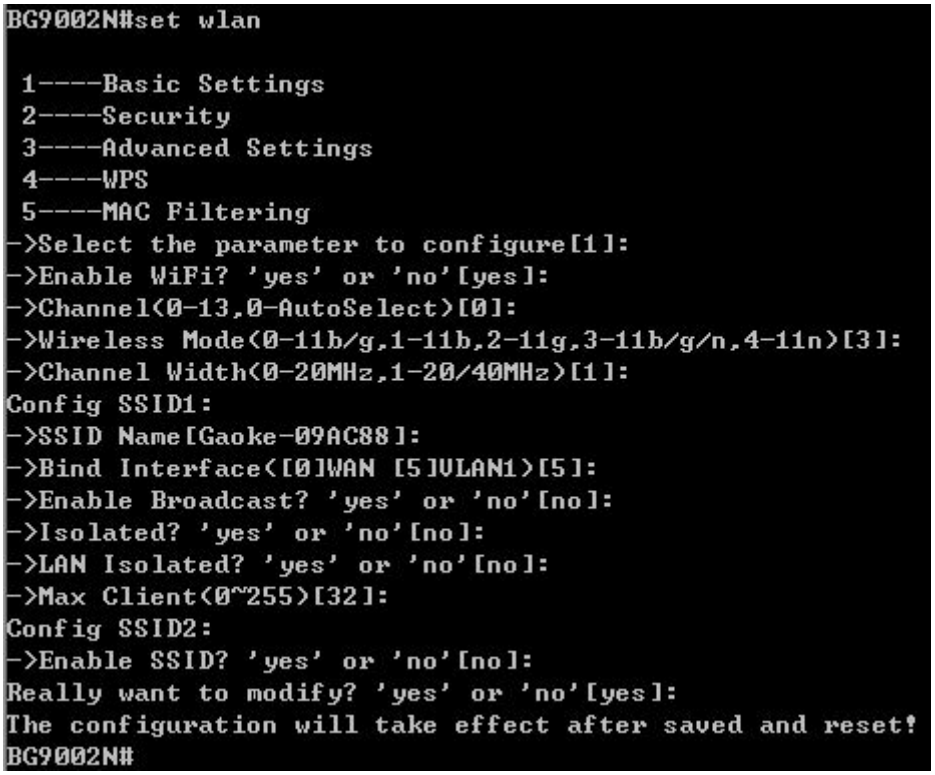


Figure 1-1 Configure Basic Settings

The following items are displayed on this part.

► **Enable WiFi:** Enable or disable the WIFI AP function globally.

► **Channel:** This field determines which operating frequency will be used. The default channel is set to **AutoSelect**, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

► **Wireless Mode:** Select the desired mode.

11b: Select if all of your wireless clients are 802.11b.

11g: Select if all of your wireless clients are 802.11g.

11n: Select only if all of your wireless clients are 802.11n.

11b/g: Select if you are using both 802.11b and 802.11g wireless clients.

11b/g/n: Select if you are using a mix of 802.11b, 11g and 11n wireless clients.

► **Channel Width:** Select any channel width from the drop-down list. The default setting is automatic, which can automatically adjust the channel width for your clients. If you choose to **11n** or **11b/g/n** Wireless mode**,** this configuration is required. Two values of width are provided: **20MHz** and **20/40MHz**.

The **Service Set Identifier (SSID)** is used to identify an 802.11 (Wi-Fi) network and it's discovered by network sniffing/scanning. FG7008N provides up to four SSID.

► **Enable SSID:** Enable or disable this entry of SSID. SSID1 can't be disabled.

►**SSID Name:** Enter the name of SSID. The name of SSID must be unique in all wireless networks nearby.

► **Bind Interface:** Select a network interface to be bridged to the SSID.

► **Enable Broadcast:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device. If you select the **Enable Broadcast** checkbox, the device will broadcast its name (SSID) on the air.

► **Isolated:** Enable or disable isolate different clients from the same wireless station.

► **LAN Isolated:** Enable or disable isolation between the LAN and SSID.

► **Max Client:** Enter the maximum number of clients allowed to connect to the SSID.

► **SSID AP Isolated:** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

Input “2” to configure security parameter as below:

```
BG9002N#set wlan

 1----Basic Settings
 2----Security
 3----Advanced Settings
 4----WPS
 5----MAC Filtering
->Select the parameter to configure[1]:2
->Select the SSID to set(0-3)[0]:

 0----Disable
 1----OPEN WEP
 2----WPAPSK
 3----WPA2PSK
 4----WPAPSKWPA2PSK
 5----WPA
 6----WPA2
 7----WPA1WPA2
 8----SHARE
 9----WEPAUTO
->Authentication[4]:
->Algorithm(0-KTIP,1-AES,2-KTIP/AES)[1]:
->Renew interval(0-2592000)[3600]:
->WAP Pre-Shared Key(length:8-63)[**********]:
->Continue or not?(yes/no)[yes]:n
->Really want to modify? 'yes' or 'no'[yes]:y

  Oprate success!

BG9002N#_
```

Figure 1-2 Configure Security Parameter

The following items are displayed on this part.

► **SSID:** The SSID enabled in **WLAN→Basic Settings** page.Read only

► **Authentication:** The authentication type selected: WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK.

► **Algorithm:** When WPA2-PSK or WPAPSK/WPA2PSK is set as the Authentication Type, you can select either **TKIP**, or **AES** or **TKIP/AES** as Encryption. When WPA-PSK is set as the Authentication Type, you can select either TKIP or AES as Encryption.

► **WPA Pre-Shared Key:** You can enter ASCII characters between 8 and 64 characters.

► **Renew Interval:** Specify the group key update interval in seconds. Enter 0 to disable the update.

Input “3” to configure advanced settings as below:

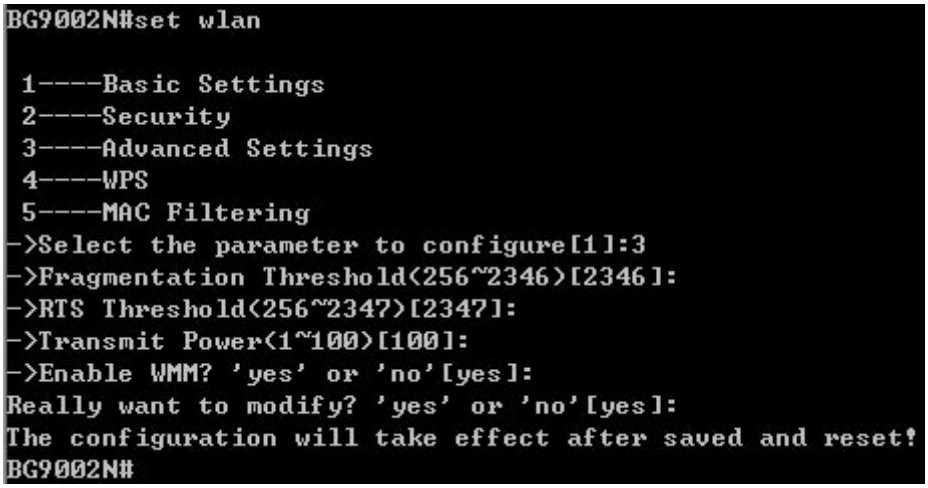


Figure 1-3 Configure Advanced Settings

The following items are displayed on this part.

► **Fragmentation Threshold:** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.

► **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2347.

► **Transmit Power:** Here you can specify the transmit power of device. 100 is the default setting and is recommended.

► **Enable WMM:** Enable or disable the WIFI WMM function globally. WMM function can guarantee the packets with high-priority messages, being transmitted preferentially. It is strongly recommended enabled.

Input “4” to configure WPS parameter as below:

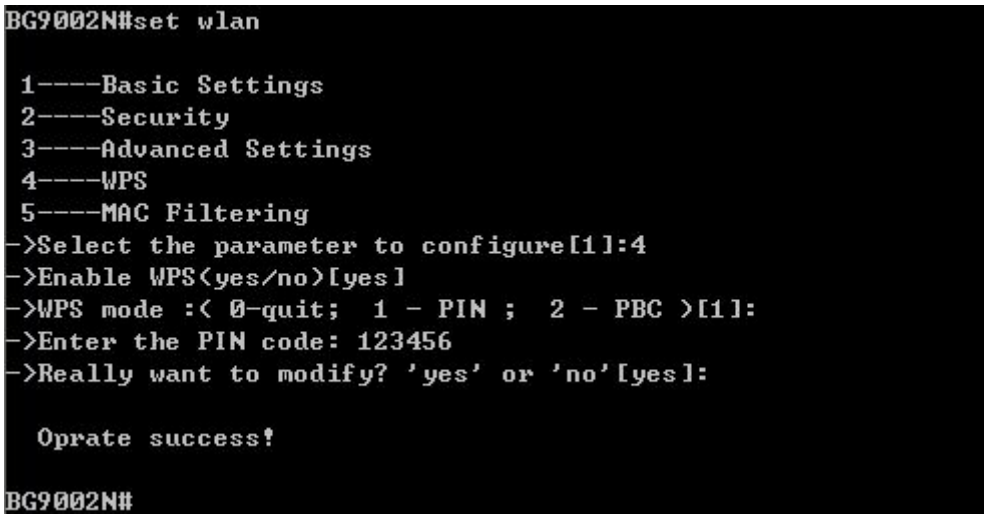


Figure 1-4 Configure WPS Parameter

The following items are displayed on this part.

► **Enable WPS:** Enable or disable the WIFI WPS function globally.

Input “4” to configure MAC filtering parameter as below:

```
BG9002N#set wlan

 1----Basic Settings
 2----Security
 3----Advanced Settings
 4----WPS
 5----MAC Filtering
->Select the parameter to configure[1]:5
WLAN MAC Filter Config:
->0-Rule,1-List[0]: 0
->Enable MAC Filter? 'yes' or 'no'[yes]:
->Filtering Rules(0-Allow,1-Deny)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#
```

```
BG9002N#set wlan

 1----Basic Settings
 2----Security
 3----Advanced Settings
 4----WPS
 5----MAC Filtering
->Select the parameter to configure[1]:5
WLAN MAC Filter Config:
->0-Rule,1-List[0]: 1
WLAN MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->MAC[]:15:41:66:88:ac:f8
The configuration will take effect after saved and reset!
BG9002N#
```

```
BG9002N#set wlan

 1----Basic Settings
 2----Security
 3----Advanced Settings
 4----WPS
 5----MAC Filtering
->Select the parameter to configure[1]:5
WLAN MAC Filter Config:
->0-Rule,1-List[0]: 1
WLAN MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+----+-------------------+
| No |        MAC        |
+----+-------------------+
|0   |af:16:80:41:43:99  |
+----+-------------------+
|1   |15:41:66:88:ac:f8  |
+----+-------------------+
->Please input number which you will modify[0-1]:1
->MAC[15:41:66:88:ac:f8]:a2:35:68:41:12:43
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#
```

```
BG9002N#set wlan

 1----Basic Settings
 2----Security
 3----Advanced Settings
 4----WPS
 5----MAC Filtering
->Select the parameter to configure[1]:5
WLAN MAC Filter Config:
->0-Rule,1-List[0]: 1
WLAN MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+--------------------+
| No |        MAC         |
+----+--------------------+
|0   |af:16:80:41:43:99   |
+----+--------------------+
|1   |a2:35:68:41:12:43   |
+----+--------------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-5 Configure MAC Filtering Parameter

The following items are displayed on this part.

► **Enable MAC Filter:** Enable or disable the Wifi MAC filtering function globally.

► **Filtering Rules:** Two MAC filtering rules are provided:

Allow: allow the stations specified by entries in the list to access.

Deny: deny the stations specified by entries in the list to access.

1.2 Data Service

1.2.1 DHCP Server

1.2.1.1 Static Address Assign

The command “show dhcp-server static-ip-assign” shows the static IP assign information as bellow:

```
BG9002N#show dhcp-server static-ip-assign

+----+---------------+---------------+--------------------+
|No  |IP             |Netmask        |MAC                 |
+----+---------------+---------------+--------------------+
|0   |192.168.4.5    |255.255.255.0  |01:02:03:04:05:06   |
+----+---------------+---------------+--------------------+
|1   |192.168.0.30   |255.255.255.0  |11:a2:3c:33:67:85   |
+----+---------------+---------------+--------------------+

BG9002N#
```

Figure 1-6 Show Static IP Assign Information

The command “set dhcp-server static-ip-assign” configures the static IP assign information as below.

Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set dhcp-server static-ip-assign
Static Ip Assign List Config:
->Select Config type(0-add,1-del,2-modify)[0]: 0
->IP[]: 192.168.4.66
->Netmask[]: 255.255.255.0
->MAC[00:00:00:00:00:00]: a4:2d:33:76:89:f3
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set dhcp-server static-ip-assign
Static Ip Assign List Config:
->Select Config type(0-add,1-del,2-modify)[0]: 2

+----+---------------+---------------+--------------------+
|No  |IP             |Netmask        |MAC                 |
+----+---------------+---------------+--------------------+
|0   |192.168.0.30   |255.255.255.0  |11:a2:3c:33:67:85   |
+----+---------------+---------------+--------------------+
|1   |192.168.12.56  |255.255.255.0  |14:34:86:99:a6:06   |
+----+---------------+---------------+--------------------+
|2   |192.168.4.66   |255.255.255.0  |a4:2d:33:76:89:f3   |
+----+---------------+---------------+--------------------+
->Please input number which you will modify[0-2]:0
->IP[192.168.0.30]:
->Netmask[255.255.255.0]:
->MAC[11:a2:3c:33:67:85]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set dhcp-server static-ip-assign
Static Ip Assign List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1

+----+---------------+---------------+--------------------+
|No  |IP             |Netmask        |MAC                 |
+----+---------------+---------------+--------------------+
|0   |192.168.0.30   |255.255.255.0  |11:a2:3c:33:67:85   |
+----+---------------+---------------+--------------------+
|1   |192.168.12.56  |255.255.255.0  |14:34:86:99:a6:06   |
+----+---------------+---------------+--------------------+
|2   |192.168.4.66   |255.255.255.0  |a4:2d:33:76:89:f3   |
+----+---------------+---------------+--------------------+

->Please choose the start index of deleting entry[0-2]:1
->Please choose the end index of deleting entry[0-2]:2
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-7 Configure Static IP Assign

The command will configure static ip assign.

The following items are displayed on this screen:

► **IP :** The IP address reserved.

► **Mask:** The subnet mask of IP address reserved.
► **MAC:** The MAC address you want to reserve IP address.

1.2.1.2 DHCP Relay

The command “show dhcp-relay” shows the DHCP relay information as below:

```
BG9002N#show dhcp-relay
->Enable DHCP Relay.....................................: Enable
->Client Interface 1....................................: none
->Client Interface 2....................................: VLAN1
->Client Interface 3....................................: none
->Client Interface 4....................................: VOICE
->Server Interface......................................: DATA
->Server IP.............................................: 138.0.60.2

BG9002N#
```

Figure 1-8 Show DHCP Relay Information

The command "set dhcp-relay” configures the DHCP relay information as below:

```
BG9002N#set dhcp-relay
->Enable DHCP Relay? 'yes' or 'no'[yes]:
->Client Interface 1<[0]DATA [1]VOICE [2]MGMT [5]VLAN1 [255]none)[255]:2
->Client Interface 2<[0]DATA [1]VOICE [2]MGMT [5]VLAN1 [255]none)[5]:
->Client Interface 3<[0]DATA [1]VOICE [2]MGMT [5]VLAN1 [255]none)[255]:
->Client Interface 4<[0]DATA [1]VOICE [2]MGMT [5]VLAN1 [255]none)[1]:
->Server Interface<[0]DATA [1]VOICE [2]MGMT [5]VLAN1 [255]none)[0]:
->Server IP[138.0.60.2]:
Really want to modify? 'yes' or 'no'[yes]:y
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-9 Set DHCP Relay Information

The following items are displayed on this screen:
► **Enable DHCP Relay:** Enable or disable DHCP Relay.
► **Client Interface:** The interface to listen for DHCP client requests. Up to four interfaces can be selected.
► **Server Interface:** Choose the interface which connects DHCP server.
► **Server IP:** Configure the DHCP server IP address.

1.2.2 NAT Config

1.2.2.1 Basic Settings

The command “show nat” shows the NAT basic settings as below:

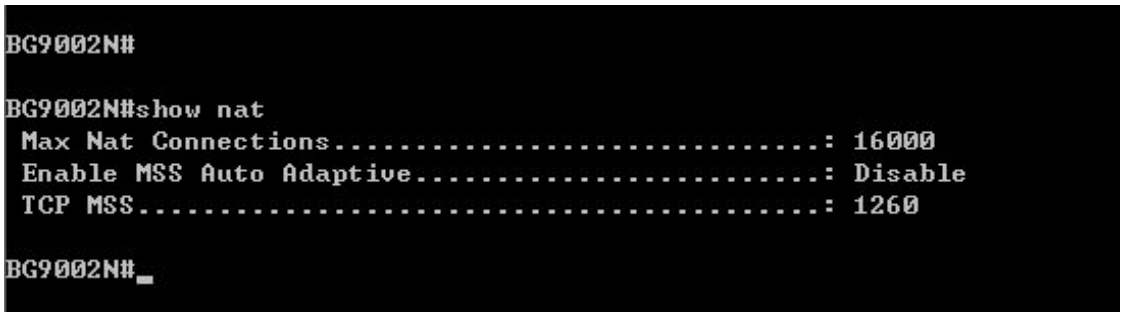


Figure 1-10 Show NAT Basic Settings

The command “set nat” configures the NAT basic settings as below:

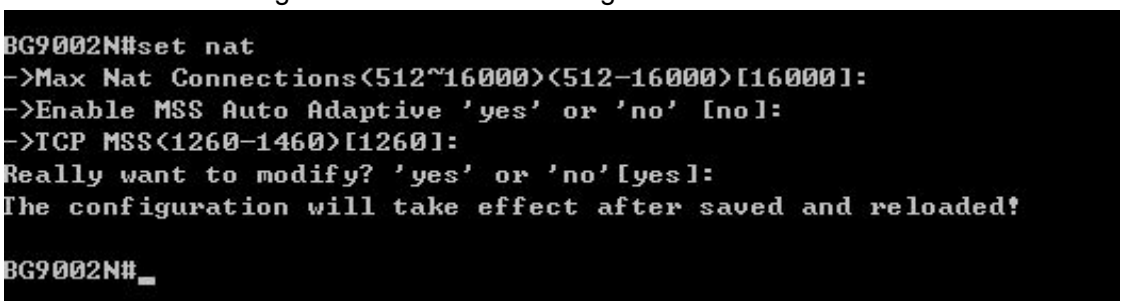


Figure 1-11 Configure NAT Basic Settings

The following items are displayed on this screen:

► **Max Nat Connections:** Specify the maximum number of NAT connections.

► **Enable MSS Auto Adaptive:** Enable or disable auto adaptive the value of MSS (Maximum Segment Size).

► **TCP MSS:** If **Enable MSS Auto Adaptive** is not selected, configure this to specify the maximum segment size of the TCP protocol.

1.2.2.2 PAT Settings

The command “show pat” shows the PAT information as below:

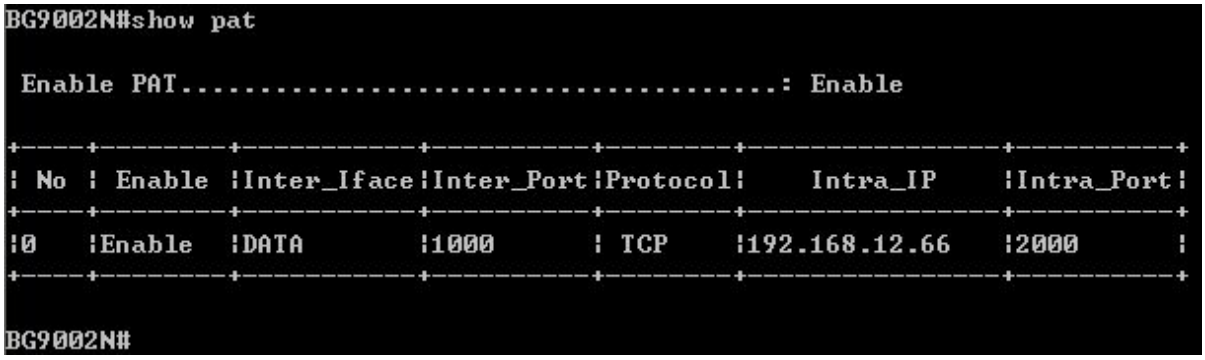


Figure 1-12 Show PAT Information

The command “set pat” configures the PAT parameters as below:

```
BG9002N#set pat
->Enable PAT? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-13 Configure PAT Parameters

The following items are displayed on this screen:

► **Enable PAT:** Enable or disable PAT globally.

The command “set pat rule” configures the PAT rule as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify .If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set pat rule
Pat Regular List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Enable the PAT rule? 'yes' or 'no'[yes]:
->Protocol Type(0-TCP, 1-UDP)[0]:1
->Internet Port(0-65535)[1000]:
->Intranet IP[0.0.0.0]:192.168.2.66
->Intranet Port(0-65535)[1000]:6000
->Internet Interface:'[0]DATA'[0]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set pat rule
Pat Regular List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+----+--------+-----------+----------+--------+----------------+----------+
| No | Enable |Inter_Iface|Inter_Port|Protocol|    Intra_IP    |Intra_Port|
+----+--------+-----------+----------+--------+----------------+----------+
|0   |Enable  |DATA       |1000      | TCP    |192.168.12.66   |2000      |
+----+--------+-----------+----------+--------+----------------+----------+
|1   |Enable  |DATA       |1000      | UDP    |192.168.2.66    |6000      |
+----+--------+-----------+----------+--------+----------------+----------+
->Please input number which you will modify[0-1]:1
->Enable the PAT rule? 'yes' or 'no'[yes]:
->Protocol Type(0-TCP, 1-UDP)[1]:
->Internet Port(0-65535)[1000]:5000
->Intranet IP[192.168.2.66]:
->Intranet Port(0-65535)[6000]:
->Internet Interface:'[0]DATA'[0]:
->Really want to modify? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

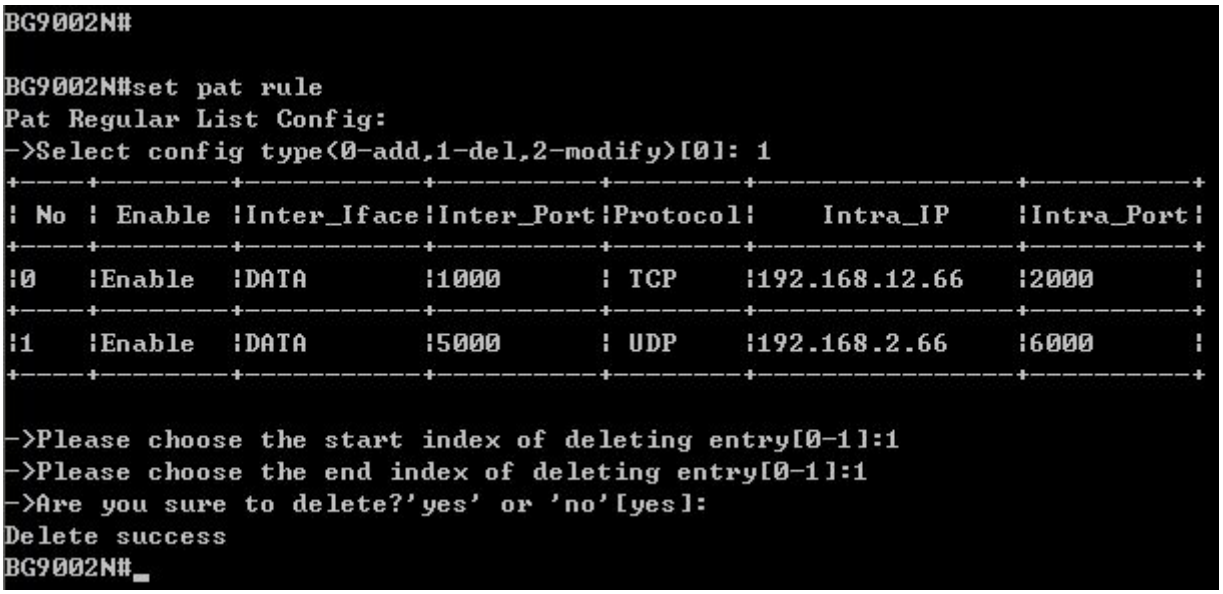


Figure 1-14 Configure PAT Rule

The following items are displayed on this screen:

- ► **Enable:** Enable or disable this PAT entry.
- ► **Internet Port:** Enter the service port provided for accessing external network. All the requests from internet to this service port will be redirected to the specified server in local network.
- ► **Intranet Port:** Specify the service port of the LAN host as virtual server.
- ► **Intranet IP:** Enter the IP address of the specified internal server for the entry. All the requests from the internet to the specified LAN port will be redirected to this host.
- ► **Protocol:** Specify the protocol used for the entry.
- ► **Internet Interface:** Specify the interface to receive requests from the internet for the entry.

1.2.2.3 DMZ Settings

The command “show dmz” shows the DMZ information as below:

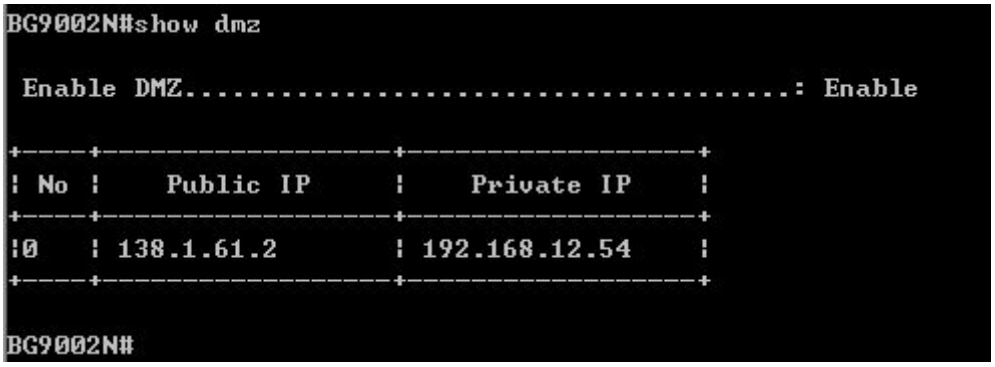


Figure 1-15 Show DMZ Information

The command “set dmz ” configures the DMZ Parameters as below:

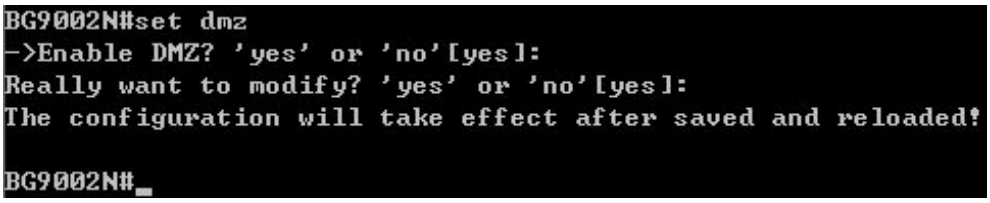


Figure 1-16 Configure DMZ Parameters

The following items are displayed on this screen:

► **Enable DMZ:** Enable or disable DMZ globally.

The command "set dmz rule" configures the DMZ rule as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

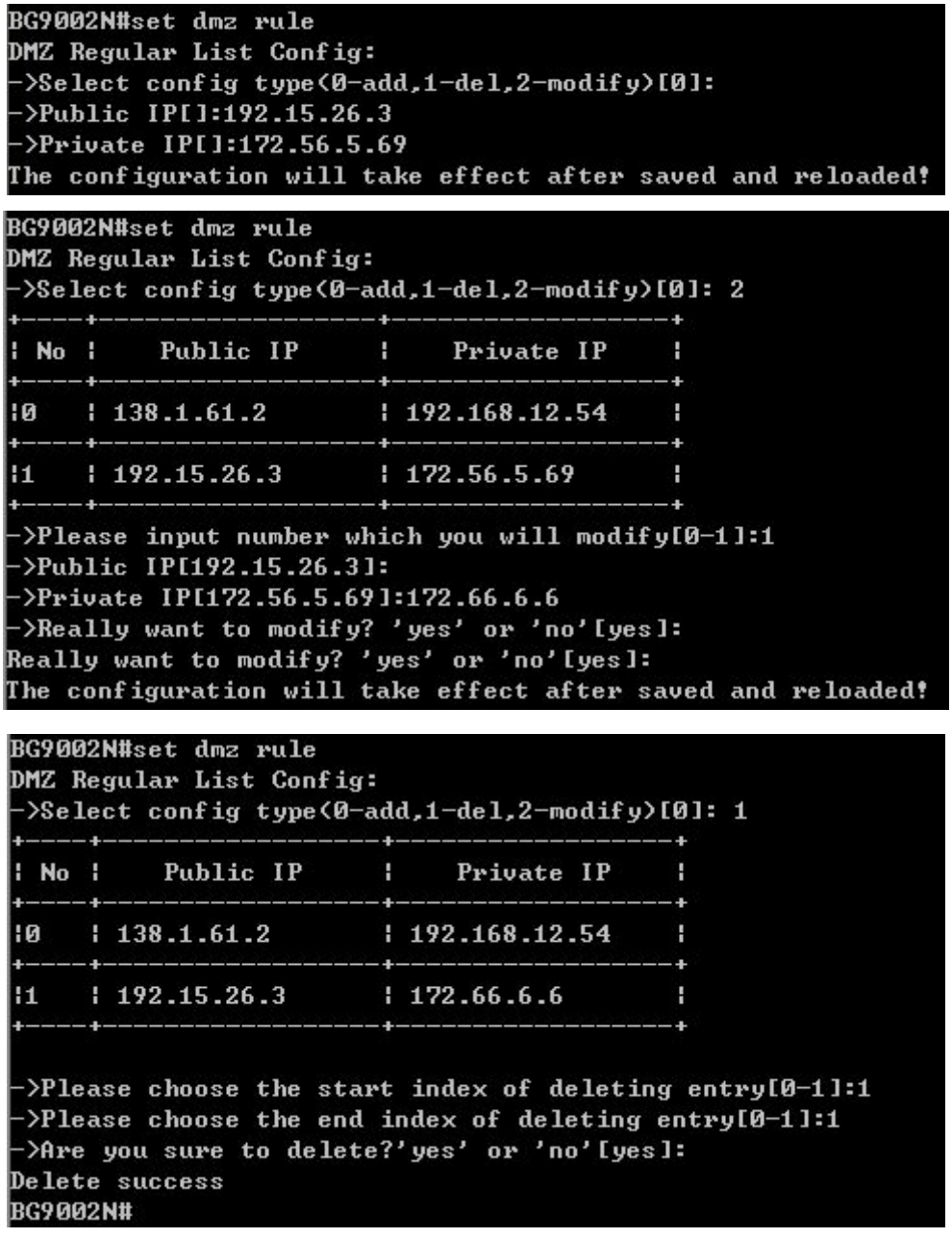


Figure 1-17 Configure DMZ Rule

The following items are displayed on this screen:

► **Public IP:** The public IP address for this DMZ entry.
► **Private IP:** The private IP address for this DMZ entry.

1.2.2.4 ALG Settings

The command “show alg” shows the ALG information as below:

```
BG9002N#show alg
 Enable SIP ALG.....................................: Disable
 Enable H323 ALG....................................: Enable
 Enable FTP ALG.....................................: Enable
 Enable RTSP ALG....................................: Enable
 RTSP Server Port...................................: 554
 Enable PPTP ALG....................................: Enable

BG9002N#
```

Figure 1-18 Show ALG Information

The command “set alg” configures the ALG parameters as below:

```
BG9002N#set alg
->Enable SIP ALG? 'yes' or 'no' [no]: y
->Enable H323 ALG? 'yes' or 'no' [yes]:
->Enable FTP ALG? 'yes' or 'no' [yes]:
->Enable RTSP ALG? 'yes' or 'no' [yes]:
->RTSP Server Port(1~65535)[554]:
->Enable PPTP ALG? 'yes' or 'no' [yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-19 Configure ALG Parameters

The following items are displayed on this screen:

► **Enable SIP:** Enable or disable SIP ALG.
► **Enable H323:** Allow Microsoft NetMeeting clients to communicate across NAT if selected.
► **Enable FTP:** Allow FTP clients and servers to transfer data across NAT if selected.
► **Enable PPTP:** Enable or disable PPTP ALG.
► **Enable RTSP:** Enable or disable RTSP ALG.

1.2.3 Firewall Config

1.2.3.1 Attack Defense

The command “show attack-defense” shows the attack defense information as below:

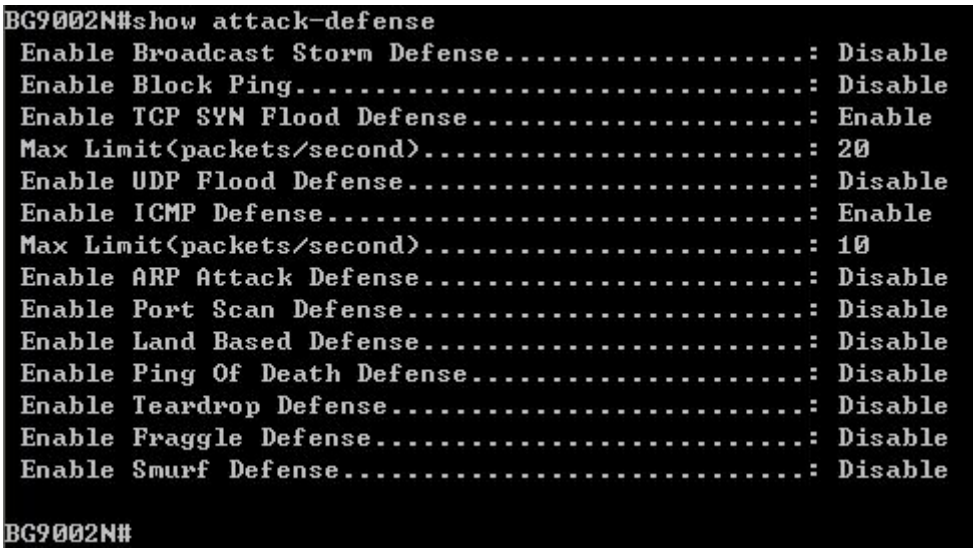


Figure 1-20 Show Attack Defense Information

The command “set attack-defense” configures the attack defense parameters as below:

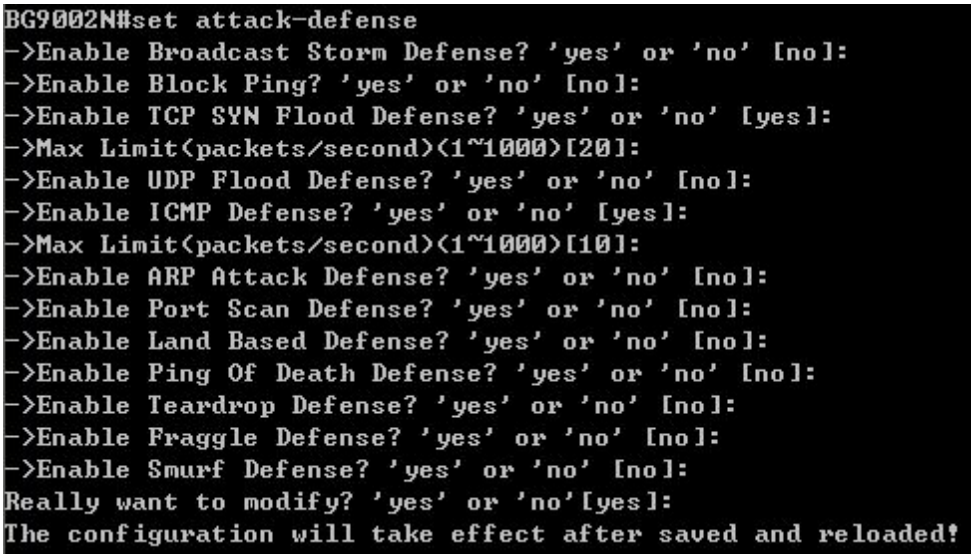


Figure 1-21 Configure Attack Defense Parameters

The following items are displayed on this screen:

- ► **Enable Broadcast Storm Defense:** Enable or disable **Broadcast Storm Defense**.
- ► **Enable Block Ping:** Enable or disable **Block Ping** function.
- ► **Enable TCP SYN Flood Defense:** Enable or disable **TCP SYN Flood Defense**.
- ► **Enable UDP Flood Defense:** Enable or disable **UDP Flood Defense**.
- ► **Enable ICMP Defense:** Enable or disable **ICMP Defense**.
- ► **Enable ARP Attack Defense:** Enable or disable **ARP Attack Defense**.
- ► **Enable Port Scan Defense:** A port scanner is a software application designed to probe a server or host for open ports. Check the box to prevent port scanning.
- ► **Enable Land Based Defense:** The Land Denial of Service attack works by sending a spoofed packet with the SYN flag - used in a "handshake" between a client and a host - set from a host to any port that is open and

listening. If the packet is programmed to have the same destination and source IP address, when it is sent to a machine, via IP spoofing, the transmission can fool the machine into thinking it is sending itself a message, which, depending on the operating system, will crash the machine. Check the box to enable **Land Based Defense**.

► **Enable Ping Of Death Defense:** Ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. Check the box to enable **Ping of Death Defense**.

► **Enable Teardrop Defense:** Teardrop is a program that sends IP fragments to a machine connected to the Internet or a network. Check the box to enable **Teardrop Defense**.

► **Enable Fraggle Defense:** A fraggle attack is a variation of a Smurf attack where an attacker sends a large amount of UDP traffic to ports 7 (echo) and 19 (chargen) to an IP Broadcast Address, with the intended victim's spoofed source IP address. Check the box to enable **Fraggle Defense**.

► **Enable Smurf Defense:** The Smurf Attack is a denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Check the box to enable **Smurf Defense**.

1.2.3.2 Service Type

The command “show service-type” shows the service type information as below:

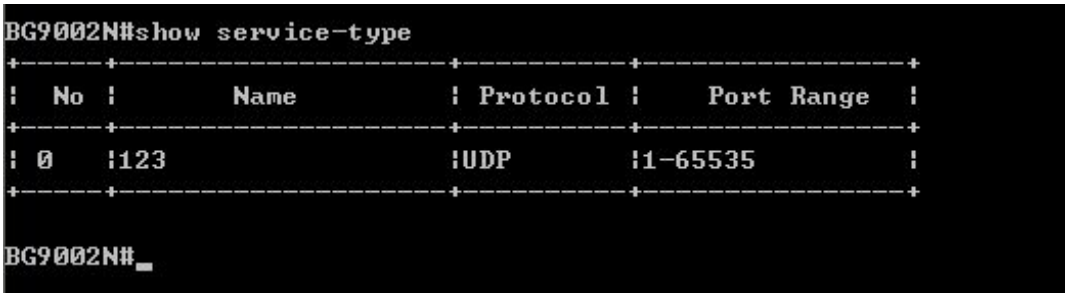


Figure 1-22 Show Service Type Information

The command “set service-type” configures the service type as below. Enter 0 add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set service-type
Service Type List Config:
->Select Config type(0-add,1-del,2-modify)[0]: 0
->Name[]:asdf
->Protocol(0-UDP,1-TCP,2-ICMP,3-ALL)[0]: 1
->Port(Start Port)(0-65535)[0]: 1000
->Port(End Port)(0-65535)[0]: 2000
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set service-type
Service Type List Config:
->Select Config type(0-add,1-del,2-modify)[0]: 2
+-----+--------------------+----------+----------------+
|  No |       Name         | Protocol |    Port Range  |
+-----+--------------------+----------+----------------+
| 0   |123                 |UDP       |1-65535         |
+-----+--------------------+----------+----------------+
| 1   |asdf                |TCP       |1000-2000       |
+-----+--------------------+----------+----------------+
->Please input number which you will modify[0-1]:0
->Name[123]:1234
->Protocol(0-UDP,1-TCP,2-ICMP,3-ALL)[0]:
->Port(Start Port)(0-65535)[1]:
->Port(End Port)(0-65535)[65535]:
Really want to modify? 'yes' or 'no'[yes]:y
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set service-type
Service Type List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+-----+--------------------+----------+----------------+
|  No |       Name         | Protocol |    Port Range  |
+-----+--------------------+----------+----------------+
| 0   |123                 |UDP       |1-65535         |
+-----+--------------------+----------+----------------+
| 1   |asdf                |TCP       |1000-2000       |
+-----+--------------------+----------+----------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-23 Configure Service Type

The following items are displayed on this screen:

- **Name:** Name of this entry, it will be list in Internet Access-Ctrl page.
- **Protocol:** Select the protocol for this entry. Four types are provided: TCP, UDP, ICMP and ALL.
- **Port Range:** Configure the port range for this entry.

1.2.3.3 Internet Access-Ctrl

1.2.3.3.1 Access Control

The command “show access-control” shows the access control information as below:

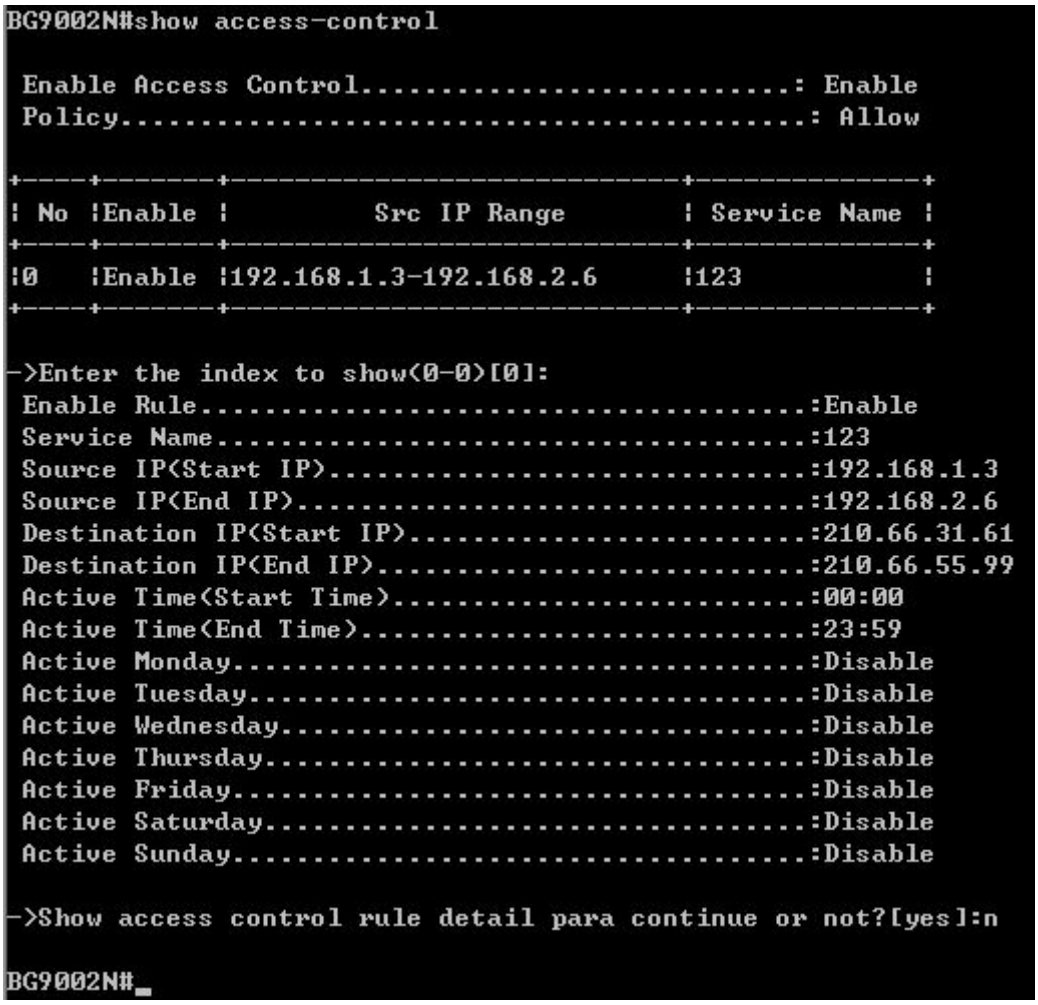


Figure 1-24 Show Access Control Information

The command “set access-control” configures the access control policy as below:

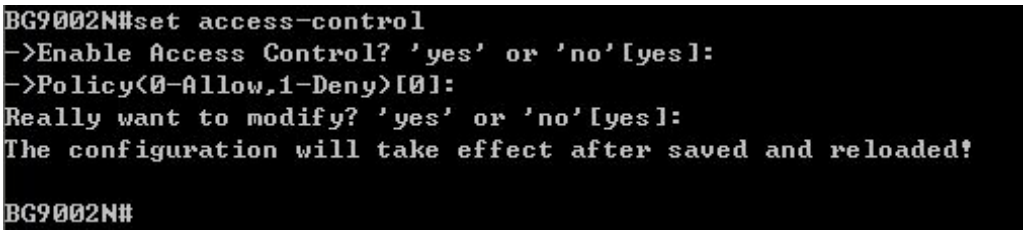


Figure 1-25 Configure Access Control

The following items are displayed on this screen:

► **Enable Access Control:** Enable or disable access control from WAN.

► **Policy:** Default policy of access control: **Allow** or **Deny**. If Allow is selected, all packets will be allowed except the entries list on this page. If Deny is selected, all packets will be denied except the entries list on this page.

The command “set access-control rule” configures the access control rule as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set access-control rule
Access Control Rule List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Enable Rule? 'yes' or 'no'[no]:y
->Source IP(Start IP)[]:192.168.5.6
->Source IP(End IP)[]:192.168.5.90
->Destination IP(Start IP)[]:139.0.1.6
->Destination IP(End IP)[]:139.0.1.66
->Service Name(0-123,255-NULL)[0]:
->Active Time(Start Time)[00:00]:
->Active Time(End Time)[00:00]:23:00
->Active Monday? 'yes' or 'no'[no]:
->Active Monday? 'yes' or 'no'[no]:
->Active Tuesday? 'yes' or 'no'[no]:
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set access-control rule
Access Control Rule List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+----+-------+---------------------------+--------------+
| No |Enable |         Src IP Range      | Service Name |
+----+-------+---------------------------+--------------+
|0   |Enable |192.168.1.3-192.168.2.6    |123           |
+----+-------+---------------------------+--------------+
|1   |Enable |192.168.5.6-192.168.5.90   |123           |
+----+-------+---------------------------+--------------+
->Please input number which you will modify[0-1]:1
->Enable Rule? 'yes' or 'no'[yes]:
->Source IP(Start IP)[192.168.5.6]:
->Source IP(End IP)[192.168.5.90]:
->Destination IP(Start IP)[139.0.1.6]:
->Destination IP(End IP)[139.0.1.66]:
->Service Name(0-123,255-NULL)[0]:
->Active Time(Start Time)[00:00]:
->Active Time(End Time)[23:00]:
->Active Monday? 'yes' or 'no'[no]:
->Active Monday? 'yes' or 'no'[no]:
->Active Tuesday? 'yes' or 'no'[no]:
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set access-control rule
Access Control Rule List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+-------+---------------------------+--------------+
| No |Enable |         Src IP Range      | Service Name |
+----+-------+---------------------------+--------------+
|0   |Enable |192.168.1.3-192.168.2.6    |123           |
+----+-------+---------------------------+--------------+
|1   |Enable |192.168.5.6-192.168.5.90   |123           |
+----+-------+---------------------------+--------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-26 Configure Access Control Rule

The following items are displayed on this screen:

► **Enable Rule:** Enable or disable this rule.

► **Source IP Range:** Enter the source IP range in dotted-decimal format (e.g. 192.168.1.23).

► **Destination IP Range:** Enter the destination IP range in dotted-decimal format (e.g. 192.168.1.23).

► **Service Name:** Choose a service type that defined in **Service Type** page.

► **Active Time:** Specify the time range for the entry to take effect.

► **Active Day:** Specify the day range for the entry to take effect.

1.2.3.3.2 User Authentication

The command “show user-authentication” shows the user authentication information as below:

```
BG9002N#show user-authentication
->Enable User Authentication.....................: Enable
+----+----------------+----------------+
| No |    Username    |     Password   |
+----+----------------+----------------+
|0   |1234            |1234            |
+----+----------------+----------------+

BG9002N#_
```

Figure 1-27 Show User Authentication Information

The command “set user-authentication” configures the user authentication parameters as below:

```
BG9002N#set user-authentication
->Enable User Authentication? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-28 Configure User Authentication Parameters

The following items are displayed on this screen:

► **Enable User Authentication:** Enable or disable user authentication globally. If enabled, only the following list of users and passwords can access the Internet.

The command “set user authentication list” configures the user authentication list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set user-authentication list
User Authentication List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Username[]:z41x43f
->Password[]:bfzy
 Auth Mode
 0-Allow Multi-PC Access
 1-Allow One PC Access
 2-Allow Special IP Access
 3-Allow Special MAC Access
->Auth Mode [0]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set user-authentication list
User Authentication List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+----+----------------+----------------+
| No |    Username    |     Password   |
+----+----------------+----------------+
|0   |1234            |1234            |
+----+----------------+----------------+
|1   |z41x43f         |bfzy            |
+----+----------------+----------------+
->Please input number which you will modify[0-1]:1
->Username[z41x43f]:
->Password[bfzy]:
 Auth Mode
 0-Allow Multi-PC Access
 1-Allow One PC Access
 2-Allow Special IP Access
 3-Allow Special MAC Access
->Auth Mode [0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set user-authentication list
User Authentication List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+----------------+----------------+
| No |    Username    |     Password   |
+----+----------------+----------------+
|0   |1234            |1234            |
+----+----------------+----------------+
|1   |z41x43f         |bfzy            |
+----+----------------+----------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-29 Configure User Authentication List

The following items are displayed on this screen:

► **Username:** Enter the username of this entry.

► **Password:** Enter the password of this entry.

► **Auth Mode:** Choose the authentication mode of this entry. Provides four modes:

Allow Multi-PC Access: Allows multiple computers to access the Internet using this account.

Allow One PC Access: Only allows one computer to access the Internet using this account.

Allow Special IP Access: Allowing only specified IP computer uses this account to access the Internet.

Allow Special MAC Access: Allowing only specified MAC computer uses this account to access the Internet

1.2.3.4 Network Access-Ctrl

1.2.3.4.1 WEB

The command “show network-access-ctrl web” shows the web access control information as below:

```
BG9002N#show network-access-ctrl w

BG9002N#show network-access-ctrl web
->HTTP Port.....: 80
->HTTPS Port.....: 443
->Enable Internet Allow Access.....: Enable
->Enable Internet IP Limit.....: Disable
->Internet IP Range(Start IP).....: 138.0.60.1
->Internet IP Range(End IP).....: 138.0.255.255
->Internet IPv6 Range(Start IP).....: 2001::60
->Internet IPv6 Range(End IP).....: 2001::ffff
->Enable Intranet Allow Access.....: Enable
->Enable Intranet IP Limit.....: Disable
->Intranet IP Range(Start IP).....: 192.168.1.2
->Intranet IP Range(End IP).....: 192.168.1.255
->Intranet IPv6 Range(Start IP).....: 2001::60
->Intranet IPv6 Range(End IP).....: 2001::ffff

BG9002N#
```

Figure 1-30 Show Web Access Control Information

The command “set network-access-ctrl web” configures the web access control parameters as below:

```
BG9002N#set network-access-ctrl web
->HTTP Port[80]:
->HTTPS Port[443]:
->Enable Internet Allow Access? 'yes' or 'no' [yes]:
->Enable Internet IP Limit? 'yes' or 'no' [no]: y
->Internet IP Range(Start IP)[138.0.60.1]:
->Internet IP Range(End IP)[138.0.255.255]:
->Internet IPv6 Range(Start IP)[2001::60]:
->Internet IPv6 Range(End IP)[2001::ffff]:
->Enable Intranet Allow Access? 'yes' or 'no' [yes]:
->Enable Intranet IP Limit? 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-31 Configure Web Access Control Parameters

The following items are displayed on this screen:

► **HTTP Port:** Port used with HTTP access device.
HTTP: Hypertext Transfer Protocol.

► **HTTPS Port:** Port used with HTTPS access device.
HTTPS: it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol.

Internet Web Access:

► **Allow Access:** If enabled, allow user to access the device from the Internet via WEB.

► **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via WEB.

► **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that is only allowed to access to the device from the Internet via WEB.

► **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that is only allowed to access to the device from the Internet via WEB.

Intranet Web Access:

► **Allow Access:** If enabled, allow user to access the device from the Intranet via WEB.

► **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via WEB.

► **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that is only allowed to access the device from the Intranet via WEB.

► **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that is only allowed to access the device from the Intranet via WEB.

1.2.3.4.2 TELNET

The command “show network-access-ctrl telnet” shows the telnet access control information as below:

```
BG9002N#show network-access-ctrl telnet
->Port.....: 23
->Enable Internet Allow Access.....: Disable
->Enable Internet IP Limit.....: Disable
->Internet IP Range(Start IP).....: 138.0.60.1
->Internet IP Range(End IP).....: 138.0.255.255
->Internet IPv6 Range(Start IP).....: 2001::60
->Internet IPv6 Range(End IP).....: 2001::ffff
->Enable Intranet Allow Access.....: Enable
->Enable Intranet IP Limit.....: Disable
->Intranet IP Range(Start IP).....: 192.168.1.2
->Intranet IP Range(End IP).....: 192.168.1.255
->Intranet IPv6 Range(Start IP).....: 2001::60
->Intranet IPv6 Range(End IP).....: 2001::ffff

BG9002N#
```

Figure 1-32 Show Telnet Access Control Information

The command “set network-access-ctrl telnet” configures the telnet access control parameters as below:

```
BG9002N#set network-access-ctrl telnet
->Port[23]:
->Enable Internet Allow Access? 'yes' or 'no' [no]: y
->Enable Internet IP Limit? 'yes' or 'no' [no]: y
->Internet IP Range(Start IP)[138.0.60.1]:
->Internet IP Range(End IP)[138.0.255.255]:
->Internet IPv6 Range(Start IP)[2001::60]:
->Internet IPv6 Range(End IP)[2001::ffff]:
->Enable Intranet Allow Access? 'yes' or 'no' [yes]:
->Enable Intranet IP Limit? 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-33 Configure Telnet Access Control Parameters

The following items are displayed on this screen:

► **Port:** Port when using telnet tools access device.

Internet Telnet Access:

► **Allow Access:** If enabled, allow access to the device from the Internet via telnet.

► **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via telnet

► **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Internet via telnet.

► **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Internet via telnet.

Intranet Telnet Access:

► **Allow Access:** If enabled, allow access to the device from the Intranet via telnet.

► **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via telnet

► **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Intranet via telnet.

► **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the

device from the Intranet via telnet.

1.2.3.4.3 SSH

The command “show network-access-ctrl ssh” shows the SSH access control information as below:

```
BG9002N#show network-access-ctrl telnet
->Port.....: 23
->Enable Internet Allow Access.....: Disable
->Enable Internet IP Limit.....: Disable
->Internet IP Range(Start IP).....: 138.0.60.1
->Internet IP Range(End IP).....: 138.0.255.255
->Internet IPv6 Range(Start IP).....: 2001::60
->Internet IPv6 Range(End IP).....: 2001::ffff
->Enable Intranet Allow Access.....: Enable
->Enable Intranet IP Limit.....: Disable
->Intranet IP Range(Start IP).....: 192.168.1.2
->Intranet IP Range(End IP).....: 192.168.1.255
->Intranet IPv6 Range(Start IP).....: 2001::60
->Intranet IPv6 Range(End IP).....: 2001::ffff

BG9002N#
```

Figure 1-34 Show SSH Access Control Information

The command “set network-access-ctrl ssh” configures the SSH access control parameters as below:

```
BG9002N#set network-access-ctrl telnet
->Port[23]:
->Enable Internet Allow Access? 'yes' or 'no' [no]: y
->Enable Internet IP Limit? 'yes' or 'no' [no]: y
->Internet IP Range(Start IP)[138.0.60.1]:
->Internet IP Range(End IP)[138.0.255.255]:
->Internet IPv6 Range(Start IP)[2001::60]:
->Internet IPv6 Range(End IP)[2001::ffff]:
->Enable Intranet Allow Access? 'yes' or 'no' [yes]:
->Enable Intranet IP Limit? 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-35 Configure SSH Access Control Parameters

The following items are displayed on this screen:

► **Port:** Port when using SSH tools access device.

Internet SSH Access:

► **Allow Access:** If enabled, allow access to the device from the Internet via SSH.

► **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via SSH

► **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Internet via SSH.

► **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Internet via SSH.

Intranet SSH Access:

► **Allow Access:** If enabled, allow access to the device from the Intranet via SSH.

► **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via SSH

► **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Intranet via SSH.

► **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Intranet via SSH.

1.2.3.5 Filter Strategy

1.2.3.5.1 Keyword Filter

The command “show keyword-filter” shows the keyword filter information as below:

```
BG9002N#show keyword-filter

 Enable Keyword Filter.............................: Enable
 Policy............................................: Deny

+----+--------------------------------+
| No |            Keyword             |
+----+--------------------------------+
|0   |12345                           |
+----+--------------------------------+

BG9002N#
```

Figure 1-36 Show Keyword Filter Information

The command “set keyword-filter” configures the keyword filter parameters as below:

```
BG9002N#set keyword-filter
->Enable Keyword Filter? 'yes' or 'no'[yes]:
->Policy(0-Deny,1-Allow)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#_
```

Figure 1-37 Configure Keyword Filter Parameters

The command “set keyword-filter list” configures the keyword filter list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set keyword-filter list
Keyword Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Keyword[]:qwer
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set keyword-filter list
Keyword Filter List Config:
->Select Config type(0-add,1-del,2-modify)[0]: 2
+----+--------------------------------+
| No |            Keyword             |
+----+--------------------------------+
|0   |1234qwe                         |
+----+--------------------------------+
|1   |qweaszyd                        |
+----+--------------------------------+
->Please input number which you will modify[0-1]:0
->Keyword[1234qwe]:bgzy41
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set keyword-filter list
Keyword Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+--------------------------------+
| No |             Keyword            |
+----+--------------------------------+
|0   |12345                           |
+----+--------------------------------+
|1   |asadf                           |
+----+--------------------------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-38 Configure Keyword Filter List

The following items are displayed on this screen:

► **Keyword Filter:** If enabled, packet filtering is enabled by keyword.

► **Policy:** The policy for filtering web page, Deny and Allow.

1.2.3.5.2 IP Filter

The command “show ip-filter” shows the IP filter information as below:

```
BG9002N#show ip-filter

 Enable MAC Filter.............................: Enable
 Policy........................................: Deny

+----+----------------+--------------------------------+
| No |      IPv4      |              IPv6              |
+----+----------------+--------------------------------+
|0   |192.168.2.3     |                                |
+----+----------------+--------------------------------+

BG9002N#_
```

Figure 1-39 Show IP Filter Information

The command “set ip-filter” configures the IP filter parameters as below:

```
BG9002N#set ip-filter
->Enable IP Filter? 'yes' or 'no'[yes]:
->Policy(0-Deny,1-Allow)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#_
```

Figure 1-40 Configure IP Filter Parameters

The command “set ip-filter list” configures the IP filter list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set ip-filter list
IP Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->IPv4[]:192.168.5.6
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set ip-filter list
IP Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+----+---------------+--------------------------------+
| No |      IPv4     |              IPv6              |
+----+---------------+--------------------------------+
|0   |192.168.2.3    |                                |
+----+---------------+--------------------------------+
|1   |192.168.5.6    |                                |
+----+---------------+--------------------------------+
->Please input number which you will modify[0-1]:1
->IPv4[192.168.5.6]:192.168.6.9
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set ip-filter list
IP Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+---------------+--------------------------------+
| No |      IPv4     |              IPv6              |
+----+---------------+--------------------------------+
|0   |192.168.2.3    |                                |
+----+---------------+--------------------------------+
|1   |192.168.6.9    |                                |
+----+---------------+--------------------------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-41 Configure IP Filter List

The following items are displayed on this screen:

► **IP Filter:** If enabled, packet filtering is enabled by IP address.

► **Policy:** The policy for IP address list. Deny and Allow.

1.2.3.5.3 MAC Filter

The command “show mac-filter” shows the MAC filter information as below:

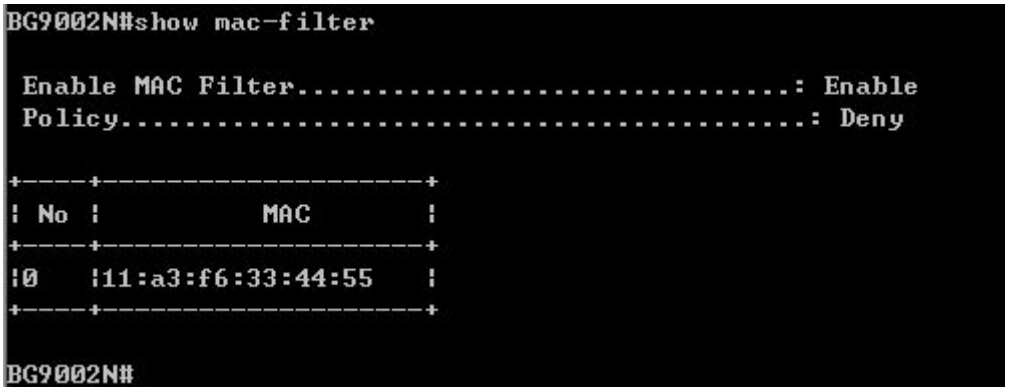


Figure 1-42 Show MAC Filter Information

The command “set mac-filter ” configures the MAC filter parameters as below:

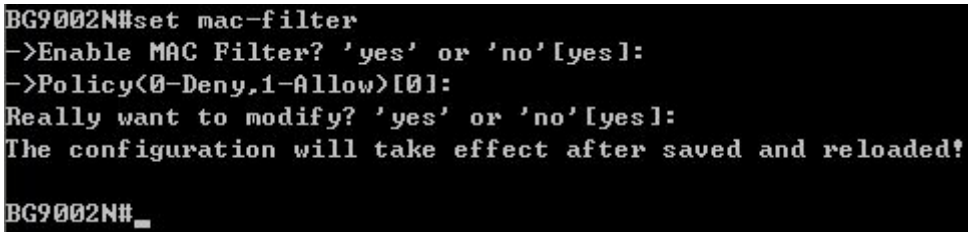
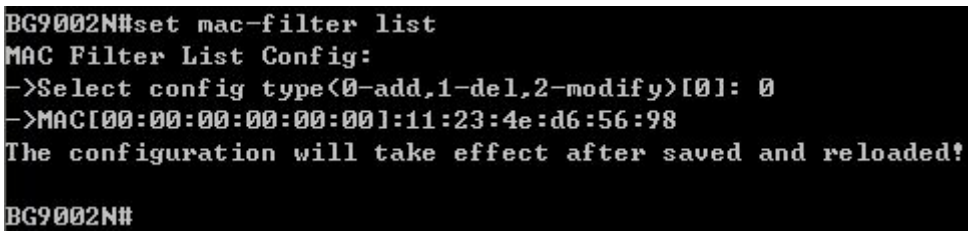
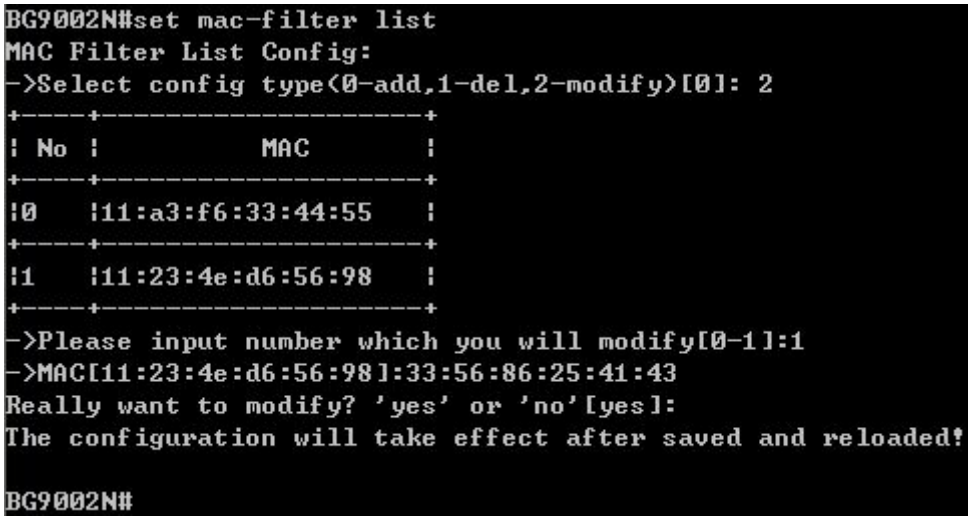


Figure 1-43 Configure IP Filter Parameters

The command “set mac-filter list” configures the MAC filter list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.





```
BG9002N#set mac-filter list
MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+--------------------+
| No |        MAC         |
+----+--------------------+
|0   |11:a3:f6:33:44:55   |
+----+--------------------+
|1   |33:56:86:25:41:43   |
+----+--------------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-44 Configure MAC Filter List

The following items are displayed on this screen:

► **MAC Filter:** If enabled, packet filtering is enabled by MAC.

► **Policy:** The policy for MAC list. Deny and Allow.

1.2.4 QoS

1.2.4.1 Basic Settings

The command “show qos basic-settings” shows the QoS basic settings as below:

```
BG9002N#show qos basic-settings
->Enable QoS.....................................: Enable
->Scheduling mode................................: PQ
->QoS Priority...................................: 802.1P
->Upstream Bandwidth(Kbps).......................: 0
->Downstream Bandwidth(Kbps).....................: 0
->Enable Voice Reservation.......................: Enable
->Voice Reservation Bandwidth(Kbps)..............: 96
->Enable Video Reservation.......................: Disable
->Enable Remap ToS/DSCP to CoS...................: Disable

BG9002N#_
```

Figure 1-45 Show QoS Basic Settings

The command “set qos basic-settings” configures the QoS basic settings as below:

```
BG9002N#set qos basic-settings
->Enable QoS? 'yes' or 'no'[yes]:
->Scheduling mode(0: PQ, 1: WRR, 2: PQ+WRR)[0]: 1
->Weight[0]: 1
->Weight[0]: 2
->Weight[0]: 3
->Weight[0]: 4
->QoS Priority(0:DSCP, 1:802.1p)[1]: 0
->Upstream Bandwidth(Kbps)[0]:
->Downstream Bandwidth(Kbps)[0]:
->Enable Voice Reservation? 'yes' or 'no'[yes]:
->Voice Reservation Bandwidth(Kbps)[96]:
->Enable Video Reservation? 'yes' or 'no'[no]:
->Enable Remap ToS/DSCP to CoS? 'yes' or 'no'[no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-46 Configure QoS Basic Settings

The following items are displayed on this screen:

► **Qos Enable:** Enable or disable QoS functionality.

► **Scheduling Mode:** **PQ:** PQ means strict priority, that is, when congestion occurs, first sending packets of high priority queue.

WRR: All queues use weighted fair queuing scheme which is defined in **Weight Ratio**

PQ+WRR: Only highest queue use strict priority; others use weighted fair queuing scheme.

► **Qos Priority:** **DSCP** and **802.1P:** depending on the value of priority classification into different queues.

► **Upstream Bandwidth:** Configure the bandwidth of upstream.

► **Downstream Bandwidth:** Configure the bandwidth of downstream.

► **Enable Voice Reservation:** Enable voice reservation and give the value to reserved for voice

► **Enable Video Reservation:** Enable video reservation and give the value to reserved for video

► **Remap Tos/DSCP to CoS:** Check the box that the system will remark 802.1P value with TOS/DSCP of upstream packets, the mapping relationship is as follows:

1.2.4.2 Port Rate Limit

The command “show qos port-limit” shows the port rate limit information as below:

```
BG9002N#show qos port-limit
Tips:UP:Unicast; MP:Multicast; BP:Broadcast;
    UUP:Unknown Unicast; UMP:Unknown Multicast;
+----+--------+------------------+------------------+----------------------+
|port|Enable  |Incoming Rate Limit|Outgoing Rate Limit|   Limit Packet type  |
+----+--------+------------------+------------------+----------------------+
|LAN1|Disable | 0 kbps           | 0kbps            |All                   |
+----+--------+------------------+------------------+----------------------+
|LAN2|Disable | 0 kbps           | 0kbps            |UP,MP,UUP,UMP         |
+----+--------+------------------+------------------+----------------------+
|LAN3|Disable | 0 kbps           | 0kbps            |                      |
+----+--------+------------------+------------------+----------------------+
|LAN4|Disable | 0 kbps           | 0kbps            |                      |
+----+--------+------------------+------------------+----------------------+

BG9002N#_
```

Figure 1-47 Show Port Rate Limit Information

The command “set qos port-limit” configures the port rate limit as below:

```
BG9002N#set qos port-limit
->Input port index(1-LAN1, 2-LAN2, 3-LAN3, 4-LAN4)[1]: 1
->Enable rate limit 'yes' or 'no' [no]:y
->Incoming Rate Limit(Kbps)(0~1024000)[0]: 102400
->Outgoing Rate Limit(Kbps)(0~1024000)[0]:
packet type:
  ->all 'yes' or 'no' [yes]:n
  ->unicast 'yes' or 'no' [no]:
  ->multicast 'yes' or 'no' [no]:
  ->broadcast 'yes' or 'no' [no]:
  ->unknown unicast 'yes' or 'no' [no]:
  ->unknown multicast 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no'[yes]:y
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-48 Configure Port Rate Limit

The following items are displayed on this screen:

- ► **Port:** Physical LAN port
- ► **Enable:** Enable or disable rate limit function.
- ► **Incoming Rate Limit:** Enter incoming maximum rate, which must is times of 32Kbsp.
- ►**Limit Packet Type:** Select the packet type which is limited rate.
- ► **Outgoing Rate Limit:** Enter Outgoing maximum rate, which must is times of 32Kbsp.

1.2.4.3 Flow Rate Limit

The command “show qos flow-limit” shows the flow rate limit information as below:

```
BG9002N#show qos flow-limit
+----+--------+---------+--------------+--------------+
| No |Protocol|Direction|   CIR(Kbps)  |   PIR(Kbps)  |
+----+--------+---------+--------------+--------------+
|0   |ANY     |up       | 0            | 0            |
+----+--------+---------+--------------+--------------+

->Enter the index to show(0-0)[0]:0
->IP Range(Start IP).............................:1.0.0.1
->IP Range(End IP)...............................:1.0.0.2
->Active Time(Start Time)........................:00:00
->Active Time(End Time)..........................:00:00
->Active Monday..................................:Disable
->Active Tuesday.................................:Disable
->Active Wednesday...............................:Disable
->Active Thursday................................:Disable
->Active Friday..................................:Disable
->Active Saturday................................:Disable
->Active Sunday..................................:Disable
->Direction......................................:up
->Protocol Type..................................:ANY
->Port Range(Start Port).........................:0
->Port Range(End Port)...........................:0
->CIR............................................:0
->PIR............................................:0

->Show flow rate limit detail para continue or not?[yes]:n

BG9002N#
```

Figure 1-49 Show Flow Rate Limit Information

The command “set qos flow-limit” configures the flow rate limit as below. Enter 0 add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set qos flow-limit
Flow Limit List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->IP Range(Start IP)[]:192.168.5.6
->IP Range(End IP)[]:192.168.5.90
->Active Time(Start Time)[00:00]:
->Active Time(End Time)[00:00]:23:00
->Active Monday? 'yes' or 'no'[no]:
->Active Monday? 'yes' or 'no'[no]:
->Active Tuesday? 'yes' or 'no'[no]:
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Direction(0-up,1-down,2-all)[0]:
->Type(0-Application,1-Custom)[0]:
->Protocol Type(0-HTTP,1-HTTPS,2-FTP,3-TFTP,4-SMTP,5-POP3,6-TELNET,7-ANY)[0]:
->CIR[0]:
->PIR[0]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set qos flow-limit
Flow Limit List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+----+--------+---------+--------------+--------------+
| No |Protocol|Direction|   CIR(Kbps)  |   PIR(Kbps)  |
+----+--------+---------+--------------+--------------+
|0   |ANY     |up       | 0            | 0            |
+----+--------+---------+--------------+--------------+
|1   |HTTP    |up       | 0            | 0            |
+----+--------+---------+--------------+--------------+
->Please input number which you will modify[0-1]:1
->IP Range(Start IP)[192.168.5.6]:
->IP Range(End IP)[192.168.5.90]:
->Active Time(Start Time)[00:00]:
->Active Time(End Time)[23:00]:
->Active Monday? 'yes' or 'no'[no]:
->Active Monday? 'yes' or 'no'[no]:
->Active Tuesday? 'yes' or 'no'[no]:
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Direction(0-up,1-down,2-all)[0]:
->Type(0-Application,1-Custom)[0]:
->Protocol Type(0-HTTP,1-HTTPS,2-FTP,3-TFTP,4-SMTP,5-POP3,6-TELNET,7-ANY)[0]:
->CIR[0]:
->PIR[0]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set qos flow-limit
Flow Limit List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+--------+---------+--------------+--------------+
| No |Protocol|Direction|   CIR(Kbps)  |   PIR(Kbps)  |
+----+--------+---------+--------------+--------------+
|0   |ANY     |up       | 0            | 0            |
+----+--------+---------+--------------+--------------+
|1   |HTTP    |up       | 0            | 0            |
+----+--------+---------+--------------+--------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#_
```

Figure 1-50 Configure Flow Rate Limit

The following items are displayed on this screen:

- ► **IP Range:** The IP range of LAN's PC.
- ► **Active Time:** If not configured, which means that all time are in active
- ► **Active Day:** If not configured, which means that all time in active
- ► **Direction:** **Up: C**heck the frame from the direction of the LAN port to the WAN port, and match the source IP and destination port;

  Down: Check the frame from the direction of the WAN port to the LAN port, and match the destination IP and source port;

Bidirectional: Limit both upstream and downstream speed.

► **Limited Bandwidth(CIR):** The limited bandwidth.

► **Maximal Bandwidth(PIR):** The maximum bandwidth.

If **Application** is selected:

► **Application Protocol:** Such as HTTP, HTTPS, FTP, TFTP, SMTP, POP3, TELNET, etc.

1.2.4.4 Service

The command “show qos service” shows the QoS service information as below:

```
BG9002N#show qos service
->Enable service queue.............................: Enable
->Remap Voice Queue Priority.......................: Enable
->Voice Priority...................................: 3
->Enable remark voice 802.1p.......................: Disable
->Enable remark Voice DSCP.........................: Disable
->Remap MGMT Queue Priority........................: Enable
->MGMT Priority....................................: 2
->Enable remark MGMT 802.1p........................: Disable
->Enable remark MGMT DSCP..........................: Disable
->Remap Video Queue Priority.......................: Enable
->Video Priority...................................: 1
->Enable remark Video 802.1p.......................: Disable
->Enable remark Video DSCP.........................: Disable

BG9002N#_
```

Figure 1-51 Show QoS Service Information

The command “set qos service” configures the QoS service as below:

```
BG9002N#set qos service
service qos:
->Enable service queue? 'yes' or 'no'[yes]:
->Remap Voice Queue Priority? 'yes' or 'no'[yes]:
->Voice Priority(0~3)[3]:
->Enable remark Voice 802.1p? 'yes' or 'no'[no]:
->Enable remark Voice DSCP? 'yes' or 'no'[no]:
->Remap MGMT Queue Priority? 'yes' or 'no'[no]:y
->MGMT Priority(0~3)[2]:
->Enable remark MGMT 802.1p? 'yes' or 'no'[no]:y
->MGMT 802.1p(0~7)[0]:
->Enable remark MGMT DSCP? 'yes' or 'no'[no]:y
->MGMT DSCP(0~63)[0]:
->Remap Video Queue Priority? 'yes' or 'no'[no]:
->Enable remark Video 802.1p? 'yes' or 'no'[no]:
->Enable remark Video DSCP? 'yes' or 'no'[no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-52 Configure QoS Service

The following items are displayed on this screen:

► **Name:** Service name. Read only.

► **Remap Queue Priority:** Check the box to remap scheduling queue.

► **Priority:** There are four levels of priority. Priority 3 is highest, and priority 0 is the lowest

► **Remark 802.1p:** Check the box to enable 802.1p priority remarking.

► **802.1p Value:** The value of remarking 802.1P.

► **Remark DSCP:** Check the box to enable DSCP remarking.

► **DSCP Value:** The value of remarking DSCP.

1.2.4.5 ACL

The command “show qos acl-rule” shows the ACL rule information as below:

```
BG9002N#show qos acl-rule
->input rule id(0~23,all)[0]:
->Rule Name.....: 123
->Bind Port(1-LAN1,2-LAN2,3-LAN3,4-LAN4,5-WAN)....: 0x06
->Rule Type.....: L3 Data
->Src IP.....: 192.168.1.2/255.255.0.0
->Dst IP.....: 139.6.5.9/255.255.0.0
->Drop.....: Disable
->Enable Remark VID.....: Disable
->Enable Remark 802.1P.....: Disable
->Enable Remark DSCP.....: Disable
->Enable Priority.....: Disable
->PIR.....: 0


BG9002N#
```

Figure 1-53 Show ACL Rule Information

The command “set qos acl-rule” configures the ACL rule as below:

```
BG9002N#set qos acl-rule
->Enable ACL 'yes' or 'no' [yes]:
->input rule id(0~23)[0]:
->enable rule 0 'yes' or 'no' [yes]:
->Rule Name[123]: 12345
->Input port member bitmap(Eg: 0x12 include port1,4)[0x6]: 0x05
->Rule Type(0-L2 Data,1-L3 Data)[1]:
 ->Src IP[192.168.1.2]:
 ->Src Netmask[255.255.0.0]:
 ->Dst IP[139.6.5.9]:
 ->Dst Netmask[255.255.0.0]:
 ->Protocol Type(1: icmp, 6: tcp, 17: udp)[0]: 1
->Drop 'yes' or 'no' [no]:
->Enable Remark VID 'yes' or 'no' [no]:
->Enable Remark 802.1P 'yes' or 'no' [no]:
->Enable Remark DSCP 'yes' or 'no' [no]:
->Enable Priority 'yes' or 'no' [no]:
->PIR(0~1024000 Kbps)[0]: 1024000
Really want to modify? 'yes' or 'no'[yes]:y
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-54 Configure ACL Rule

The following items are displayed on this screen:

► **Rule Name:** The custom name.
► **Physical Port:** Rule's source port
► **Rule Type:** Type of rule: **L2 data** or **L3 data**.
► **Src IP/Netmask:** The source IP address and netmask of packets, such as 192.168.100.1/255.255.255.0.
► **Dest IP/Netmask:** The destination IP address and netmask of packets.
► **Protocol:** E.g. ICMP, UDP, TCP, or custom IP protocol types.
► **SRC MAC:** Source MAC address of packets.
► **DEST MAC:** Destination MAC address of packets.
► **Ether Type:** The ether type of packets.
► **VLAN ID:** The VLAN id of packets.
► **802.1p:** The VLAN priority of packets.
► **Drop:** Drop the packets matched with the rule.
► **Remark VID:** Change the VID of packets matched with the rule.
► **Remark 802.1p:** Change the 802.1P priority of packets matched with the rule.
► **Remark DSCP:** Change the DSCP of packets matched with the rule.
► **Priority:** Change the scheduling queue of packets matched with the rule.
► **Maximal Bandwidth:** Limit the bandwidth of packet matched with the rule.

1.2.5 DDNS

The command "show ddns status" shows the DDNS status as below:

```
BG9002N#show ddns status
 DDNS status.....................................: DDNS_TASK_NOT_INIT

BG9002N#
```

Figure 1-55 Show DDNS Status

The command "show ddns parameter" shows the DDNS parameters as below:

```
BG9002N#show ddns parameter
 Enable DDNS.....................................: Enable
 Username........................................: dydns
 Password........................................: 123456
 First Url.......................................: dydns1.com
 Second Url......................................: dydns2.com
 Update Interval.................................: 600
 Server Type.....................................: CUSTOM
 Server Name.....................................: dydns.com
 Server Url......................................: dydns.com
 Dyn DNS Server Name.............................: dydns.com
 Dyn DNS Server Url..............................: dydns.com
 System Item.....................................: dydns.com

BG9002N#
```

Figure 1-56 Show DDNS Parameters

The command "set ddns" configures the DDNS parameters as below:

Figure 1-57 Configure DDNS Parameters

The following items are displayed on this screen:

► **DDNS Enable:** Active or inactive dynamic DNS service.

► **Username:** Enter account name of your DDNS account.

► **Password:** Enter password of your DDNS account.

► **First Url:** First domain name that you registered your DDNS service provider.

► **Second Url:** First domain name that you registered your DDNS service provider.

► **Update Interval:** How often, in seconds, the IP is updated.

► **Server Type:** optional DDNS server type, can select from pull-dwon list:

DYNDNS: For dyndns.org

FREEDNS: For freedns.afraid.org

ZONE: For zoneedit.com

NOIP: For no-ip.com

3322: For 3322.org

CUSTOM: For custom self-defined DDNS server type.

► **Server Name:** If CUSTOM is selected, specify server name of the device.

► **Server Url:** If CUSTOM is selected, specify server URL of the device.

► **Dyn DNS Server Name:** If CUSTOM is selected, specify dyndns DNS server name of custom self-defined.

► **Dyn DNS Server Url:** If CUSTOM is selected, specify dyndns DNS server URL of custom self-defined.

► **System Item:** If CUSTOM is selected, specify system item of custom self-defined.

► **DDNS Status:** Display the status of DDNS service. Read only.

1.2.6 VPN

1.2.6.1 PPTP Server

The command “show pptp-server” shows the pptp server information as below:

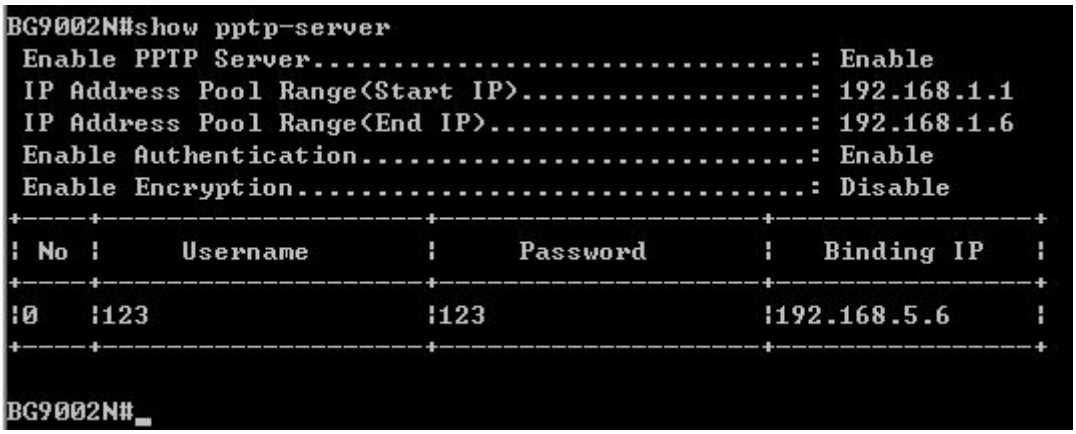


Figure 1-58 Show PPTP Server Information

The command “set pptp-server” configures the pptp server parameters as below:

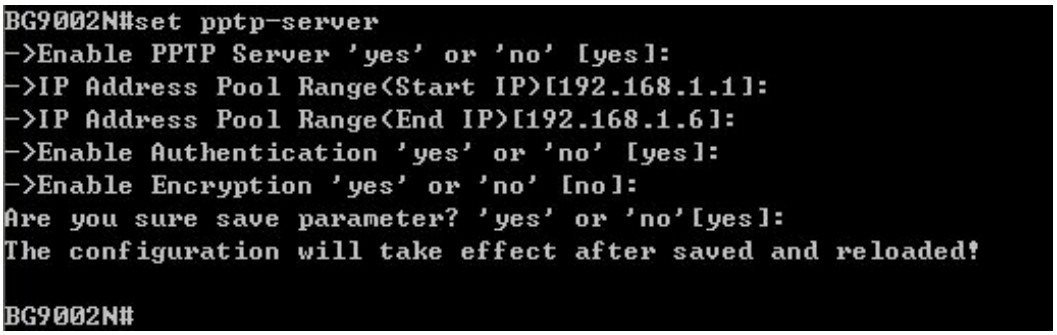


Figure 1-59 Configure PPTP Server Parameters

The following items are displayed on this screen:

► **Enable PPTP Server:** Enable or disable the PPTP server function globally.

► **IP Address Pool Range:** Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP ranges must not overlap.

► **Enable Authentication:** Specify whether to enable authentication for the tunnel.

► **Enable Encryption:** Specify whether to enable the encryption for the tunnel. If enabled, the PPTP tunnel will be encrypted by MPPE.

The command “set pptp-server user” configures the pptp server user list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set pptp-server user
PPTPServer User List Config:
->Select Config type(0-add,1-del,2-modify)[0]: 1
+----+--------------------+--------------------+----------------+
| No |     Username       |     Password       |   Binding IP   |
+----+--------------------+--------------------+----------------+
|0   |123qwe              |qweasd              |192.168.5.6     |
+----+--------------------+--------------------+----------------+
|1   |wepasd              |123456              |136.23.6.8      |
+----+--------------------+--------------------+----------------+

->Please choose the start Index of deleting entry[0-1]:1
->Please choose the end Index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-60 Configure PPTP Server User

The following items are displayed on this screen:

► **Username:** Enter the account name of PPTP tunnel. It should be configured identically on server and client.

► **Password:** Enter the password of PPTP tunnel. It should be configured identically on server and client.

► **Binding IP:** Enter the IP address of the client which is allowed to connect to this PPTP server.

1.2.6.2 L2TP Server

The command “show l2tp-server” shows the l2tp server information as below:

```
BG9002N#show l2tp-server
 Enable L2TP Server.................................: Enable
 Local IP...........................................: 10.0.0.1
 IP Address Pool Range(Start IP)....................: 10.0.0.1
 IP Address Pool Range(End IP)......................: 10.0.0.1
 Enable Authentication..............................: Enable
 L2TP Auth Secret...................................: 123456
 Enable Debug.......................................: Enable
+----+--------------------+--------------------+----------------+
| No |     Username       |     Password       |   Binding IP   |
+----+--------------------+--------------------+----------------+
|0   |1234                |1234                |138.2.61.136    |
+----+--------------------+--------------------+----------------+
|1   |1123                |54321               |136.56.22.65    |
+----+--------------------+--------------------+----------------+

BG9002N#
```

Figure 1-61 Show L2TP Server Information

The command “set l2tp-server” configures the l2tp server parameters as below:

```
BG9002N#set l2tp-server
->Enable L2TP Server 'yes' or 'no' [yes]:
->Local IP[10.0.0.1]:
->IP Address Pool Range(Start IP)[10.0.0.1]:
->IP Address Pool Range(End IP)[10.0.0.1]:
->Enable Authentication 'yes' or 'no' [yes]:
->L2TP Auth Secret[123456]:
->Enable Debug 'yes' or 'no' [yes]:
Are you sure save parameter? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-62 Configure L2TP Server Parameters

The following items are displayed on this screen:

► **Enable L2TP Server:** Enable or disable the L2TP server function globally.

► **Local IP:** Enter the local IP address of L2TP server.

► **IP Address Pool Range:** Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP ranges must not overlap.

► **Enable Authentication:** Specify whether to enable authentication for the tunnel. If enabled, enter the authentication secret.

► **Enable Debug:** Specify whether to enable the debug for L2TP.

The command “set l2tp-server user” configures the l2tp server user list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify .If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set l2tp-server user
L2TPServer User List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Username[]:yzasd
->Password[]:123654
->Pointed IP[]:195.6.5.9
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set l2tp-server user
L2TPServer User List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+----+--------------------+--------------------+----------------+
| No |     Username       |     Password       |   Binding IP   |
+----+--------------------+--------------------+----------------+
|0   |1234                |1234                |138.2.61.136    |
+----+--------------------+--------------------+----------------+
|1   |1123                |54321               |136.56.22.65    |
+----+--------------------+--------------------+----------------+
|2   |yzasd               |123654              |195.6.5.9       |
+----+--------------------+--------------------+----------------+
->Please input number which you will modify[0-2]:2
->Username[yzasd]:
->Password[123654]:123456
->Pointed IP[195.6.5.9]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set l2tp-server user
L2TPServer User List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+--------------------+--------------------+----------------+
| No |     Username       |     Password       |   Binding IP   |
+----+--------------------+--------------------+----------------+
|0   |1234                |1234                |138.2.61.136    |
+----+--------------------+--------------------+----------------+
|1   |1123                |54321               |136.56.22.65    |
+----+--------------------+--------------------+----------------+
|2   |yzasd               |123456              |195.6.5.9       |
+----+--------------------+--------------------+----------------+

->Please choose the start index of deleting entry[0-2]:2
->Please choose the end index of deleting entry[0-2]:2
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-63 Configure L2TP Server User

The following items are displayed on this screen:

► **Username:** Enter the account name of L2TP tunnel. It should be configured identically on server and client.

► **Password:** Enter the password of L2TP tunnel. It should be configured identically on server and client.

► **Binding IP:** Enter the IP address of the client which is allowed to connect to this L2TP server.

1.2.6.3 IPSEC

1.2.6.3.1 IKE Safety Proposal

The command “show ike-proposal” shows the IKE Proposal information as below:

```
BG9002N#show ike-proposall
+----+------------------+--------------------+----------------+----------+
| No |    Proposal Name  |Encryption Algorithm| Auth Algorithm | DH Group |
+----+------------------+--------------------+----------------+----------+
|0   | ike123            | 3DES               | SHA1           | modp1536 |
+----+------------------+--------------------+----------------+----------+

BG9002N#
```

Figure 1-64 Show IKE Proposal Information

The command “set ike-proposal” configures the IKE Proposal as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set ike-proposall

->IKE Proposal:0-Add,1-Delete,2-Modify[0]:0
->Proposal Name[]:ike_pro_11
->Encryption Algorithm(0-3DES,1-DES,2-AES)[0]:
->Auth Algorithm(0-SHA1,1-MD5)[0]:
->DH Group(0-modp1536,1-modp1024 ,2-modp768)[0]:
->Really want to modify? 'yes' or 'no'[yes]:

  Oprate success!
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set ike-proposall

->IKE Proposal:0-Add,1-Delete,2-Modify[0]:2
+----+------------------+--------------------+----------------+----------+
| No |    Proposal Name  |Encryption Algorithm| Auth Algorithm | DH Group |
+----+------------------+--------------------+----------------+----------+
|0   | ike123            | 3DES               | SHA1           | modp1536 |
+----+------------------+--------------------+----------------+----------+
|1   | ike_pro_11        | 3DES               | SHA1           | modp1536 |
+----+------------------+--------------------+----------------+----------+
->Enter the index to modify(0-1)[0]:0
->Proposal Name[ike123]:ike1
->Encryption Algorithm(0-3DES,1-DES,2-AES)[0]:1
->Auth Algorithm(0-SHA1,1-MD5)[0]:1
->DH Group(0-modp1536,1-modp1024 ,2-modp768)[0]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

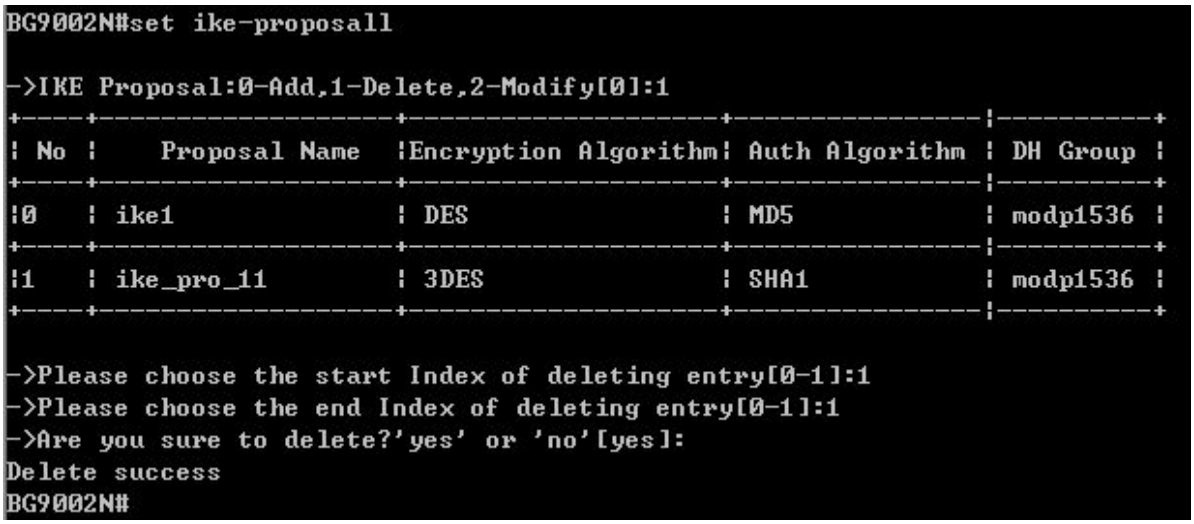


Figure 1-65 Configure IKE Proposal

The following items are displayed on this screen:

► **Proposal Name:** Specify a unique name to the IKE proposal for identification and management purposes. The IKE proposal can be applied to IPSEC proposal.

► **Encryption Algorithm:** Specify the encryption algorithm for IKE negotiation. Options include:

DES: DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a 56-bit key.

3DES: Triple DES, encrypts a plain text with 168-bit key.

AES: Uses the AES algorithm for encryption.

► **Auth Algorithm:** Select the authentication algorithm for IKE negotiation. Options include:

MD5: MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.

SHA1: SHA1 (Secure Hash Algorithm) takes a message less than 2^64 (the 64th power of 2) in bits and generates a 160-bit message digest.

► **DH Group:** Select the DH (Diffie-Hellman) group to be used in key negotiation phase 1. The DH Group sets the strength of the algorithm in bits. Options include **DH 768 modp**, **DH 1024 modp** and **DH 1536 modp**.

1.2.6.3.2 IKE Safety Policy

The command “show ike-policy” shows the IKE Policy information as below:

```
BG9002N#show ike-policy
+----+-----------------+-------------+----------+--------------+
| No |   Policy Name   |Operation Mode| Auth Mode|  PreShareKey |
+----+-----------------+-------------+----------+--------------+
|0   | ike_policy_1    |Main Mode    | PSK      | 123321       |
+----+-----------------+-------------+----------+--------------+

->Enter the index to show(0-0)[0]:
 Policy Name.....................................:ike_policy_1
 Operation Mode..................................:Main Mode
 Enable Local ID.................................:Disable
 Enable Remote ID................................:Disable
 Auth Mode.......................................:PSK
 Pre Share Key...................................:123321
 Enable Safety Proposal1.........................:Enable
 Proposal Name1..................................:ike123
 Enable Safety Proposal2.........................:Disable
 Enable Safety Proposal3.........................:Disable
 Enable Safety Proposal4.........................:Disable

->Show IKE policy detail para continue or not?[yes]:n

BG9002N#
```

Figure 1-66 Show IKE Policy Information

The command “set ike-policy” configures the IKE Policy as below. Enter 0 add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set ike-policy

->IKE Policy:0-Add,1-Delete,2-Modify[0]:0
->Policy Name[]:ike_po_2
->Operation Mode(0-Main Mode,1-Challenge Mode)[0]:1
->Enable Local ID(yes/no)[no]:
->Enable Remote ID(yes/no)[no]:
->Auth Mode(0-PSK,1-RSA,2-Certificate)[0]:1
->Pre Share Key[]:123456
->Enable Safety Proposal 1(yes/no)[no]:
->Enable Safety Proposal 2(yes/no)[no]:
->Enable Safety Proposal 3(yes/no)[no]:
->Enable Safety Proposal 4(yes/no)[no]:
->Really want to modify? 'yes' or 'no'[yes]:

  Oprate success!
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set ike-policy

->IKE Policy:0-Add,1-Delete,2-Modify[0]:2
+----+----------------+-------------+----------+--------------+
| No |   Policy Name  |Operation Mode| Auth Mode|  PreShareKey |
+----+----------------+-------------+----------+--------------+
|0   | ike_policy_1   |Main Mode    | PSK      | 123321       |
+----+----------------+-------------+----------+--------------+
|1   | ike_po_2       |Challenge Mode| RSA      | 123456       |
+----+----------------+-------------+----------+--------------+
->Enter the index to modify(0-1)[0]:1
->Policy Name[ike_po_2]:
->Operation Mode(0-Main Mode,1-Challenge Mode)[1]:0
->Enable Local ID(yes/no)[no]:
->Enable Remote ID(yes/no)[no]:
->Auth Mode(0-PSK,1-RSA,2-Certificate)[1]:
->Pre Share Key[123456]:
->Enable Safety Proposal 1(yes/no)[no]:
->Enable Safety Proposal 2(yes/no)[no]:
->Enable Safety Proposal 3(yes/no)[no]:
->Enable Safety Proposal 4(yes/no)[no]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set ike-policy

->IKE Policy:0-Add,1-Delete,2-Modify[0]:1
+----+----------------+-------------+----------+--------------+
| No |   Policy Name  |Operation Mode| Auth Mode|  PreShareKey |
+----+----------------+-------------+----------+--------------+
|0   | ike_policy_1   |Main Mode    | PSK      | 123321       |
+----+----------------+-------------+----------+--------------+
|1   | ike_po_2       |Main Mode    | RSA      | 123456       |
+----+----------------+-------------+----------+--------------+

->Please choose the start Index of deleting entry[0-1]:1
->Please choose the end Index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-67 Configure IKE Policy

The following items are displayed on this screen:

► **Policy Name:** Specify a unique name to the IKE policy for identification and management purposes. The IKE policy can be applied to IPSEC policy.

► **Operation Mode:** Select the IKE Exchange Mode in phase 1, and ensure the remote VPN peer uses the same mode.

Main: Main mode provides identity protection and exchanges more information, which applies to the scenarios with higher requirement for identity protection.

Challenge: Challenge Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirement for identity protection.

► **Enable Local ID:** If enabled, enter a name for the local device as the ID in IKE negotiation.

► **Enable Remote ID:** If enabled, enter the name of the remote peer as the ID in IKE negotiation.

► **Auth Mode:** Select the authentication mode for this IKE policy entry.

► **Pre Share Key:** Enter the Pre-shared Key for IKE authentication, and ensure both the two peers use the same key. The key should consist of visible characters without blank space.

► **Enable Safety Proposal:** Select the Proposal for IKE negotiation phase 1. Up to four proposals can be selected.

1.2.6.3.3 IPSEC Safety Proposal

The command “show ipsec-proposal” shows the IPSEC Proposal information as below:

```
BG9002N#show ipsec-proposal
+----+----------------+--------------------+----------------+--------------+
| No |  Proposal Name |Encryption Algorithm| Auth Algorithm |IPSEC Protocol|
+----+----------------+--------------------+----------------+--------------+
|0   |ipsec123        |3DES                | SHA1           | ESP          |
+----+----------------+--------------------+----------------+--------------+

BG9002N#
```

Figure 1-68 Show IPSEC Proposal Information

The command “set ipsec-proposal” configures the IPSEC Proposal as below. Enter 0 add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set ipsec-proposall

->IPSEC Proposal:0-Add,1-Delete,2-Modify[0]:
->Proposal Name[]:1234
->Encryption Algorithm(0-3DES,1-DES,2-AES)[0]:1
->Auth Algorithm(0-SHA1,1-MD5)[0]:1
->IPSEC Protocol(0-ESP,1-AH,2-ESP+AH)[0]:1
->Really want to modify? 'yes' or 'no'[yes]:

  Oprate success!
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set ipsec-proposall

->IPSEC Proposal:0-Add,1-Delete,2-Modify[0]:2
+----+---------------+--------------------+----------------+--------------+
| No |  Proposal Name |Encryption Algorithm| Auth Algorithm |IPSEC Protocol|
+----+---------------+--------------------+----------------+--------------+
|0   |ipsec123        |3DES                | SHA1           | ESP          |
+----+---------------+--------------------+----------------+--------------+
|1   |1234            |DES                 | MD5            | AH           |
+----+---------------+--------------------+----------------+--------------+
->Enter the index to modify(0-1)[0]:1
->Proposal Name[1234]:
->Encryption Algorithm(0-3DES,1-DES,2-AES)[1]:2
->Auth Algorithm(0-SHA1,1-MD5)[1]:1
->IPSEC Protocol(0-ESP,1-AH,2-ESP+AH)[1]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set ipsec-proposall

->IPSEC Proposal:0-Add,1-Delete,2-Modify[0]:1
+----+---------------+--------------------+----------------+--------------+
| No |  Proposal Name |Encryption Algorithm| Auth Algorithm |IPSEC Protocol|
+----+---------------+--------------------+----------------+--------------+
|0   |ipsec123        |3DES                | SHA1           | ESP          |
+----+---------------+--------------------+----------------+--------------+
|1   |1234            |AES                 | MD5            | AH           |
+----+---------------+--------------------+----------------+--------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-69 Configure IPSEC Proposal

The following items are displayed on this screen:

► **Proposal Name:** Specify a unique name to the IPSEC Proposal for identification and management purposes. The IPSEC proposal can be applied to IPSEC policy.

► **IPSec Protocol:** Select the security protocol to be used. Options include:

AH: AH (Authentication Header) provides data origin authentication, data integrity and anti-replay services.

ESP: ESP (Encapsulating Security Payload) provides data encryption in addition to origin authentication, data integrity, and anti-replay services.

ESP+AH: Both ESP and AH security protocol.

► **Encryption Algorithm:** Select the algorithm used to encrypt the data for ESP encryption. Options include:

DES: DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a 56-bit key. The key should be 8 characters.

3DES: Triple DES, encrypts a plain text with 168-bit key. The key should be 24 characters.

AES: Uses the AES algorithm for encryption. The key should be 16 characters.

► **Auth Algorithm:** Select the algorithm used to verify the integrity of the data. Options include:

MD5: MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.

SHA: SHA (Secure Hash Algorithm) takes a message less than the 64th power of 2 in bits and generates a 160-bit message digest.

1.2.6.3.4 IPSEC Safety Policy

The command “show ipsec-policy” shows the IPSEC Policy information as below:

```
BG9002N#show ipsec-policy
+----+----------------+-----------+---------+-------------+----------------+
| NO |IPSEC Policy Name|Enable IPSEC|Interface|   VPN Mode    | Remote Address |
+----+----------------+-----------+---------+-------------+----------------+
|0   |ipsec_policy_1   | Enable     | DATA    |PC To Site    |138.60.61.20    |
+----+----------------+-----------+---------+-------------+----------------+

->Enter the index to show(0-0)[0]:
 Proposal Name.....................................:ipsec_policy_1
 Enable IPSEC......................................:Enable
 VPN Mode..........................................:PC To Site
 Interface.........................................:DATA
 Local Subnet IP...................................:192.168.20.9
 Local Subnet Netmask..............................:255.255.255.0
 Remote Address....................................:138.60.61.20
 Remote Subnet IP..................................:0.0.0.0
 Remote Subnet Netmask.............................:0.0.0.0
 IKE Policy Name...................................:ike_policy_1
 Enable IPSEC Proposal1............................:Enable
 Proposal Name1....................................:ipsec123
 Enable IPSEC Proposal2............................:Disable
 Enable IPSEC Proposal3............................:Disable
 Enable IPSEC Proposal4............................:Disable

->Show IPSEC policy detail para continue or not?[yes]:n

BG9002N#
```

Figure 1-70 Show IPSEC Policy Information

The command “set ipsec-policy” configures the IPSEC Policy as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set ipsec-policy

->IPSEC Policy:0-Add,1-Delete,2-Modify[0]:
->Proposal Name[]:12345
->Enable IPSEC(yes/no)[no]:y
->VPN Mode(0-Site To Site,1-PC To Site)[0]:
->Interface([0]DATA)[0]:
->Local Subnet IP[]:192.168.1.2
->Local Subnet Netmask[]:255.255.0.0
->Remote Address[]:139.6.5.8
->Enable IPSEC Proposal 1(yes/no)[no]:
->Enable IPSEC Proposal 2(yes/no)[no]:
->Enable IPSEC Proposal 3(yes/no)[no]:
->Enable IPSEC Proposal 4(yes/no)[no]:
->IKE Policy Name[]:ike_policy_1
->Really want to modify? 'yes' or 'no'[yes]:

  Oprate success!
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set ipsec-policy

->IPSEC Policy:0-Add,1-Delete,2-Modify[0]:2
+----+----------------+-----------+---------+-------------+----------------+
| NO |IPSEC Policy Name|Enable IPSEC|Interface|   VPN Mode   | Remote Address |
+----+----------------+-----------+---------+-------------+----------------+
|0   |ipsec_policy_1   | Enable     | DATA    |PC To Site    |138.60.61.20    |
+----+----------------+-----------+---------+-------------+----------------+
|1   |12345            | Enable     | DATA    |Site To Site  |139.6.5.8       |
+----+----------------+-----------+---------+-------------+----------------+
->Enter the index to modify(0-1)[0]:1
->Proposal Name[12345]:asdfg
->Enable IPSEC(yes/no)[yes]:
->VPN Mode(0-Site To Site,1-PC To Site)[0]:
->Interface([0]DATA)[0]:
->Local Subnet IP[192.168.1.2]:
->Local Subnet Netmask[255.255.0.0]:
->Remote Address[139.6.5.8]:
->Enable IPSEC Proposal 1(yes/no)[no]:
->Enable IPSEC Proposal 2(yes/no)[no]:
->Enable IPSEC Proposal 3(yes/no)[no]:
->Enable IPSEC Proposal 4(yes/no)[no]:
->IKE Policy Name[ike_policy_1]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set ipsec-policy

->IPSEC Policy:0-Add,1-Delete,2-Modify[0]:1
+----+-----------------+------------+---------+--------------+-----------------+
| NO |IPSEC Policy Name|Enable IPSEC|Interface|   VPN Mode   | Remote Address |
+----+-----------------+------------+---------+--------------+-----------------+
|0   |ipsec_policy_1   | Enable     | DATA    |PC To Site    |138.60.61.20     |
+----+-----------------+------------+---------+--------------+-----------------+
|1   |asdfg            | Enable     | DATA    |Site To Site  |139.6.5.8        |
+----+-----------------+------------+---------+--------------+-----------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-71 Configure IPSEC Policy

The following items are displayed on this screen:

► **Enable Ipsec:** Enable or disable this IPSEC entry.

► **IPSEC Policy Name:** Specify a unique name to the IPSEC policy.

► **Select Interface:** Specify the local WAN port for this Policy.

► **VPN Mode:** Select the network mode for IPSEC policy. Options include:

Site To Site: Select this option when the client is a network.

PC to Site: Select this option when the client is a host.

► **Local Subnet IP & Local Subnet Netmask:** Specify IP address range on your local LAN to identify which PCs on your LAN are covered by this policy.

► **Remote Address:** If **PC to Site** is selected, specify IP address on your remote network to identify which PCs on the remote network are covered by this policy.

► **Remote Subnet IP & Remote Subnet Netmask:** Specify IP address range on your remote network to identify which PCs on the remote network are covered by this policy.

► **IKE Safety Policy:** Specify the IKE policy.

► **Enable Safety Prososal: If enabled,** Select IPSEC Proposal.

1.2.7 Routing

1.2.7.1 Static Route

1.2.7.1.1 IPv4

The command “show static-route ipv4” shows the IPv4 static route information as below:

```
BG9002N#show static-route ipv4
+----+--------+----------------+---------------+---------------+----------+
| No | Enable |   Destination  |     Netmask   |     Next Hop  |   Valid  |
+----+--------+----------------+---------------+---------------+----------+
|0   |Enable  |192.168.12.6    |255.255.255.0  |DATA           |Invalid   |
+----+--------+----------------+---------------+---------------+----------+

BG9002N#_
```

Figure 1-72 Show IPv4 Static Route Information

The command “set static-route ipv4” configures the IPv4 static route as below.

```
BG9002N#set static-route ipv4
->Please input ipv4 static route index(0-9)[0]: 1
->Enable Route 'yes' or 'no' [no]:y
->Destination[192.168.16.5]:
->Netmask[255.255.255.0]:
->Next Hop Type(0-Interface,1-Address)[1]:
->Gateway[192.168.10.1]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-73 Configure IPv4 Static Route

The following items are displayed on this screen:

- ► **Enable:** Select it to add and modify the current route. Conversely, disable the current route.
- ► **Destination IP:** Enter the destination host the route leads to.
- ► **Netmask:** Enter the Subnet mask of the destination network.
- ► **Next Hop Type:** Include **Next Hop Interface** and **Next Hop Address**(see following option)
- ► **Next Hop Interface:** Specify the interface of next hop for current route
- ► **Next Hop Address:** Specify the address of next hop for current route
- ► **Valid:** Show the status of current route.

1.2.7.1.2 IPv6

The command “show static-route ipv6” show the IPv6 static route information as below:

```
BG9002N#show static-route ipv6
+----+--------+------------------------------+--------------------+----------+
| No | Enable |Destination IPv6/Prefix Length|       Next Hop     |   Valid  |
+----+--------+------------------------------+--------------------+----------+
|0   |Enable  |2001::1/64                    |WAN                 |Valid     |
+----+--------+------------------------------+--------------------+----------+

BG9002N#
```

Figure 1-74 Show IPv6 Static Route Information

The command “set static-route ipv6” configures the IPv6 static route as below.

```
BG9002N#set static-route ipv6
->Please input ipv6 static route index(0-9)[0]: 1
->Enable Route 'yes' or 'no' [no]:y
->Destination IPv6[]: 2001::2
->IPv6 Prefix Length[64]:
->Next Hop Type(0-Interface,1-Address)[0]:
->Next Hop Interface(0-WAN)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-75 Configure IPv6 Static Route

The configuration options of Ipv6 is similar to Ipv4, the prefix length is equal to mask of Ipv4 address.

1.2.7.2 Policy Route

The command “show policy-route” shows the policy route information as below:

```
BG9002N#show policy-route
+----+-------+------------------------------+----------------+---------------+
| No | Enable|          Src IP Range        | Dst Port Range |    Next Hop   |
+----+-------+------------------------------+----------------+---------------+
|0   |Enable |0.0.0.0-0.0.0.0               |0-0             |DATA           |
+----+-------+------------------------------+----------------+---------------+

->Enter the index to show(0-0)[0]:
 Enable Polocy Route.............................:Enable
 Next Hop Type(0-Interface,1-Address)............:Interface
 Next Hop Interface..............................:DATA
 Protocol Type(0-ALL,1-TCP,2-UDP)................:ALL
 Source IP(Start IP).............................:0.0.0.0
 Source IP(End IP)...............................:0.0.0.0
 Destination IP(Start IP)........................:0.0.0.0
 Destination IP(End IP)..........................:0.0.0.0
 Destination Port(Start Port)....................:0
 Destination Port(End Port)......................:0
 Active Time(Start Time).........................:00:00
 Active Time(End Time)...........................:23:59
 Active Monday...................................:Disable
 Active Tuesday..................................:Disable
 Active Wednesday................................:Disable
 Active Thursday.................................:Disable
 Active Friday...................................:Disable
 Active Saturday.................................:Disable
 Active Sunday...................................:Disable

->Show policy route detail para continue or not?[yes]:n

BG9002N#
```

Figure 1-76 Show Policy Route Information

The command “set policy-route” configure thes policy route as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set policy-route
Policy Route List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Enable Polocy Route? 'yes' or 'no'[no]:y
->Next Hop Type(0-Interface,1-Address)[0]:
->Next Hop Interface([0]DATA [30]3G Modem [31]DATA VPN)[0]:30
->Protocol Type(0-ALL,1-TCP,2-UDP)[0]:
->Source IP(Start IP)[]:192.16.5.6
->Source IP(End IP)[]:192.168.5.90
->Destination IP(Start IP)[]:136.5.6.4
->Destination IP(End IP)[]:136.5.6.8
->Destination Port(Start Port)[0]:1000
->Destination Port(End Port)[0]:2000
->Active Time(Start Time)[00:00]:
->Active Time(End Time)[00:00]:23:00
->Active Monday? 'yes' or 'no'[no]:
->Active Monday? 'yes' or 'no'[no]:
->Active Tuesday? 'yes' or 'no'[no]:
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set policy-route
Policy Route List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+----+-------+-------------------------------+----------------+---------------+
| No | Enable|           Src IP Range        | Dst Port Range |    Next Hop   |
+----+-------+-------------------------------+----------------+---------------+
|0   |Enable |0.0.0.0-0.0.0.0                |0-0             |DATA           |
+----+-------+-------------------------------+----------------+---------------+
|1   |Enable |192.16.5.6-192.168.5.90        |1000-2000       |3G             |
+----+-------+-------------------------------+----------------+---------------+
->Please input number which you will modify[0-1]:1
->Enable Polocy Route? 'yes' or 'no'[yes]:
->Next Hop Type(0-Interface,1-Address)[0]:
->Next Hop Interface([0]DATA [30]3G Modem [31]DATA VPN)[30]:
->Protocol Type(0-ALL,1-TCP,2-UDP)[0]:
->Source IP(Start IP)[192.16.5.6]:
->Source IP(End IP)[192.168.5.90]:
->Destination IP(Start IP)[136.5.6.4]:
->Destination IP(End IP)[136.5.6.8]:
->Destination Port(Start Port)[1000]:
->Destination Port(End Port)[2000]:
->Active Time(Start Time)[00:00]:
->Active Time(End Time)[23:00]:
->Active Monday? 'yes' or 'no'[no]:
->Active Monday? 'yes' or 'no'[no]:
->Active Tuesday? 'yes' or 'no'[no]:
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set policy-route
Policy Route List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+----+-------+------------------------------+----------------+---------------+
| No | Enable|           Src IP Range       | Dst Port Range |    Next Hop   |
+----+-------+------------------------------+----------------+---------------+
|0   |Enable |0.0.0.0-0.0.0.0               |0-0             |DATA           |
+----+-------+------------------------------+----------------+---------------+
|1   |Enable |192.16.5.6-192.168.5.90       |1000-2000       |3G             |
+----+-------+------------------------------+----------------+---------------+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

Figure 1-77 Configure Policy Route

The following items are displayed on this screen:

- ► **Enable PoliceRoute:** Enable or disable the entry
- ► **Next Hop Type:** Select from pull-down list: **Interface, Address.**
- ► **Interface:** Specify the interface of next hop for the entry.
- ► **Address:** Specify the address of next hop for the entry.
- ► **Description:** Give description for the entry.
- ► **Protocol:** Specify the protocol, **TCP**, **UDP** or **ALL**.
- ► **Source IP:** Enter IP address or IP range of source in the rule entry.
- ► **Destination IP:** Enter IP address or IP range of destination in the rule entry.
- ► **Destination Port:** Specify port or port range of destination in the rule entry.
- ► **Active Time:** Specify the active time range for the rule entry.
- ► **Active Day:** Specify the active days for the rule entry.

1.2.7.3 RIP

1.2.7.3.1 RIP Service

The command “show rip” shows the RIP information as below:

```
BG9002N#set ip-filter conf
->Enable IP Filter? 'yes' or 'no'[yes]:y
->Policy(0-Deny,1-Allow)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-78 Show RIP Information

The command “set rip switch” configures the RIP switch as below:

```
BG9002N#set rip switch
->Enable RIP Protocol 'yes' or 'no' [yes]:
Really want to modify? 'yes' or 'no'[yes]:

BG9002N#_
```

Figure 1-79 Configure RIP Switch

The following items are displayed on this page:

► **Enable RIP Service:** Enable or disable RIP service function globally.

The command “set rip interface” configures the RIP interface as below.

```
BG9002N#set rip interface

RIP Interface List:
  +----+--------+-------+-------+----------+----------+----------------+
  | NO |Inteface|Version|Auth   |AuthKeyMode |KeyFrom    |Key             |
  +----+--------+-------+-------+----------+----------+----------------+
  |0   |DATA    |R2 S2  |disable|simple key  |string     |                |
  +----+--------+-------+-------+----------+----------+----------------+
Rip Interface List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Interface(0-Data,1-Voice,2-Mgmt,3-Other1,4-Other2):[0] 1
->Interface Recv RIP Version(1-RIPv1, 2-RIPv2)[2]:
->Interface Send RIP Version(1-RIPv1, 2-RIPv2)[2]:
->Enable Interface RIP Authentication 'yes' or 'no' [no]:y
->Interface RIP Authentication Key Mode(0-text, 1-md5)[0]:
->Interface RIP Authentication Key Get Mode(0-simple Key, 1-key chain)[0]:
->Interface RIP Authentication Simple Key[]: 123
->Continue to Add RIP Interface? 'yes' or 'no'[no]: n

BG9002N#
```

```
BG9002N#set rip interface

RIP Interface List:
  +----+--------+-------+-------+----------+----------+----------------+
  | NO |Inteface|Version|Auth   |AuthKeyMode |KeyFrom    |Key             |
  +----+--------+-------+-------+----------+----------+----------------+
  |0   |DATA    |R2 S2  |disable|simple key  |string     |                |
  +----+--------+-------+-------+----------+----------+----------------+
  |1   |VOICE   |R2 S2  |enable |simple key  |string     |123             |
  +----+--------+-------+-------+----------+----------+----------------+
Rip Interface List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
Enter the index to modify(0-1)[0]: 1
->Interface(0-Data,1-Voice,2-Mgmt,3-Other1,4-Other2)[1]: 2
->Interface Recv RIP Version(1-RIPv1, 2-RIPv2)[2]: 1
->Interface Send RIP Version(1-RIPv1, 2-RIPv2)[2]:
->Enable Interface RIP Authentication 'yes' or 'no' [yes]:
->Interface RIP Authentication Key Mode(0-text, 1-md5)[0]:
->Interface RIP Authentication Key Get Mode(0-simple Key, 1-key chain)[0]:
->Interface RIP Authentication Simple Key[123]:
->Really want to modify? 'yes' or 'no'[no]: y
  The configuration will take effect after saved and reloaded!
```

```
RIP Interface List:
  +----+--------+-------+-------+-----------+-----------+----------------+
  | NO |Inteface|Version|Auth   |AuthKeyMode |KeyFrom    |Key             |
  +----+--------+-------+-------+-----------+-----------+----------------+
  |0   |DATA    |R2 S2  |disable|simple key  |string     |                |
  +----+--------+-------+-------+-----------+-----------+----------------+
  |1   |MGMT    |R1 S2  |enable |simple key  |string     |123             |
  +----+--------+-------+-------+-----------+-----------+----------------+
Rip Interface List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
->Please input begin index(0-1)[0]: 1
->Please input end index(0-1)[0]: 1
  Delete success

BG9002N#
```

Figure 1-80 Configure RIP Interface

The following items are displayed on this screen:

- ► **Interface:** Specify the interface for the entry.
- ► **Receive RIP Version:** Specify receiving RIP version for the entry.
- ► **Send RIP Version:** Specify sending RIP version for the entry.
- ► **Authorization Enable:** Check the box to enable authorization.
- ► **Key Mode:** Specify the encryption mode of key, **TEXT**(plaintext),**MD5**(cipertext).
- ► **Key Type:** Specify the key from **Simple String** or **Key Chain**.
- ► **Simple String:** If select Simple String in item of Key Type, enter simple string as key.

1.2.7.3.2 Key Chain

The command “set rip key-chain” configures the RIP key chain as below.

```
BG9002N#set rip key-chain
Current Key-Chain Name:12345
Want to Modify Key Chain Name? 'yes' or 'no'[no]n

Key List of Key-Chain:
  +----+------+---------------+
  | No |Key ID|Key-String     |
  +----+------+---------------+
  |0   |3     |12345          |
  +----+------+---------------+
Sure to Config Key List of the Key-Chain?  'yes' or 'no'[no]: y
Key List Config of Key-Chain:
->Select config type(0-add,1-del,2-modify)[0]:
->Key ID: 1
->Key String: qwer
->Continue to Add Key to Key Chain? 'yes' or 'no'[no]: n

BG9002N#
```

```
BG9002N#set rip key-chain
Current Key-Chain Name:12345
Want to Modify Key Chain Name? 'yes' or 'no'[no]

Key List of Key-Chain:
  +----+------+----------------+
  | No |Key ID|Key-String      |
  +----+------+----------------+
  |0   |3     |12345           |
  +----+------+----------------+
  |1   |1     |qwer            |
  +----+------+----------------+
Sure to Config Key List of the Key-Chain?  'yes' or 'no'[no]: y
Key List Config of Key-Chain:
->Select config type(0-add,1-del,2-modify)[0]: 2
->Please input index to modify(0-1)[0]: 1
->Key ID[1]: 2
->Key String[qwer]:
->Really want to modify? 'yes' or 'no'[no]: y
  The configuration will take effect after saved and reloaded!
```

```
BG9002N#set rip key-chain
Current Key-Chain Name:12345
Want to Modify Key Chain Name? 'yes' or 'no'[no]

Key List of Key-Chain:
  +----+------+----------------+
  | No |Key ID|Key-String      |
  +----+------+----------------+
  |0   |3     |12345           |
  +----+------+----------------+
  |1   |2     |qwer            |
  +----+------+----------------+
Sure to Config Key List of the Key-Chain?  'yes' or 'no'[no]: y
Key List Config of Key-Chain:
->Select config type(0-add,1-del,2-modify)[0]: 1
->Please input begin index(0-1)[0]: 1
->Please input end index(0-1)[0]: 1
  Delete success

BG9002N#
```

Figure 1-81 Configure RIP Key Chain

The following items are displayed on this screen:

► **Key Chain Name:** Enter the name of key chain.

► **Key ID:** Enter the ID of the entry.

► **Key String:** Enter the Key of the entry.

1.2.8 Advanced Parameters

1.2.8.1 UPnP Parameter

The command “show upnp” shows the UPnP information as below:

```
BG9002N#show upnp

 Enable Upnp.....................................: Enable
 Upstream Interface..............................: VLAN1
 Downstream Interface............................: STB

BG9002N#
```

Figure 1-82 Show UPnP Information

The command “set upnp” configures the UPnP parameters as below.

```
BG9002N#set upnp
->Enable Upnp 'yes' or 'no' [yes]:
->Upstream Interface([0]DATA [5]VLAN1)[5]:0
->Downstream Interface([5]VLAN1 [21]STB)[21]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 1-83 Configure UPnP Parameters

The following items are displayed on this screen:

► **Enable UPnP:** Enable or disable the UPnP function globally.

► **Upstream Interface:** The network interface connected to the DLNA server.

► **Downstream Interface:** The network interface connected to the DLNA client.

1.2.9 Multicast

The command “show multicast” shows the multicast information as below:

```
BG9002N#show multicast

 Enable IGMP proxy...............................: Enable

BG9002N#
```

Figure 1-84 Show Multicast Information

The command “set multicast” configures the multicast parameters as below.

```
BG9002N#set multicast
->Enable IGMP proxy? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#_
```

Figure 1-85 Configure Multicast Parameters

The following items are displayed on this screen:

► **Enable IGMP Proxy:** Enable or disable the IGMP proxy function globally. Currently, IGMP proxy is mainly used for IPTV.

1.3 VOIP Service

1.3.1 SIP Service

The command “show sip” shows the sip service information as bellow:

```
BG9002N#show sip
+-----------------------------------------------------------------------------+
|No. | ID |    Register Server |   Server IP/Domain    | Port |Register Cycle |
+----+----+--------------------+-----------------------+------+---------------+
|  0 |  1 |         RegServer1 |      192.168.100.124 | 5060 |          1200 |
+-----------------------------------------------------------------------------+

 Enable backup server or not.....................:yes
 Backup Register server IP or domain.............:192.168.100.106
 Backup Register server port.....................:5060
 Enable proxy server or not......................:yes
 Proxy server domain name or IP..................:192.168.100.123
 Proxy server port...............................:5060
 Enable backup agent register or not.............:yes
 Back agent register server ip or domain.........:192.168.100.122
 Back agent Register server port.................:5060
 RTP Port........................................:1024-65535
 Local SIP Port(1024-65535)......................:5060

BG9002N#
```

Figure 1-86 Show Sip Server Information

Execute the command “set sip” to set the sip information as below:

```
BG9002N#set sip
+-----------------------------------------------------------------------------+
|No. | ID |    Register Server |   Server IP/Domain    | Port |Register Cycle |
+----+----+--------------------+-----------------------+------+---------------+
|  0 |  1 |         RegServer1 |      192.168.100.124  | 5060 |          1200 |
+-----------------------------------------------------------------------------+
->Input register server name[RegServer1]:
->Register server ip or domain[192.168.100.124]:
->Register server port(1024-65535)[5060]:
->Enable backup server or not[yes]:
->Backup Register server IP or domain(Enter SPACE key to clear)[192.168.100.106]
:
->Backup Register server port(1024-65535)[5060]:
->Enable proxy server or not[yes]:n
->Enable backup proxy register or not[yes]:
->Backup proxy register server ip or domain[192.168.100.122]:
->Backup proxy Register server port(1024-65535)[5060]:
->Register interval(60-3600s)[1200]:
->Rtp begin Port(1024-65535)[1024]:
->Rtp end Port(1024-65535)[65535]:
->Local SIP Port(1024-65535)[5060]:
->Really want to modify? 'yes' or 'no'[yes]:

  Operate success!

  The configuration will take effect after saved and reloaded!
```

Figure 1-87 Configure Sip Server

At first, the command will show the sip server information, and then begin to configure sip server.

The following items are displayed on this screen:

► **Register server ip or domain:** Domain or IP of SIP server.

► **Register Server Port:** Listening port of SIP server.

► **Enable Backup Server or not:** Enable or disable backup SIP server.

► **Backup Server IP or Domain:** Domain or IP of backup SIP server.

► **Backup Register Server Port:** Listening port of backup SIP server.

► **Enable Proxy Server or not:** Enable or disable Proxy server.

► **Proxy Server domain name or IP:** Domain or IP of proxy server.

► **Proxy Server Port:** Listening port of proxy server.

► **Enable Backup Proxy register or not:** Enable or disable backup proxy server.

► **Backup Proxy Register Server ip or domain:** Domain or IP of backup proxy server.

► **Backup Proxy Register Server Port:** Listening port of backup proxy server.

► **Register Interval:** Enter the desired time interval at which the sip UA will send register message.

► **RTP begin:** Local RTP port range begin.

► **RTP end:** Local RTP port range end.

► **Local SIP Port:** Local listening port.

The command “show sipadvance” shows the advanced SIP information as below:

```
BG9002N#show sipadvance

 SBC enable or not.................................:no
 Enable Keeping Alive..............................:yes
 Alive Time(20-3600s)..............................:500
 Keep Alve Mode....................................:OPTIONS
 Enable Realm......................................:yes
 Realm PIN.........................................:
 Enable Session ...................................:yes
 Conversation Refresh Interval(90-3800s).........:90
 Conversation Refresh Preference..................:UAS
 Enable Sip Retrans Timer..........................:yes
 Retrans Interval..................................:200
 Retrans Times.....................................:3
 User Agent........................................:usersec
 SDP Mode When Call holding.......................:Send-Only
 Enable NextNonce..................................:yes
 Max Value of NextNonce............................:9
 Support PRACK or not..............................:yes
 Support USER-PHONE or not.........................:yes
 Auto Update Register Cycle or not.................:yes
 Support Full Register or not......................:yes
 First Package with Information....................:yes
 SDP with Audio when T38 Faxing....................:no
 Tos/DiffServ settings.............................:DiffServ(Dscp)
 Signaling Precedence..............................:0
 Voice Precedence..................................:0
 Enable Call In Black&White........................:Black User List
 Enable Call Out Black&White.......................:Black User List
BG9002N#
```

Figure 1-88 Show Adavance Sip Information

The command “set sipadvance” configures the advanced SIP information as below:

```
BG9002N#set sipadvance
->SBC enable or not[no]:
->Enable Keeping Alive[yes]:
->Alive Time(20-3600s)[500]:
->Keep Alve Mode(0-CLRF,1-OPTIONS,2-PING)[1]:
->Enable Realm[yes]:
->Realm PIN[]:
->Enable Session [yes]:
->Conversation Refresh Interval(90-3800s)[90]:
->Conversation Refresh Preference(0-UAC,1-UAS)[1]:
->Enable Sip Retrans Timer[yes]:
->Retrans Interval(1-360s)[200]:
->User Agent[usersec]:
->SDP Mode When Call holding(0-0.0.0.0,1-Send-Only)[1]:
->Enable NextNonce[yes]:
->Max Value of NextNonce(1-65535)[9]:8
->Tos/DiffServ settings(0-Tos Ip Presedence,1-DiffServ(Dscp))[1]:
->Signaling Precedence(0-7)[0]:
->Voice Precedence(0-7)[0]:
->Support PRACK or not[yes]:
->Support USER-PHONE or not[yes]:
->Auto Update Register Cycle or not[yes]:
->Support Full Register or not[yes]:
->First Package with Information[yes]:
->SDP with Audio when T38 Faxing[no]:
->Enable Call In Black&White(0-Black User List,1-White User List)[0]:
->Enable Call Out Black&White(0-Black User List,1-White User List)[0]:
->Really want to modify? 'yes' or 'no'[yes]:

  The configuration will take effect after saved and reloaded!
```

Figure 1-89 Configure Advance Sip Parameter

The following items are displayed on this screen:

- ► **Enable Keeping Alive:** After successful registration, whether to send keep-alive packets.
- ► **Keep Alive Mode:** Keep alive mode: **CLRF**, **OPTIONS** or **PING**.
- ► **Enable Realm:** Check the box to enable SIP signaling packets with realm field information.
- ► **Enable Session:** Enable or disable UAC / UAS session refresh mode.
- ► **Enable SIP Retrans Timer:** When registration fails, whether to initiate retransmission, retransmission cycle and time with configuration.
- ► **User Agent:** Check the box to enable signaling packets with **User Agent** field.
- ► **SDP Mode When Call holding:** Select the SIP signal format of call hold.
- ► **Enable Next Nonce:** Enable SIP packets with nonce count field information, incremented each one and with a maximum value.
- ► **Support PRACK or not:** Enable or disable provisional response. If enabled, 1xx (except 100rel) messages are required to respond with ACK.
- ► **Support User-Phone or not:** Whether SIP signaling packets with User = Phone field information.
- ► **Auto Update Register Cycle:** Based on server response to update registration period.
- ► **Support Full Register or not:** Each registration packets are generated, rather than re-issued.
- ► **First Package With Infomation:** The first registration packet with authentication information.
- ► **SDP With Audio When T38 Faxing:** T38 fax signaling packet with audio information.

1.3.2 User

1.3.2.1 User

The command “show sipuser” shows the sip user parameters as below:

```
BG9002N#show sipuser
+-------------------------------------------------------------------------------+
|No. | ID  |Account Name | Extension  |Register Account|Register| Authen User|
+----+-----+-------------+------------+----------------+--------+------------+
|  0 |   1 |    Phone_001|         700|          phone1|     no |   phonetest|
+----+-----+-------------+------------+----------------+--------+------------+
|  1 |   2 |    Phone_002|         701|           ghjfh|     no |            |
+-------------------------------------------------------------------------------+

->Enter the index to show(0-1)[0]:
 Register State.....................................:Unregister
 Phone Number.......................................:700
 Register Account...................................:phone1
 Auth User Name.....................................:phonetest
 Password...........................................:******
 Enable Register....................................:no

->See detail information continue or not?[yes]:n

BG9002N#
```

Figure 1-90 Show sip user Parameter

The command “set sipuser” configures the sip parameter as below:

```
BG9002N#set sipuser
+-------------------------------------------------------------------------------+
|No. | ID  |Account Name | Extension  |Register Account|Register| Authen User|
+----+-----+-------------+------------+----------------+--------+------------+
|  0 |   1 |    Phone_001|         700|          phone1|     no |   phonetest|
+----+-----+-------------+------------+----------------+--------+------------+
|  1 |   2 |    Phone_002|         701|           ghjfh|     no |            |
+-------------------------------------------------------------------------------+
->Enter the index to modify(0-1)[0]:
->Phone number[700]:
->Register Account[phone1]:
->Auth User Name[phonetest]:phoneauth
->Password[******]:
->Enable Register(yes/no)[no]:
->Really want to modify? 'yes' or 'no'[yes]:

  Operate success!

  The configuration will take effect after saved and reloaded!
```

Figure 1-91 Configure sip user Parameter

The following items are displayed on this screen:

- ► **Register Account:** Account name registered to SIP server.
- ► **Auth Username:** Username of the account.
- ► **Password:** Password of the account.
- ► **Phone number:** Caller and called number of subscriber line.

► **Enable Register:** Enable registering.

1.3.2.2 Wildcard Group

The command “show groupregister” show wildcard group as below:

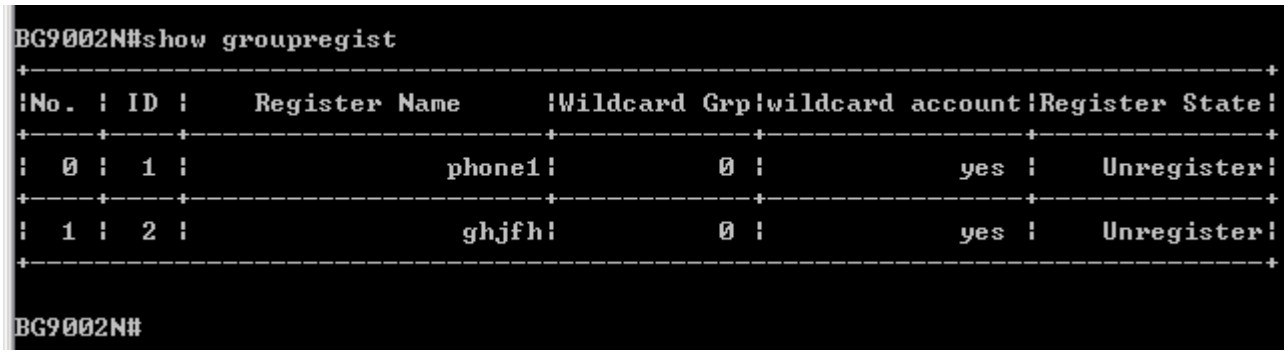


Figure 1-92 Show Wildcard Group Parameter

The command “set groupregister” sets wildcard group as below:

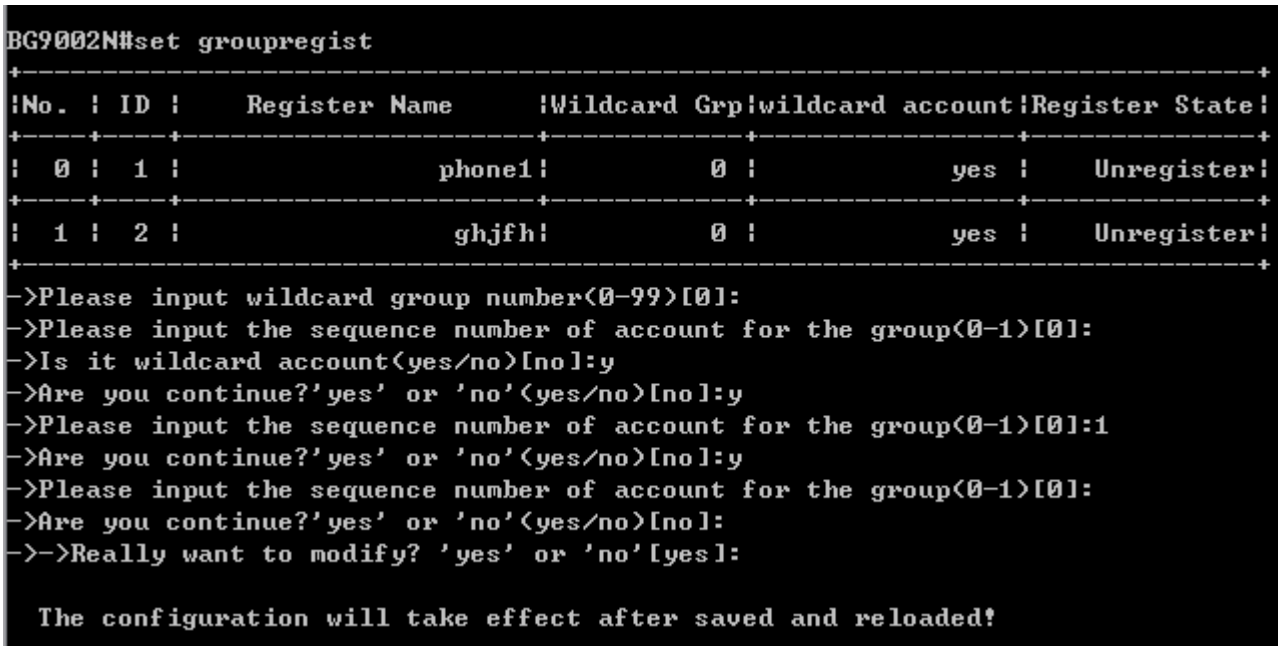


Figure 1-93 Configure Wildcard Group Parameter

1.3.3 Supplementary

The command “show extended-server” shows user supplementary as below:

```
BG9002N#show extended-service

 Min Flash Detect Time(50-750).....................:90 ms
 Max Flash Detect Time.............................:500 ms
 Switch&Release Call...............................:Flash+1
 Enable flash key or not...........................:yes
 Reject key........................................:Flash+0
 Switch call key...................................:Flash+2
 Three Party Call..................................:Flash+3
 Keep the hold call when onhook or not............:no
 # is quick dial key or not.......................:no
 Adterisk to be the function key or not..........:no
 Tap Report........................................:no
 Escape Seq........................................:no
 CID Enable........................................:yes
 Enable Callee Inverse Polarity....................:no
 Enable Caller Inverse Polarity....................:no
+-------------------------------------------------------------------+
|No. | ID  |     Account Name        | Extension  |Extention Type|
+----+-----+-------------------------+------------+--------------+
|  0 |   1 |              Phone_001  |         700| Intern/Extern|
+----+-----+-------------------------+------------+--------------+
|  1 |   2 |              Phone_002  |         701| Intern/Extern|
+-------------------------------------------------------------------+
->Enter the index to show(0-1)[0]:

 Call Forwarding Unconditional....................:no
 Call Forwarding When No Reply....................:yes
 Transfer Call Number.............................:701
 Wait Time Long...................................:0s
 Call Forwarding On Busy..........................:no
 Phone Number.....................................:
 Set to Instant Hotline...........................:no
 Delay Time.......................................:0s
 CID Restriction..................................:no
 Enable No Disturb................................:no
 Enable Call Waiting..............................:yes
 CID Enable.......................................:yes
 CID Mode.........................................:FSK
 Enable MWI.......................................:yes
->Show account extended srvice para continue or not?[yes]:n
```

Figure 1-94 Show User Supplementary

The command “set extended-server” configures the user supplementary parameter as below:

```
BG9002N#set extended-service

->Min Flash Detect Time(50-750)[90 ms]:80
->Max Flash Detect Time(80-1200)[500 ms]:400
->Switch&Release Call:Flash+(1-9)[1]:
->Enable flash key or not(yes/no)[yes]:
->Reject key:Flash+(0-9)[0]:
->Switch call key:Flash+(0-9)[2]:
->Three Party Call:Flash+(1-9)[3]:
->Keep the hold call when onhook or not[no]:
->Adterisk to be the function key or not[no]:
->Tap Report[no]:
->Escape Seq[no]:
->CID Enable[yes]:
->Enable Callee Inverse Polarity[no]:
->Enable Caller Inverse Polarity[no]:
+-----------------------------------------------------------------------------+
|No. | ID  |Account Name | Extension  |Register Account|Register| Authen User|
+----+-----+-------------+------------+----------------+--------+------------+
|  0 |   1 |    Phone_001|         700|          phone1|     no |   phoneauth|
+----+-----+-------------+------------+----------------+--------+------------+
|  1 |   2 |    Phone_002|         701|           ghjfh|     no |            |
+-----------------------------------------------------------------------------+

->Enter the index to modify(0-1)[0]:
->Call Forwarding Unconditional(yes/no)[no]:
->Call Forwarding When No Reply(yes/no)[yes]:
->Transfer Call Number[701]:
->Wait Time Long(1-120)[0]:
->Call Forwarding On Busy(yes/no)[no]:
->Phone Number[]:
->Set to Instant Hotline(yes/no)[no]:
->Delay Time(0-10s)[0]:
->CID Restriction(yes/no)[no]:
->Enable Call Waiting(yes/no)[yes]:
->CID Enable[yes]:
->CID Enable(0-FSK,2-FXS+TYPE II)[0]:
->Enable MWI(yes/no)[yes]:
->Really want to modify? 'yes' or 'no'[yes]:

  The configuration will take effect after saved and reloaded!
```

Figure 1-95 Configure User Supplementary

The following items are displayed on this screen:

- ► **Min Flash Detect Time:** The minimum time to detect the flash.
- ► **Max Flash Detect Time:** The maximum time to detect the flash.
- ► **Flash Key Enable:** Whether to enable digit detect after flash.
- ► **Switch&Release Call:** If the digit specified is detected after flash, terminate the active call and recover the call on hold.
- ► **Three Party Call:** If the digit specified is detected after flash, enter the conference mode.
- ► **Reject Key:** If the digit specified is detected after flash, reject the call on hold.
- ► **Switch Call Key:** If the digit specified is detected after flash, hold the active call and recover the call on hold.
- ► **Keep the hold call when onhook:** If selected, when hanging up in this context, the telephone rings

to notify the user there is still a call on hold.

► **(#)Quick Dial Key:** Whether to send telephone number immediately after receiving the # key.

► **Asterisk Func Key:** Whether to use the '*' key as flash key.

► **Tap Report:** Whether to report an event to server when flash detected.

► **Escape Seq:** Whether to use an escape characters when sending special DTMF.

► **CID Enable:** Whether to enable caller id globally.

► **Callee Inverse Polarity:** Whether to activate the Polarity Reversal for FXS callee.

► **Caller Inverse Polarity:** Whether to activate the Polarity Reversal for FXS caller.

► **Call Forwarding Unconditional:** Enable or disable CFU function, if enabled, enter **Call Number**.

1) Set by keypad service system: ***57*TN#**, TN is the phone number to be redirected to.

2) Cancel by keypad service system: **#57#**.

► **Call Forwarding No Reply:** Enable or disable CFNR, if enabled, enter **Call Number** and **Wait Time Long**.

1) Set by keypad service system: ***41*TN#**, TN is the phone number to be redirected to.

2) Cancel by keypad service system: **#41#**.

► **Call Forwarding On Busy:** Enable or disable CFB function, if enabled, enter **Call Number**.

1) Set by keypad service system: ***40*TN#**, TN is the phone number to be redirected to.

2) Cancel by keypad service system: **#40#**.

► **Hotline Number:** Enter number to hotline function, empty expressed disable.

1) Set **delay hotline** number by Keypad service system: ***52*TN#**, TN is the hotline number.

2) Cancel **delay hotline** number by Keypad service system: **#52#**.

3) Set **instant hotline** number by Keypad service system: ***42*TN#**, TN is the hotline number.

4) Cancel **instant hotline** number by Keypad service system: **#42*EN#**, instant hotline can only be deactivated with other extension; EN is the extension number which needs to deactivate instant hotline.

► **Delay Time:** Time 0 indicates immediate Hotline, Otherwise, indicates delay Hotline. The Delay Time must be configured on the WEB.

► **CID Restriction:** Enable or disable CID Restriction. If **Anonymous As UserName** is chosen, user name content is Anonymous also.

► **Enable No Disturb:** Allows block incoming calls at any time.

► **Enable Call Waiting:** When you talking, a third party phone comes in, you can hear the beep tone.

► **Enable MWI:** Enable or disable MWI (Message-waiting indicator) function.

► **Enable CID:** Enable or disable to send CID to phone.

► **CID Mode:** There are two methods used for sending caller ID information depending on the application and country specific requirements:

FSK: caller ID generation using Frequency Shift Keying (FSK)

DTMF: caller ID generation using DTMF signaling.

The command "show abbr-dial" shows the abbreviated number of the user as below:

```
BG9002N#show abbr-dial
+-----------------------------------------------------------------------------+
|No. | ID  |Account Name | Extension  |Register Account|Register| Authen User|
+----+-----+-------------+------------+----------------+--------+------------+
|  0 |   1 |    Phone_001|         700|          phone1|    yes |   phoneauth|
+----+-----+-------------+------------+----------------+--------+------------+
|  1 |   2 |    Phone_002|         701|           ghjfh|     no |            |
+-----------------------------------------------------------------------------+

->Enter the index to show(0-1)[0]:
+-------------------------------------------------+
|No. | ID |     Phone Number     |Abbreviated Number|
+----+----+----------------------+------------------+
|  0 |  1 |                 1112 |               10 |
+----+----+----------------------+------------------+
|  2 |  3 |                 3445 |               34 |
+----+----+----------------------+------------------+
|  3 |  4 |                 8493 |               84 |
+-------------------------------------------------+
```

Figure 1-96 Show Abbreviated Number

The command “set abbr-dial” sets the abbreviated number of the user as below:

```
BG9002N#set abbr-dial
+-----------------------------------------------------------------------------+
|No. | ID  |Account Name | Extension  |Register Account|Register| Authen User|
+----+-----+-------------+------------+----------------+--------+------------+
|  0 |   1 |    Phone_001|         700|          phone1|     no |   phoneauth|
+----+-----+-------------+------------+----------------+--------+------------+
|  1 |   2 |    Phone_002|         701|           ghjfh|     no |            |
+-----------------------------------------------------------------------------+

->Enter the index to modify(0-1)[0]:
+-------------------------------------------------+
|No. | ID |     Phone Number     |Abbreviated Number|
+----+----+----------------------+------------------+
|  0 |  1 |                 1112 |               10 |
+----+----+----------------------+------------------+
|  2 |  3 |                 3445 |               34 |
+----+----+----------------------+------------------+
|  3 |  4 |                 8493 |               84 |
+-------------------------------------------------+

->0-add,1-delete,2-modify[0]:
->Phone Number[]:23534534
->Abbreviated Number[]:23
->Really want to modify? 'yes' or 'no'[yes]:

  Operate success!

  The configuration will take effect after saved and reloaded!
```

Figure 1-97 Configure Abbreviated Number

The following items are displayed on this screen:

►**0-add,1-delete,2-modify**: Input “0” to add new abbreviated number item, input “1” to delete a abbreviated numbe from thelist, input “2” to modify one of the abbreviated

numbe from the list.

► **Abbreviated Number:** The abbreviated number.
► **Phone Number:** The Actual phone number.

The command “show whiteblack-list” shows the white list and the black list of the user as below:

```
BG9002N#show whiteblack-list
+-------------------------------------------------------------------+
|No. | ID  |     Account Name        | Extension  |Extention Type|
+----+-----+-------------------------+------------+--------------+
|  0 |   1 |              Phone_001  |         700| Intern/Extern|
+----+-----+-------------------------+------------+--------------+
|  1 |   2 |              Phone_002  |         701| Intern/Extern|
+-------------------------------------------------------------------+
->Enter the index to show(0-1)[0]:
+-----------------------------------------------+
|No. | ID |   List Type         | Phone Number   |
+----+----+---------------------+----------------+
|  0 |  1 |  Call In Black List|            1134|
+----+----+---------------------+----------------+
|  1 |  2 |  Call In Black List|            6678|
+----+----+---------------------+----------------+
|  6 |  7 |  Call In Black List|          566874|
+----+----+---------------------+----------------+
|  7 |  8 |  Call In Black List|            5566|
+-----------------------------------------------+

->Show account white or black list para continue or not?[yes]:n
```

Figure 1-98 Show White & Black List

The command “set whiteblack-list” configures the white list and the black list of the user as below:

```
BG9002N#set whiteblack-list
+-----------------------------------------------------------------------------+
|No. | ID  |Account Name | Extension  |Register Account|Register| Authen User|
+----+-----+-------------+------------+----------------+--------+------------+
|  0 |   1 |    Phone_001|         700|          phone1|    yes |   phoneauth|
+----+-----+-------------+------------+----------------+--------+------------+
|  1 |   2 |    Phone_002|         701|           ghjfh|     no |            |
+-----------------------------------------------------------------------------+

->Enter the index to modify(0-1)[0]:
+-----------------------------------------------+
|No. | ID |   List Type         | Phone Number   |
+----+----+---------------------+----------------+
|  0 |  1 |  Call In Black List|            1134|
+----+----+---------------------+----------------+
|  1 |  2 |  Call In Black List|            6678|
+----+----+---------------------+----------------+
|  6 |  7 |  Call In Black List|          566874|
+----+----+---------------------+----------------+
|  7 |  8 |  Call In Black List|            5566|
+-----------------------------------------------+
->0-add,1-delete,2-modify[0]:
->List Type(
 0-Call In Black List
 1-Call In White List
 2-Call Out Black List
 3-Call Out White List)[0]:2
->Phone Number[]:453656
->->Really want to modify? 'yes' or 'no'[yes]:

  Operate success!

  The configuration will take effect after saved and reloaded!

->Set account white or black list para continue or not?[yes]:
```

Figure 1-99 Configure White & Black List

The following items are displayed on this screen:

► **List Type:** Choose type of Black&White List, four types are provided:
Incoming Blacklist, Incoming Whitelist, Outgoing Blacklist, Outgoing Whitelist.

► **Phone Number:** the phone number or sip account.

1.3.4 Codec Parameters

The command “show codec” shows the codec parameters as below:

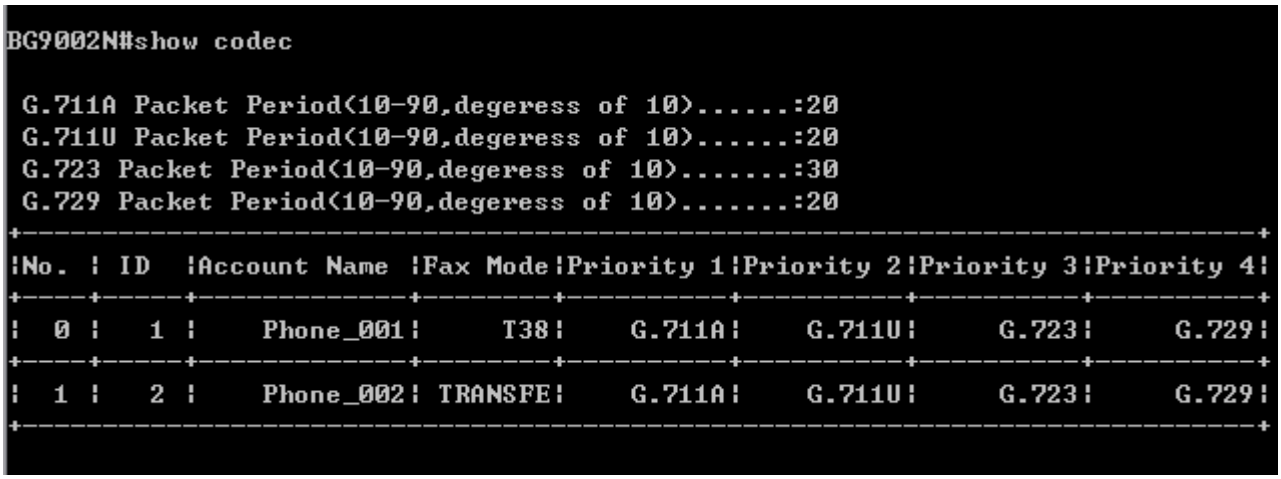


Figure 1-100 Show Codec Parameters

The command “set codec” configures the codec parameters as below:

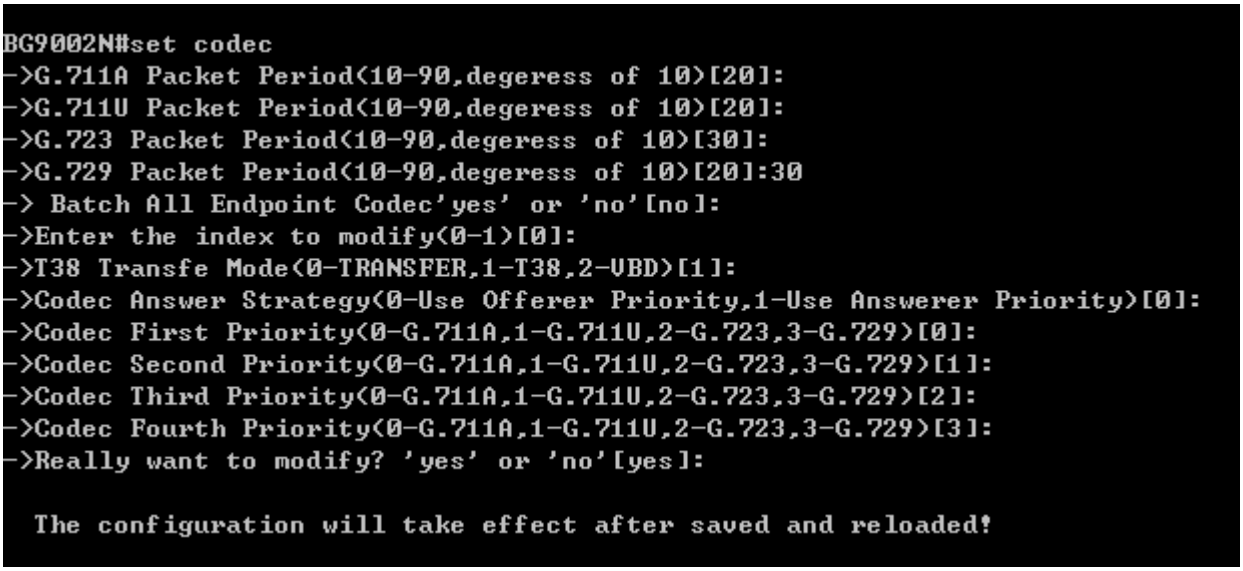


Figure 1-101 Configure Codec Parameters

► **G.711A Packet Period:** RTP packetization period of G.711A codec.

► **G.711u Packet Period:** RTP packetization period of G.711U codec.

► **G.723 Packet Period:** RTP packetization period of G.723 codec.

► **G.729 Packet Period:** RTP packetization period of G.729 codec.

► **Fax Mode:** Choose fax mode, three types are provided: **Transparent, T38, VBD.**

► **Codec Answer Strategy:** Two modes are provided:

Use Answerer Priority: Codec selection decisions based on the priority level configuration

Use Offerer Priority: Codec selection decision based on caller’s priority.

► **Codec Priority:** If **Use Answerer Priority** is selected, set the priority of codec.

1.3.5 DSP Parameters

The command “show dsp” shows DSP information as below:

```
BG9002N#show dsp

 Echo Clear up or not.............................:no
 Silence Compress.................................:no
 Input Gain(-10-12db).............................:0
 Ouput Gain(-10-12db).............................:0
 Delay Level......................................:delay large
 DTMF Transfer Model..............................:RFC2833
 T38 Max FAX Rate.................................:Unlimited
 T38 FAX Signaling Reduncancy(0-7)................:4
 T38 FAX Data Redundancy(0-3).....................:0
 Ring Frequency...................................:25HZ
 Impedance........................................:600 Ohm
BG9002N#_
```

Figure 1-102 Show DSP Parameter

The command “set dsp” configures DSP parameters as below:

```
BG9002N#set dsp

->Echo Clear up or not[no]:
->Silence Compress[no]:y
->Input Gain(-10-12db)[0]:
->Ouput Gain(-10-12db)[0]:
 Delay Level:
 0-delay mininum
 1-delay smaller
 2-delay moderate
 3-delay large
 4-delay Maxinum
->Delay Level(0-4)[3]:
->DTMF Transfer Model(0-info,1-In-band,2-RFC2833)[0]:
 T38 Max FAX Rate:
 0-Unlimited
 1-2400bps
 2-4800bps
 3-7200bps
 4-9600bps
 5-12000bps
 6-14400bps
->T38 Max FAX Rate(0-6)[0]:
->T38 FAX Signaling Reduncancy(0-7)[4]:
->T38 FAX Data Redundancy(0-3)[0]:
->Ring Frequency(0-20HZ,1-25HZ)[1]:
->Impedance(0-600 Ohm,1-Ternary,2-Switzerland standard)[0]:1
->Really want to modify? 'yes' or 'no'[yes]:

  The configuration will take effect after saved and reloaded!
```

Figure 1-103 Configure DSP Parameters

The following items are displayed on this screen:

- ► **Echo Cancellation:** Enable or disable echo cancellation.
- ► **Silence Detection/Suppression:** Enable or disable silence detection and silence suppression.
- ► **Input Gain:** Configure the input gain value.
- ► **Output Gain:** Configure the input gain value
- ► **Delay Level:** Choose the delay level, five levels are provided: **Minimum,**

Smaller, Moderate, Larger, Maximum.

► **DTMF Transfer Model:** Select DTMF transmission mode**: In-Band, INFO, RFC2833**.

► **RFC2833 Load Type:** If RFC2833 is selected, specify payload type of RFC2833.

► **T38 Max FAX Rate:** Select the maximum rate, when using T38 fax mode: **Unlimited, 2400bps, 4800bps, 7200bps, 9600bps, 12000bps, 14400bps**.

► **T38 Signaling Redundancy:** Configure the redundancy of T38 signal.

► **T38 Data Redundancy:** Configure the redundancy of T38 data.

► **Ring Frequency:** Choose the ring frequency: **20Hz, 25Hz**.

► **Impedance Type:** Choose the impedance type: **600Ω, China Standard, Switzerland Standard**.

1.3.6 Digitmap

The command “show digitmap” shows digitmap information as below:

```
BG9002N#show digitmap

 Enable Digitmap.....................................:no
 Digitmap Short Timer S(1-30).......................:5s
 Digit Map Content...................................:xxxxxxx
BG9002N#
```

Figure 1-104 Show Digit Map Parameter

The command “set digitmap” configures digitmap parameters as below:

```
BG9002N#set digitmap

->Enable Digitmap[no]:
->Digitmap Short Timer S(1-30)[5s]:
->Digit Map Content[xxxxxxx]:
->Really want to modify? 'yes' or 'no'[yes]:

  The configuration will take effect after saved and reloaded!
```

Figure 1-105 Configure Digit Map Parameter

► **Enable:** Enable or disable digit map function.

► **Short Timer:** The time of Short Timer in second.

► **Digit Map:** The digit map rules.

1.3.7 Signal Tone

The command “show tone” shows signal tone information as below:

```
BG9002N#show tone

 Tone Type.....................................:China
 Dial Tone User Define Enable..................:no
 Dial tone frequency 1(100-2000HZ).............:0
 Dial tone frequency 2(100-2000HZ).............:0
 Busy Tone User Define Enable..................:no
 Busy Tone Frequency1(100-2000HZ)..............:0
 Busy Tone Frequency2(100-2000HZ)..............:0
 On Time(100-10000ms)..........................:500
 Off Time(100-10000ms).........................:500
 Ring Back Tone User Define Enable.............:yes
 Ring Back Tone Frequency 1(100-2000HZ)........:400
 Ring Back Tone Frequency 2(100-2000HZ)........:500
 On Time(100-10000ms)..........................:500
 Off Time(100-10000ms).........................:500
 Internal ring on time1(*100ms)................:10
 Internal ring off time1(*100ms)...............:40
 Internal ring on time2(*100ms)................:0
 Internal ring off time2(*100ms)...............:0
 External ring on time1(*100ms)................:10
 External ring off time1(*100ms)...............:40
 External ring on time2(*100ms)................:0
 External ring off time2(*100ms)...............:0
BG9002N#
```

Figure 1-106 Show Signal Tone Parameter

The command “set tone” configures signa l tone parameters as below:

```
BG9002N#set tone

 0----China
 1----Chile
 2----Peru
 3----America
 4----Mexico
 5----Telmex_Columbia
 6----Switzerland
 7----Other
->Tone Type(0-7)[0]:
->Dial Tone User Define Enable[no]:
->Dial tone frequency 1(100-2000HZ)[0]:
->Dial tone frequency 2(100-2000HZ)[0]:
->Busy Tone User Define Enable[no]:
->Busy Tone Frequency1(100-2000HZ)[0]:
->Busy Tone Frequency2(100-2000HZ)[0]:
->On Time(100-10000ms)[500]:
->Off Time(100-10000ms)[500]:
->Ring Back Tone User Define Enable[yes]:
->Ring Back Tone Frequency 1(100-2000HZ)[400]:
->Ring Back Tone Frequency 2(100-2000HZ)[500]:
->On Time(100-10000ms)[500]:
->Off Time(100-10000ms)[500]:
->Internal ring on time1(1-100)(*100ms)[10]:
->Internal ring off time1(1-100)(*100ms)[40]:
->Internal ring on time2(1-100)(*100ms)[0]:
->Internal ring off time2(1-100)(*100ms)[0]:
->External ring on time1(1-100)(*100ms)[10]:
->External ring off time1(1-100)(*100ms)[40]:
->External ring on time2(1-100)(*100ms)[0]:
->External ring off time2(1-100)(*100ms)[0]:
->Really want to modify? 'yes' or 'no'[yes]:

  The configuration will take effect after saved and reloaded!
```

Figure 1-107 Configure Signal Tone Parameter

The following items are displayed on this screen:

► **Tone Type:** Select the type of signal tone.

Dial Tone

► **User Define Enable:** Whether to use user-defined dial tone frequency.

► **Dial Tone Frequency 1:**

► **Dial Tone Frequency 2:**

Busy Tone

► **User Define Enable:** Whether to use user-defined busy tone frequency.

► **Busy Tone Frequency 1:**

► **Busy Tone Frequency 2:**

► **On Time:**

► **Off Time:**

Ring Back Tone

► **User Define Enable:** Whether to use user-defined ringback tone frequency.

► **Ring Back Tone Frequency 1:**
► **Ring Back Tone Frequency 2:**
► **On Time:**
► **Off Time:**

Distinction Ring: Specify the ring cadence for the FXS port. In these fields, you specify the on and off pulses for the ring. The ring cadence that should be configured differs between internal call and external call.

1.3.8 Centrex

The command “show inline” shows centrex information as below:

```
BG9002N#show inline

 Enable Centrex.....................................:yes
+-----------------------------------+
|NO.  | ID |Group |Ring Policy|Time|
+-----+----+------+-----------+----+
|  0  |  1 |   700|  Alternate|30s |
+-----+----+------+-----------+----+
|  1  |  2 |   111|  Alternate|20s |
+-----+----+------+-----------+----+
|  2  |  3 |  4356|  Alternate|20s |
+-----------------------------------+
+---------------------------+
|NO.  |  Group   | Telephone  |
+-----+----------+------------+
|  0  |      700|        4321|
+-----+----------+------------+
|  0  |      700|         700|
+-----+----------+------------+
|  1  |      111|         987|
+-----+----------+------------+
|  2  |     4356|        4545|
+---------------------------+
```

Figure 1-108 Show Centrex Parameter

The command “set inline” configures centrex parameters as below:

```
BG9002N#set inline

->Enable Centrex(yes/no)[yes]:
+--------------------------------+
|NO.  | ID |Group |Ring Policy|Time|
+-----+----+------+-----------+----+
|  0  |  1 |   700|  Alternate|30s |
+-----+----+------+-----------+----+
|  1  |  2 |   111|  Alternate|20s |
+-----+----+------+-----------+----+
|  2  |  3 |  4356|  Alternate|20s |
+--------------------------------+
+---------------------------+
|NO.  |  Group  | Telephone  |
+-----+---------+------------+
|  0  |      700|        4321|
+-----+---------+------------+
|  0  |      700|         700|
+-----+---------+------------+
|  1  |      111|         987|
+-----+---------+------------+
|  2  |     4356|        4545|
+---------------------------+

->Ring Group:0-add,1-delete,2-modify[0]:
->Group Number[]:701
->Ring Policy(0-Alternate,1-Ordinal,2-Parallel)[0]:
->Ring Time(5-90)[20]:
->Really want to modify? 'yes' or 'no'[yes]:
  Operate success!

->Set Group Member or not?[yes]:

->Ring Group Member:0-add,1-delete,2-modify[0]:
->Telephone number[]:353543
->Really want to modify? 'yes' or 'no'[yes]:
  Operate success!

  The configuration will take effect after saved and reloaded!
```

Figure 1-109 Configure Centrex Parameter

The following items are displayed on this screen:

► **Enable Centrex:** Whether to enable centrex function globally.

► **Group Number:** The phone number of this ring group.

► **Ringing Policy:** Phone ringing policy: **Alternate**, **Ordinal**, **Parallel**.

► **Ring Time:** Ring time of each member.

► **Telephone Number:** The number will be added to the ring group.

1.3.9 Phone Book

The command “show callroute” shows telephone book information as below:

```
BG9002N#show callroute
+-----------------------------------------------------------------------+
|No.  |Phone Prefix|Total Length|Prefic Mode|Modify Len|Modify Code|
+-----+------------+------------+-----------+----------+-----------+
|  1  |         112|   Unlimited|     Normal|         0|           |
+-----+------------+------------+-----------+----------+-----------+
|  2  |         435|   Unlimited|     Normal|         0|           |
+-----+------------+------------+-----------+----------+-----------+
+-----------------------------------------------+
|NO.  |    IP/DOMAIN     | Port  |   Description  |
+-----+------------------+-------+----------------+
|  1  |       138.0.60.3| 5060  |      phoneroute|
+-----+------------------+-------+----------------+
|  2  |  192.168.100.124| 5060  |     phoneroute1|
+-----+------------------+-------+----------------+
```

Figure 1-110 Show Phone Book Parameter

The command “set callroute” configures telephone book parameters as below:

```
BG9002N#set callroute
+-----------------------------------------------------------------------+
|No.  |Phone Prefix|Total Length|Prefic Mode|Modify Len|Modify Code|
+-----+------------+------------+-----------+----------+-----------+
|  1  |         112|   Unlimited|     Normal|         0|           |
+-----+------------+------------+-----------+----------+-----------+
|  2  |         435|   Unlimited|     Normal|         0|           |
+-----+------------+------------+-----------+----------+-----------+
+-----------------------------------------------+
|NO.  |    IP/DOMAIN     | Port  |   Description  |
+-----+------------------+-------+----------------+
|  1  |       138.0.60.3| 5060  |      phoneroute|
+-----+------------------+-------+----------------+
|  2  |  192.168.100.124| 5060  |     phoneroute1|
+-----+------------------+-------+----------------+

->Call Route:0-add,1-delete,2-modify[0]:
->Phone Prefix(length can't be zero)[]:56756
->Total Length(0-32,0-unlimited)(0-32)[0]:
->Description(length can't be zero)[]:phoneroute2
->IP/DOMAIN[138.0.60.3]:192.168.100.106
->Input static-iptrunk port(1-65535)[5060]:
->PreFix Mode(0-Normal;1-Delete;2-add;3-modify)[0]:
->Really want to modify? 'yes' or 'no'[yes]:

  Operate success!

  The configuration will take effect after saved and reloaded!
```

Figure 1-111 Configure Phone Book Parameter

The following items are displayed on this screen:

► **Phone Prefix:** The prefix of this phone book.

► **Total Length:** The total length of number to wait before sending.

► **Prefix Mode:** Mode of processing number prefix: **Unmodify**, **Remove**, **Add**, **Modify**.

► **IP/Domain:** The IP address or domain of destination.

► **Port:** The port of destination.

► **Description:** Description of this rule.

1.3.10 Save and Reload VOIP Parameter

VOIP parameter will take effect after save and reload commands:

```
BG9002N#save

  Save operation successful!


BG9002N#reload
Really want to modify? 'yes' or 'no'[yes]:
 Voice parameter reload success!

BG9002N#
```

Figure 1-112 Save and Reload Parameter

1.4 System

1.4.1 Time Management

The command “show time-management” show the time management information as below:

```
BG9002N#show time-management

 Enable NTP.....................................: Enable
 NTP Service Mode...............................: Client
 Primary NTP Server.............................: ntp.ucsd.edu
 Secondory NTP Server...........................: ntp.univ-lyon1.fr
 Time Zone......................................: -2
 Update Interval................................: 3600
DST Config:
 Enable DST.....................................: Enable
 DST Offset(min): 0
 DST Start At 1:00 on First Sunday in Jan.
 DST End At 4:00 on Third Monday in Feb.

BG9002N#_
```

Figure 1-113 Show Time Management Information

The command “set time-management” configure the time management parameters as below.

```
BG9002N#set time-management
->Enable NTP? 'yes' or 'no'[yes]:
->NTP Service Mode(0-Client,1-Server And Client)[0]:
->Primary NTP Server[ntp.ucsd.edu]:
->Secondory NTP Server[ntp.univ-lyon1.fr]:
->Time Zone[1]: -2
->Update Interval(60~36000s)[3600]:
->Enable Daylight Savings Time(DST)? 'yes' or 'no'[yes]:
->DST Offset(0-120min)[0]:
Start Time of DST:
->Month(1~12)[1]:
->Select Weekday:
    0-Sunday   1-Monday  2-Tuesday   3-Wednesday
    4-Thursday 5-Friday  6-Saturday
->Weekday(0~6)[0]:
->Select Order of Weekday in Month:
    1-First in Month   2-Second in Month  3-Third in Month
    4-Fourth in Month  5-Last in Month
->Order of Weekday in Month(1~5)[1]:
->Hour of Day(0~23)[0]: 1
End Time of DST:
->Month(1~12)[1]: 2
->Select Weekday:
    0-Sunday   1-Monday  2-Tuesday   3-Wednesday
    4-Thursday 5-Friday  6-Saturday
->Weekday(0~6)[0]: 1
->Select Order of Weekday in Month:
    1-First in Month   2-Second in Month  3-Third in Month
    4-Fourth in Month  5-Last in Month
->Order of Weekday in Month(1~5)[1]: 3
->Hour of Day(0~23)[0]: 4
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

Figure 1-114 Configure Time Management Parameters

The following items are displayed on this screen:

► **Enable NTP:** Enable or disable NTP.

► **Enable DST:** Enable or disable the Daylight Saving Time(DST).

► **DST Offset:** Enter the offset of DST.

► **Month:** Specify the month of DST, range from 1 to 12 in one year.

► **Weekday :** Specify the weekday of DST, range from Sunday to Saturday.

► **Order of Weekday in Month:** Specify the order of start weekday in the month from pull-down list as following:

- **First in Month**
- **Second in Month**
- **Third in Month**
- **Fourth in Month**
- **Last in Month**

► **Hour of Day:** Specify the start hour of DST, range from 0 to 23 in one day.

1.4.2 Reboot System

Enter command “reset” to reset the device.

1.4.3 Backup/Restore

The command "load config" backup/restore the configurations as blow. Enter 0 to save current parameters as custom default configurations, Enter 1 to reset to custom default parameters, Enter 2 to reset to factory parameters.

```
BG9002N#load config
->Select Load config source(0-Default,1-FileSystem,2-Flash)[0]:
```

Figure 1-115 Backup/Restore Configurations

1.4.4 Diagnostic

1.4.4.1 Ping

The command "ping" can used to check connectivity of your network in the following screen.

```
BG9002N#ping 192.168.100.182
->If Using Interface when ping 'yes' or 'no' [no]:
->Set ping packet size(0-65500)[56]:
->Set ping count(1-86400)[4]:
->If Using mark when ping 'yes' or 'no' [no]:
PING 192.168.100.182 (192.168.100.182): 56 data bytes
64 bytes from 192.168.100.182: seq=0 ttl=64 time=0.860 ms
64 bytes from 192.168.100.182: seq=1 ttl=64 time=1.260 ms
64 bytes from 192.168.100.182: seq=2 ttl=64 time=0.740 ms
64 bytes from 192.168.100.182: seq=3 ttl=64 time=0.740 ms

--- 192.168.100.182 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.740/0.900/1.260 ms

BG9002N#
```

Figure 1-116 PING Diagnostic

► **Ping:** Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.

► **Interface:** By selecting the interface, through this interface to send Echo Request messages.

►**Ping Packet Size:** Specifies the packet size of Echo Request messages sent.

► **Ping Count:** Specifies the number of Echo Request messages sent.

1.4.5 System Log

The command “show syslog” show the system log information as below:

Figure 1-117 Show System Log Information

The command “set syslog” configure the system log parameters as below.

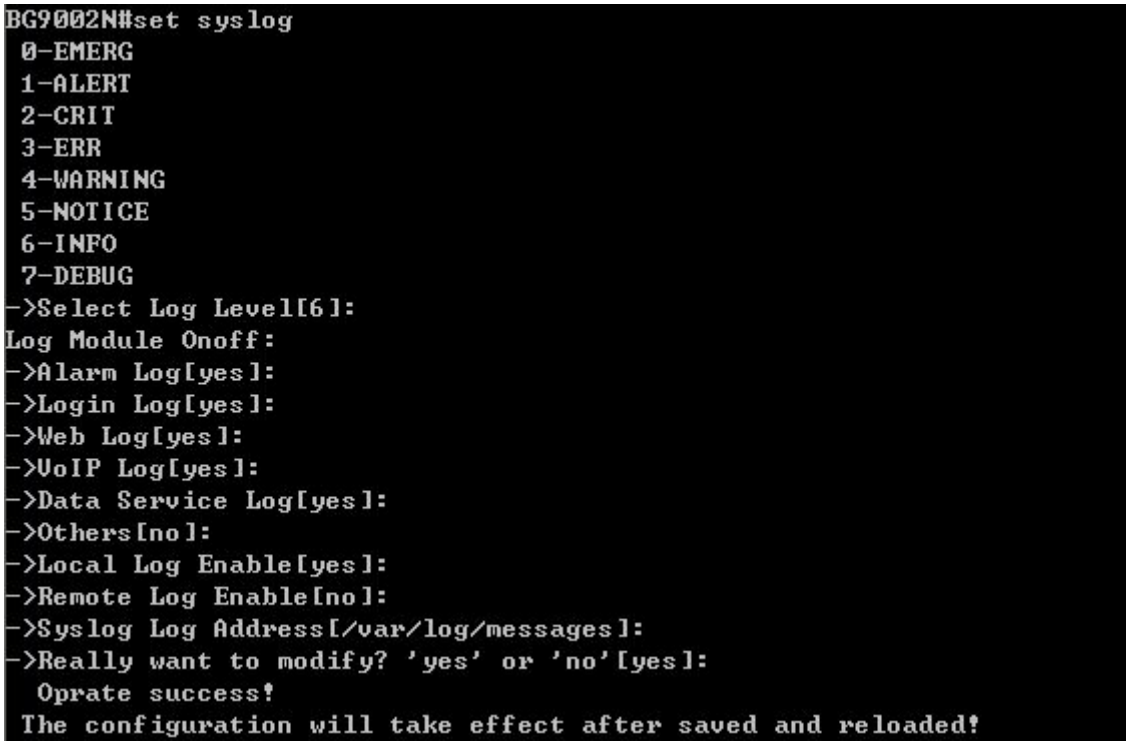


Figure 1-118 Configure System Log Parameters

The following items are displayed on this screen:

1.4.6 TR069

The command “show tr069” show the tr069 information as below:

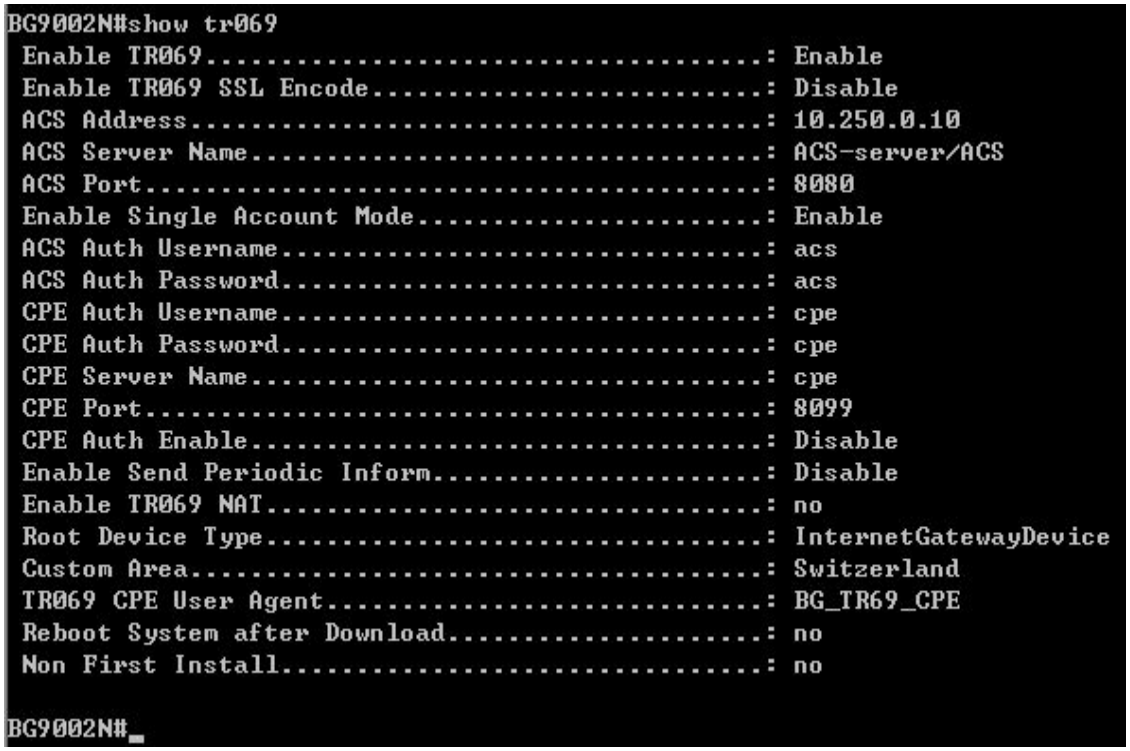


Figure 1-119 Show TR069 Information

The command “set tr069” configure the tr069 parameters as below.

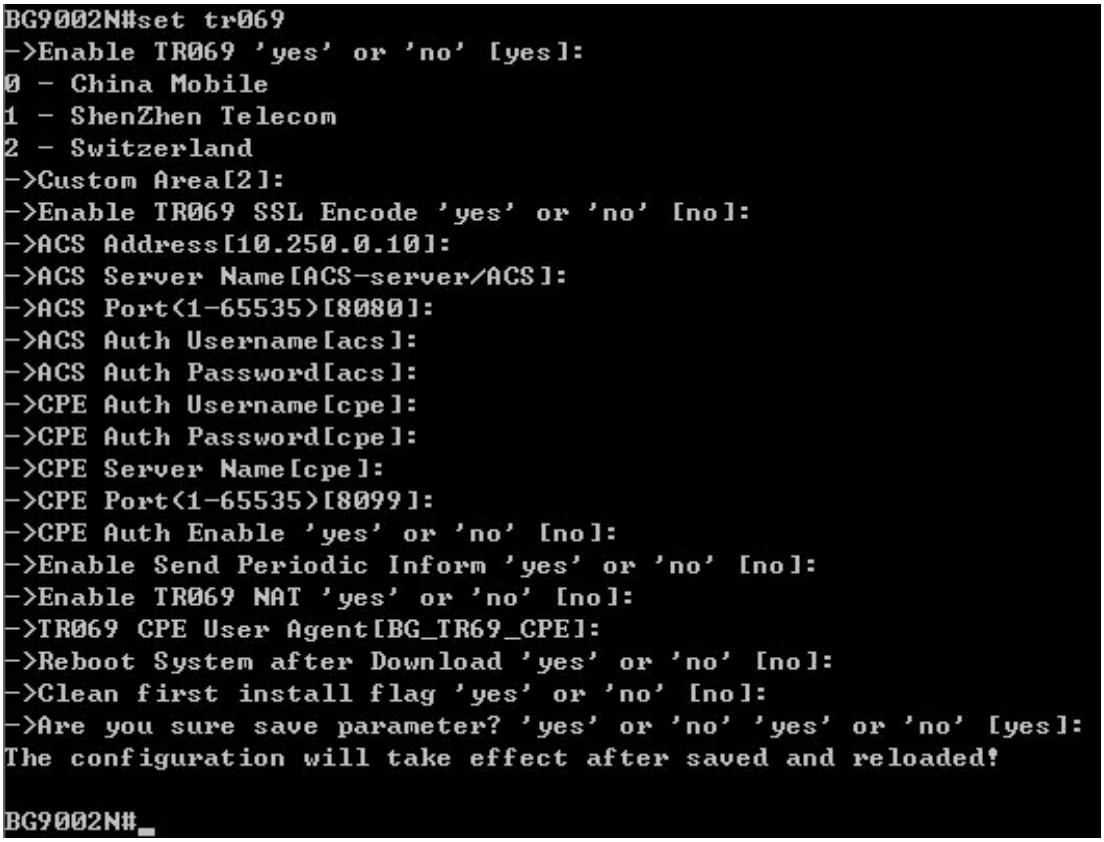


Figure 1-120 Configure TR069 Parameters

The following items are displayed on this screen:

► **Serial Number:** The serial number of device. Read only.

- ► **Enable:** Enable or disable the TR069 function globally.
- ► **ACS Address:** Enter the IP address or domain name of ACS.
- ► **ACS Port:** Enter the port of ACS.
- ► **ACS Server Name:** Enter the TR069 server name of ACS.
- ► **SSL Enable:** Enable or disable the SSL(Secure Sockets Layer) for TR069.
- ► **Schedular Send Inform:** Whether or not the CPE must periodically send CPE information to Server using the Inform method call. Enter the duration in seconds of the interval if enabled.
- ► **Single Account Enable:** Whether or not the TR069 Account is enabled.
- ► **TR069 Account:** Username used to authenticate the CPE when making a connection to the ACS.
- ► **TR069 password:** Password used to authenticate the CPE when making a connection to the ACS.
- ► **Connection Request Auth:** Whether to authenticate an ACS making a Connection Request to the CPE.
- ► **Connection Request Username:** Username used to authenticate an ACS making a Connection Request to the CPE.
- ► **Connection Request Password:** Password used to authenticate an ACS making a Connection Request to the CPE.
- ► **CPE Server Name:** A part of the HTTP URL for an ACS to make a Connection Request notification to the CPE. In the form:http://host:port/**path**
- ► **CPE Port:** A part of the HTTP URL for an ACS to make a Connection Request notification to the CPE. In the form:http://host:**port**/path
- ► **Status:** Connection Status when CPE making a connection to the ACS. Read only.
- ► **Fail Reason:** Show reason for the failure when CPE making a connection to the ACS. Read only.

1.4.7 SNMP

The command “show snmp” show the snmp information as below:

```
BG9002N#show snmp
 Enable Register Server.............................: yes
 Server Address or Domain...........................: 138.0.60.2
 Server Port........................................: 162
 Enable Double Register Server......................: no
 TRAP Message Interval..............................: 30s
 Regional Identity..................................: BG9002N
 Device Identifier..................................:
 Discard Wrong Community Package....................: yes
 Community Name.....................................: public
 Registration Status................................: Register Failed

BG9002N#_
```

Figure 1-121 Show SNMP Information

The command “set snmp” configure the snmp parameters as below.

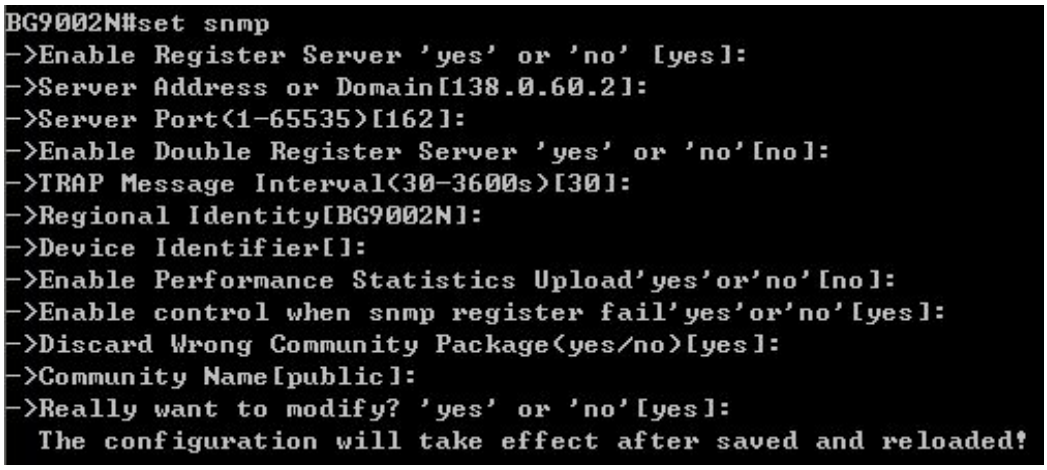


Figure 1-122 Configure SNMP Parameters

The following items are displayed on this screen:

- ► **Register Enable:** Check this box to enable SNMP register.
- ► **Server Address or Domain:** Enter the IP address or domain name of register server.
- ► **Server Port:** Enter the port of Register Server.
- ► **TRAP Message Interval:** Set the sending interval between TRAP messages.
- ► **Regional Identity:** Set the identity of regional.
- ► **Device Identifier:** Set the identifier of device.
- ► **Enable Double Register Server:** Check this box to enable backup Register Server.
- ► **Backup Server Address or Domain:** Enter the IP Address or Domain Name of Backup Register Server.
- ► **Backup Server Port:** Enter the port of Backup Register Server.
- ► **Registration Status:** The status of registration.Read only.

FCC Caution.

§ 15.19 Labelling requirements.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

§ 15.21 Information to user.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

§ 15.105 Information to the user.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the

equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

***RF warning for Mobile device:**
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.