modbus-rtu
```

Example

```
1 configure terminal
2 modbus-rtu
```

34.2 Slave ID

Function: Set the Modbus RTU slave address

Syntax

```
1 slave id <1-247>
```

Parameters

Parameter	Description
<1-247>	Modbus slave address, range: 1-247

Example

```
1 modbus-rtu
2 slave id 1
```

34.3 Serial Port Mode

Function: Set the serial port mode used by Modbus RTU

Syntax

```
1 serial mode <0-1>
```

Parameters

Parameter	Description
0	RS-232 mode
1	RS-485 mode

Example

```
1 modbus-rtu
2 serial mode 1
```

34.4 DI/DO Address Mapping

Function: Configure Modbus register addresses for Digital Input (DI) and Digital Output (DO)

Syntax

```
1 di-1-address <0-255>
2 di-2-address <0-255>
3 do-1-address <0-255>
4 do-2-address <0-255>
```

Parameters

Parameter	Description
<0-255>	Modbus register address

Example

```
1 modbus-rtu
```

34.5 Transmit/Receive Delay

Function: Set the delay time between receiving a request and sending a response for Modbus RTU

Syntax

```
1 delay <10-1000>
2 no delay
```

Parameters

Parameter	Description
<10-1000>	Delay time in milliseconds

Example

```
1 modbus-rtu
2 delay 50
```

34.6 Enable/Disable Modbus RTU

Function: Enable or disable the Modbus RTU service.

Syntax

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 modbus-rtu
2 no shutdown
3 enable startup
```

35. Modbus TCP

35.1 Enter Modbus TCP Configuration

Function: Enter the Modbus TCP slave configuration view

Syntax

```
1 modbus-tcp
```

Example

```
1 configure terminal
2 modbus-tcp
```

35.2 Listening Port

Function: Set the Modbus TCP service listening port

Syntax

```
1 port <1-65535>
```

Parameters

Parameter	Description
<1-65535>	Listening port; the standard Modbus TCP port is 502

Notes

- Port 502 requires root privileges; using a high port such as 5020 is recommended

Example

```
1 modbus-tcp
2 port 502
```

35.3 DI/DO Address Mapping

Function: Configure DI/DO register address mapping for Modbus TCP

Syntax

```
1 di-1-address <0-255>
2 di-2-address <0-255>
3 do-1-address <0-255>
4 do-2-address <0-255>
```

Example

```
1 modbus-tcp
```

35.4 Enable/Disable Modbus TCP

Function: Enable or disable the Modbus TCP service.

Syntax

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 modbus-tcp
2 no shutdown
3 enable startup
```

36. Modbus Master

36.1 Enter Modbus Master Configuration

Function: Enter the Modbus Master configuration view; the master actively polls slave data

Syntax

```
1 modbus-master
```

Example

```
1 configure terminal
2 modbus-master
```

36.2 Add Slave

Function: Add a Modbus slave device

Syntax

```
1 modbus-master slave NAME ip A.B.C.D port <1-65535> c <1-247>
```

Parameters

Parameter	Description
NAME	Slave name identifier
A.B.C.D	Slave IP address (TCP mode)
port	Slave port
slave-id	Slave address

Example

```
1 modbus-master
2 modbus-master slave plc1 ip 192.168.1.100 port 502 slave-id 1
```

36.3 Add Collection Instruction

Function: Add data collection instructions for a slave, defining the register type and address to read

Syntax

```
1 modbus-master instruction NAME command (1|2 |3|4|5 |6|15 |16)
2 modbus-master instruction NAME data-type <1-8>
3 modbus-master instruction NAME order <0-4>
4 modbus-master instruction NAME sign
5 no modbus-master instruction NAME sign
6 modbus-master instruction NAME deminal <0-9>
7 modbus-master instruction NAME delete
8 modbus-master instruction delete all
```

Parameters

Parameter	Description
NAME	Instruction name
command	Modbus function code
1	Read Coils
2	Read Discrete Inputs
3	Read Holding Registers
4	Read Input Registers
5	Write Single Coil
6	Write Single Register
15	Write Multiple Coils
16	Write Multiple Registers
data-type	Data type (1-8)
order	Byte order (0-4)
sign	Signed number
deminal	Decimal places (0-9)

Example

```
1 modbus-master
2 modbus-master instruction temp command 3
3 modbus-master instruction temp data-type 2 4 modbus-master instruction temp sign
5 modbus-master instruction temp deminal 1
```

37. USB Management

37.1 USB Link Control

Function: Enable or disable the USB network link

Syntax

```
1 link-usb (up|down)
```

Parameters

Parameter	Description
up	Enable USB link
down	Disable USB link

Example

```
1 configure terminal
2 link-usb up
```

38. Storage Management

38.1 Format Storage Media

Function: Format TF card or SSD storage media

Syntax

```
1 storage format (tfcard|ssd)
```

Parameters

Parameter	Description
tfcard	TF/SD card
ssd	Solid-state drive

Notes

- Formatting is irreversible and will erase all data on the storage medium
- Confirm that important data has been backed up before proceeding

Example

```
1 configure terminal
2 storage format tfcard
```

38.2 Detect Storage Media

Function: Detect whether the storage medium is properly inserted and available

Syntax

```
1 storage detect (tfcard|ssd)
```

Example

```
1 configure terminal
2 storage detect tfcard
```

39. Python Applications

39.1 Python SDK Configuration

Function: Configure the Python application SDK runtime environment

Syntax

```
1 python sdk
```

Example

```
1 configure terminal
2 python sdk
```

39.2 Application Management

Function: Install, start, stop, or delete Python applications

Syntax

```
1 python app install NAME
2 python app start NAME
3 python app stop NAME
4 python app delete NAME
```

Parameters

Parameter	Description
NAME	Python application name

Notes

- Application packages must be uploaded to device storage in advance

Example

```
1 configure terminal
2 python app install myapp
3 python app start myapp
```

39.3 Enable/Disable Python Runtime

Function: Enable or disable the Python application runtime environment

Syntax

```
1 enable startup
2 no enable startup
```

Example

40. Network Interface Basic Configuration

40.1 Set Interface Properties

Function: Set the network role property of the interface (LAN/WAN/Cellular)

Syntax

```
1 property (lan|wan|cell)
```

Parameters

Parameter	Description
lan	LAN interface
wan	WAN interface
cell	Cellular network interface

Notes

- Must first enter the interface configuration view: interface IFNAME

Example

```
1 configure terminal
2 interface eth0
3 property wan
```

40.2 Configure IPv4 Address

Function: Configure a static IPv4 address for the interface

Syntax

```
1 ip address A.B.C.D/M
2 no ip address A.B.C.D/M
3 ip address A.B.C.D/M label LINE
```

Parameters

Parameter	Description
A.B.C.D/M	IP address and prefix length in CIDR format
label LINE	Address label (used for policy routing identification)

Example

```
1 configure terminal
2 interface eth1
3 ip address 192.168.1.1/24
```

40.3 Configure IPv6 Address

Function: Configure a static IPv6 address for the interface

Syntax

```
1 ipv6 address X:X::X:X/M
2 no ipv6 address X:X::X:X/M
```

Parameters

Parameter	Description
X:X::X:X/M	IPv6 address and prefix length

Example

```
1 configure terminal
2 interface eth1
3 ipv6 address 2001:db8::1/64
```

40.4 Interface Description

Function: Add a description to the interface

Syntax

```
1 description LINE
2 no description
```

Parameters

Parameter	Description
LINE	Description string

Example

```
1 configure terminal
2 interface eth0
3 description WAN-to-ISP
```

40.5 Interface Bandwidth

Function: Set interface bandwidth (used for routing protocol metric calculation)

Syntax

```
1 bandwidth <1-10000000>
2 no bandwidth
```

Parameters

Parameter	Description
<1-10000000>	Bandwidth value in Kbps

Example

```
1 configure terminal
2 interface eth0
3 bandwidth 100000
```

40.6 Enable/Disable Interface

Function: Enable or shut down the network interface

Syntax

```
1 no shutdown
2 shutdown
```

Notes

- shutdown causes the interface to stop sending and receiving packets

Example

```
1 configure terminal
2 interface eth1
3 no shutdown
```

40.7 Link Detection

Function: Enable interface link status detection; the interface is automatically marked as down when the link is disconnected

Syntax

```
1 link-detect
2 link-detect default
3 no link-detect
```

Example

```
1 configure terminal
2 interface eth0
3 link-detect
```

40.8 Multicast Support

Function: Enable or disable multicast on the interface

Syntax

```
1 multicast
2 no multicast
```

Example

```
1 configure terminal
2 interface eth0
3 multicast
```

40.9 Interface Monitor Interval

Function: Set the polling interval for the interface status monitoring thread

Syntax

```
1 interface-monitor interval <1-60>
```

Parameters

Parameter	Description
<1-60>	Monitoring interval in seconds

Example

```
1 configure terminal
2 interface-monitor interval 5
```

41. DHCP Client

41.1 Enable DHCP Client

Function: Enable DHCP automatic IPv4 address acquisition on the interface

Syntax

```
1 ip address dhcp
2 no ip address dhcp
```

Notes

- After enabling, the interface will request IP address, gateway, DNS, etc., from the DHCP server
- Mutually exclusive with static IP configuration

Example

```
1 configure terminal
2 interface eth0
3 ip address dhcp
```

41.2 DHCP Client ID

Function: Set the DHCP client identifier used to identify itself to the server

Syntax

```
1 ip dhcp client client-id (INTERFACE | ascii STRING | hex STRING)
```

Parameters

Parameter	Description
INTERFACE	Use interface name as client ID
ascii STRING	ASCII string format
hex STRING	Hexadecimal format

Example

```
1 configure terminal
2 interface eth0
3 ip dhcp client client-id ascii myrouter
```

41.3 DHCP Hostname

Function: Set the hostname carried in DHCP requests

Syntax

```
1 ip dhcp client hostname HOSTNAME
```

Parameters

Parameter	Description
HOSTNAME	Hostname string

Example

```
1 configure terminal
2 interface eth0
3 ip dhcp client hostname mydevice
```

41.4 Use DHCP Provided DNS

Function: Whether to use the DNS server address provided by the DHCP server

Syntax

```
1 ip dhcp client use peer dns
2 no ip dhcp client use peer dns
```

Example

```
1 configure terminal
2 interface eth0
3 ip dhcp client use peer dns
```

41.5 Release/Renew DHCP Lease

Function: Manually release or renew the DHCP lease on the specified interface

Syntax

```
1 release dhcp IFNAME
2 renew dhcp IFNAME
```

Parameters

Parameter	Description
IFNAME	Interface name, e.g., eth0

Example

```
1 configure terminal
2 release dhcp eth0
3 renew dhcp eth0
```

41.6 IPv6 DHCP Client

Function: Enable DHCPv6 automatic IPv6 address acquisition on the interface

Syntax

```
1 ipv6 address dhcp
2 no ipv6 address dhcp
3 ipv6 dhcp client use peer dns
4 ipv6 request-mode (none|try|force)
5 ipv6 prefix-len <0-64>
```

Parameters

Parameter	Description
request-mode none	Do not request prefix
request-mode try	Try to request prefix
request-mode force	Force prefix request
prefix-len	Requested prefix length

Example

```
configure terminal interface eth0
ipv6 address dhcp
ipv6 request-mode try
```

42. DHCP Server

42.1 Enable DHCP Service

Function: Globally enable or disable the DHCP server

Syntax

```
1 service dhcp
2 no service dhcp
```

Example

```
1 configure terminal
2 service dhcp
```

42.2 Enter DHCP Server Configuration

Function: Enter the DHCP server global configuration view

Syntax

```
1 ip dhcpd
```

Example

```
1 configure terminal
2 ip dhcpd
```

42.3 Declare DHCP Subnet

Function: Declare a DHCP address pool subnet, specifying the network address and mask

Syntax

```
1 declare subnet WORD A.B.C.D A.B.C.D
2 no declare subnet WORD
```

Parameters

Parameter	Description
WORD	Subnet name identifier
First A.B.C.D	Network address
Second A.B.C.D	Subnet mask

Example

```
1 ip dhcpd
2 declare subnet lan1 192.168.1.0 255.255.255.0
```

42.4 Address Pool Range

Function: Set the dynamic allocation address range for the DHCP subnet

Syntax

```
1 range A.B.C.D A.B.C.D
2 range A.B.C.D A.B.C.D secondary
3 no range A.B.C.D A.B.C.D
```

Parameters

Parameter	Description
First A.B.C.D	Start IP
Second A.B.C.D	End IP
secondary	Secondary address pool

Example

```
1 ip dhcpd
2 declare subnet lan1 192.168.1.0 255.255.255.0
3 range 192.168.1.100 192.168.1.200
```

42.5 Bind Interface

Function: Bind the DHCP subnet to a specified interface

Syntax

```
1 ifname WORD
```

Parameters

Parameter	Description
WORD	Interface name, e.g., eth1, br0

Example

```
1 ip dhcpd
2 declare subnet lan1 192.168.1.0 255.255.255.0
3 ifname br0
```

42.6 Default Gateway

Function: Set the default gateway delivered to DHCP clients

Syntax

```
1 default-router A.B.C.D
2 no default-router
```

Parameters

Parameter	Description
A.B.C.D	Gateway IP address

Example

```
1 ip dhcpd
2 declare subnet lan1 192.168.1.0 255.255.255.0
3 default-router 192.168.1.1
```

42.7 DNS Server

Function: Set the DNS server address delivered to DHCP clients

Syntax

```
1 dns-server A.B.C.D [A.B.C.D]
2 no dns-server
```

Parameters

Parameter	Description
A.B.C.D	DNS server IP; up to two can be configured

Example

```
1 ip dhcpd
2 declare subnet lan1 192.168.1.0 255.255.255.0
3 dns-server 8.8.8.8 8.8.4.4
```

42.8 Lease Time

Function: Set the DHCP address lease time

Syntax

```
1 lease-time <60-2592000>
2 default-lease-time <60-2592000>
3 max-lease-time <60-2592000>
```

Parameters

Parameter	Description
<60-2592000>	Lease time in seconds (max 30 days)

Example

```
ip dhcpd
declare subnet lan1 192.168.1.0 255.255.255.0 default-lease-time 86400
max-lease-time 604800
```

42.9 Static Address Binding

Function: Bind a fixed IP to a specified MAC address (static DHCP)

Syntax

```
1 declare host WORD
2 no declare host WORD
3 hardware ethernet MAC
4 fixed-address A.B.C.D
```

Parameters

Parameter	Description
WORD	Host name identifier
MAC	MAC address, format: XX:XX:XX:XX:XX:XX
A.B.C.D	Bound fixed IP address

Example

```
ip dhcpd
declare host printer
hardware ethernet 00:11:22:33:44:55 fixed-address 192.168.1.50
```

42.10 Authoritative Mode

Function: Set this DHCP server as authoritative; sends DHCPNAK to unknown clients

Syntax

```
1 authoritative
2 no authoritative
```

Notes

- There should only be one authoritative DHCP server on the network

Example

```
1 ip dhcpd
2 declare subnet lan1 192.168.1.0 255.255.255.0
3 authoritative
```

42.11 Enable/Disable Subnet

Function: Enable or disable the specified DHCP subnet

Syntax

```
1 no shutdown
2 shutdown
```

Example

```
1 ip dhcpd
2 declare subnet lan1 192.168.1.0 255.255.255.0
3 no shutdown
```

43. DHCP Relay

43.1 DHCP Relay Helper Address

Function: Configure DHCP relay destination server address (Helper Address) to forward client requests to the specified server

Syntax

```
1 ip helper-address A.B.C.D [A.B.C.D] ... [A.B.C.D]
2 no ip helper-address [A.B.C.D] ...
```

Parameters

Parameter	Description
A.B.C.D	DHCP server IP address; supports up to 8

Notes

- Must be executed under the interface configuration view
- The interface must be in the same subnet as the clients

Example

```
1 configure terminal
2 interface eth0
3 ip helper-address 10.0.0.1 10.0.0.2
```

43.2 Relay Listening Port

Function: Set the listening port for the DHCP relay agent

Syntax

```
1 ip dhcp relay port NUM
```

Parameters

Parameter	Description
NUM	Port number, default: 67

Example

```
1 configure terminal
2 ip dhcp relay port 67
```

43.3 Relay Information Option

Function: Configure whether the DHCP relay inserts Option 82 (Relay Agent Information Option)

Syntax

```
1 ip dhcp relay information option
2 no ip dhcp relay information option
3 ip dhcp relay information policy (append|drop|keep|replace)
4 ip dhcp relay information check
5 no ip dhcp relay information check
6 ip dhcp relay information trust-all
```

Parameters

Parameter	Description
append	Append relay information
drop	Drop packets containing relay information
keep	Keep original relay information
replace	Replace relay information

Example

```
1 configure terminal
2 ip dhcp relay information option
3 ip dhcp relay information policy replace
```

44. DNS Configuration

44.1 DNS Server Address

Function: Configure the DNS server address used by the system

Syntax

```
1 ip name-server A.B.C.D
2 no ip name-server A.B.C.D
```

Parameters

Parameter	Description
A.B.C.D	DNS server IP address

Example

```
1 configure terminal
2 ip name-server 8.8.8.8
3 ip name-server 114.114.114.114
```

44.2 DNS Domain Name

Function: Configure the local domain name search suffix

Syntax

```
1 ip domain-name WORD
2 no ip domain-name
```

Parameters

Parameter	Description
WORD	Domain name, e.g., example.com

Example

```
1 configure terminal
2 ip domain-name example.com
```

44.3 DNS Forwarding

Function: Enable DNS forwarding to forward DNS queries to upstream servers

Syntax

```
1 ip dns forwarding
2 no ip dns forwarding
3 ip dns forwarding server A.B.C.D
4 no ip dns forwarding server A.B.C.D
```

Parameters

Parameter	Description
A.B.C.D	Upstream DNS server address

Example

```
1 configure terminal
2 ip dns forwarding
3 ip dns forwarding server 8.8.8.8
```

45. Static Routing

45.1 Add Static Route (CIDR Format)

Function: Add a static IPv4 route, specifying the destination network and next hop

Syntax

```
1 ip route A.B.C.D/M A.B.C.D
2 ip route A.B.C.D/M INTERFACE
3 ip route A.B.C.D/M A.B.C.D <1-255>
4 ip route A.B.C.D/M A.B.C.D tag <1-65535>
5 ip route A.B.C.D/M (reject|blackhole)
```

Parameters

Parameter	Description
A.B.C.D/M	Destination network (CIDR format)
A.B.C.D (second)	Next hop IP address
INTERFACE	Egress interface name
<1-255>	Administrative distance (default: 1)
tag	Route tag
reject	Send ICMP unreachable
blackhole	Silently discard

Notes

- Lower administrative distance means higher priority
- reject and blackhole are used for null routes (to prevent routing loops)

Example

```
configure terminal
ip route 0.0.0.0/0 192.168.1.254
ip route 10.0.0.0/8 172.16.0.1 10 ip route 192.168.99.0/24 blackhole
```

45.2 Delete Static Route

Function: Delete a configured static route

Syntax

```
1 no ip route A.B.C.D/M A.B.C.D
2 no ip route A.B.C.D/M INTERFACE
3 no ip route A.B.C.D/M (reject|blackhole)
```

Example

```
1 configure terminal
2 no ip route 0.0.0.0/0 192.168.1.254
```

46. VLAN Configuration

46.1 Create/Delete VLAN

Function: Create or delete a specified VLAN ID

Syntax

```
1 vlan <1-4094>
2 no vlan <1-4094>
```

Parameters

Parameter	Description
<1-4094>	VLAN ID; 1 is the default VLAN, 4094 is the maximum

Notes

- VLAN 1 is the default VLAN and is generally not recommended to delete

Example

```
1 configure terminal 2 vlan 10
3 vlan 20
```

46.2 Interface VLAN Mode

Function: Set the VLAN operating mode of the switch interface (Access or Trunk)

Syntax

```
1 switchport mode (access|trunk)
2 no switchport mode
```

Parameters

Parameter	Description
access	Access mode; the interface belongs to a single VLAN

Parameter	Description
trunk	Trunk mode; the interface can carry multiple VLANs

Example

```
1 configure terminal
2 interface eth1
3 switchport mode access
```

46.3 Access Interface VLAN

Function: Set the VLAN to which the Access mode interface belongs

Syntax

```
1 switchport access vlan <1-4094>
2 no switchport access vlan
```

Parameters

Parameter	Description
<1-4094>	VLAN ID

Example

```
1 configure terminal
2 interface eth1
3 switchport mode access
4 switchport access vlan 10
```

46.4 Trunk Interface Allowed VLAN

Function: Set the list of VLANs allowed on the Trunk interface

Syntax

```
1 switchport trunk allowed vlan <1-4094>
2 switchport trunk allowed vlan add <1-4094>
3 switchport trunk allowed vlan remove <1-4094>
4 no switchport trunk allowed vlan
```

Parameters

Parameter	Description
<1-4094>	VLAN ID or range

Example

```
1 configure terminal
2 interface eth0
3 switchport mode trunk
```

46.5 VLAN Interface (SVI)

Function: Create a VLAN Layer 3 interface (SVI) for inter-VLAN routing

Syntax

```
1 interface vlan <1-4094>
```

Parameters

Parameter	Description
<1-4094>	VLAN ID

Example

```
1 configure terminal
2 interface vlan 10
3 ip address 192.168.10.1/24
4 no shutdown
```

47. Switch Configuration

47.1 Switch WAN Port VLAN

Function: Configure the VLAN ID for the switch WAN port

Syntax

```
1 switch wan vid <1-4094>
```

Parameters

Parameter	Description
<1-4094>	WAN port VLAN ID

Example

```
1 configure terminal
2 switch wan vid 100
```

47.2 Port Join VLAN

Function: Add or remove a physical port from a specified VLAN

Syntax

```
1 port select (1|2|cpu|1t|2t|cput)
2 port unselect (1|2|cpu|1t|2t|cput)
```

Parameters

Parameter	Description
1 2	Physical port number
cpu	CPU port
1t 2t cput	Tagged mode port

Example

```
configure terminal vlan 10
port select 1
port select 2t
```

47.3 Apply Switch Configuration

Function: Apply switch configuration changes immediately

Syntax

```
1 switch config apply
```

Notes

- This command must be executed for switch configuration changes to take effect

Example

```
1 configure terminal
2 switch config apply
```

48. WiFi (WLAN) Configuration

48.1 Show WiFi Information

Function: View WiFi channel list, configuration, associated clients, and other information

Syntax

```
1 show dot11 channel-list
2 show dot11 config
3 show dot11 associations
4 show dot11 sta associations
5 show dot11 access-points
```

Example

```
1 configure terminal
2 show dot11 config
3 show dot11 associations
```

48.2 Configure SSID

Function: Create or modify the WiFi SSID name

Syntax

```
1 dot11 ssid modify WORD WORD
2 dot11 ssid modify WORD WORD encoded
```

Parameters

Parameter	Description
First WORD	SSID identifier name
Second WORD	SSID string (broadcast name)
encoded	SSID is in encoded format (hidden SSID)

Example

```
1 configure terminal
2 dot11 ssid modify ssid0 MyWiFiNetwork
```

48.3 WiFi Authentication Method

Function: Set the WiFi access authentication method

Syntax

```
1 dot11 authentication (open|shared|wpa-psk|wpa2-psk|wpa-enterprise|wpa2- 2 enterprise)
```

Parameters

Parameter	Description
open	Open authentication (no password)

Parameter	Description
shared	Shared secret key(WEP)
wpa-psk	WPA Personal mode
wpa2-psk	WPA2 Personal mode (recommended)
wpa-enterprise	WPA Enterprise mode (requires RADIUS)
wpa2-enterprise	WPA2 Enterprise mode (requires RADIUS)

Notes

- WPA2-PSK or WPA2-Enterprise is recommended
- WEP has been proven insecure and is not recommended

Example

```
1 configure terminal
2 dot11 authentication wpa2-psk
```

48.4 WiFi Encryption Method

Function: Set the WiFi data encryption algorithm

Syntax

```
1 dot11 encryption (none|wep|tkip|ccmp|tkip+ccmp)
```

Parameters

Parameter	Description
none	No encryption
wep	WEP encryption (insecure)
tkip	TKIP encryption (WPA)
ccmp	AES-CCMP encryption (WPA2, recommended)
tkip+ccmp	Support both TKIP and CCMP

Example

```
1 configure terminal
2 dot11 encryption ccmp
```

48.5 WiFi Password

Function: Set WPA/WPA2 Pre-Shared Key(PSK)

Syntax

```
1 dot11 passphrase WORD
2 dot11 passphrase WORD encoded
```

Parameters

Parameter	Description
WORD	WiFi password, 8-63 characters
encoded	Password is in encoded format

Notes

- Password must be at least 8 characters; strong passwords are recommended

Example

```
1 configure terminal
2 dot11 passphrase MySecureWiFi123
```

48.6 WiFi Channel

Function: Set the WiFi operating channel

Syntax

```
1 dot11 channel <1-165>
2 dot11 channel auto
```

Parameters

Parameter	Description
<1-14>	2.4 GHz channels (1-14)
<36-165>	5 GHz channels
auto	Auto-select the best channel

Notes

- For 2.4 GHz, channels 1, 6, and 11 are recommended (non-overlapping)
- 5 GHz channels have less interference and are recommended

Example

```
1 configure terminal
2 dot11 channel 6
```

48.7 WiFi Transmit Power

Function: Set the WiFi transmit power

Syntax

```
1 dot11 power <1-100>
```

Parameters

Parameter	Description
<1-100>	Transmit power percentage

Example

```
1 configure terminal
2 dot11 power 100
```

48.8 Hide SSID

Function: Enable or disable SSID broadcast (hide WiFi network)

Syntax

```
1 dot11 ssid-broadcast (enable|disable)
```

Parameters

Parameter	Description
enable	Broadcast SSID (default, visible)
disable	Hide SSID

Notes

- Hiding the SSID does not significantly improve security and only adds minor inconvenience

Example

```
1 configure terminal
2 dot11 ssid-broadcast disable
```

48.9 WiFi Max Clients

Function: Set the maximum number of clients allowed to connect simultaneously on a single SSID

Syntax

```
1 dot11 max-associations <1-255>
```

Parameters

Parameter	Description
<1-255>	Maximum associated clients

Example

```
1 configure terminal
2 dot11 max-associations 32
```

48.10 Enable/Disable WiFi

Function: Enable or disable the WiFi interface

Syntax

```
1 no shutdown
2 shutdown
3 enable startup
4 no enable startup
```

Example

```
1 configure terminal
2 dot11 no shutdown
3 enable startup
```

49. Bridge Configuration

49.1 Create Bridge Interface

Function: Create a bridge interface to bridge multiple interfaces into the same Layer 2 domain

Syntax

```
1 bridge WORD
2 no bridge WORD
```

Parameters

Parameter	Description
WORD	Bridge interface name, e.g., br0

Example

```
1 configure terminal
2 bridge br0
```

49.2 Add Interface to Bridge

Function: Add a physical interface to the bridge

Syntax

```
1 bridge WORD add IFNAME
2 bridge WORD del IFNAME
```

Parameters

Parameter	Description
WORD	Bridge name
IFNAME	Interface name to add

Example

```
1 configure terminal
2 bridge br0 add eth1
3 bridge br0 add eth2
```

49.3 STP Spanning Tree Protocol

Function: Enable or disable STP (Spanning Tree Protocol) on the bridge to prevent Layer 2 loops

Syntax

```
1 bridge WORD stp (enable|disable)
2 bridge WORD priority <0-65535>
3 bridge WORD forward-delay <4-30>
4 bridge WORD hello-time <1-10>
5 bridge WORD max-age <6-40>
```

Parameters

Parameter	Description
priority	Bridge priority; lower values are more likely to become root bridge, default: 32768
forward-delay	Forward delay (seconds), default: 15
hello-time	Hello message interval (seconds), default: 2
max-age	Max age (seconds), default: 20

Example

```
1 configure terminal
2 bridge br0 stp enable
3 bridge br0 priority 4096
```