SMCWTVG
Personal Mobile Gateway
Management Guide

The easy way to make all your network connections

SMC® Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

January 2006
Revision Number: R01 F1.0.6.x

Copyright

Trademarks:
SMC is a registered trademark; and EliteConnect is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

Table of Contents

Tables

Figures

Chapter 1: Introduction

The Personal Mobile Gateway, SMCWTVG, offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above), Firefox (version 1.5 or above), or Opera (version 8.51 or above).

The initial configuration steps can be made through the web browser interface using the Setup Wizard. It is recommended to make the initial changes by connecting a PC directly to the Personal Mobile Gateway's LAN port.

Operating Modes

The Personal Mobile Gateway operates in one of three possible modes:

- Gateway
- Wireless Client
- Access Point

The Personal Mobile Gateway's Setup Wizard and Advanced Configuration menus display only settings that are valid for the current operating mode. Before making any configuration settings, be sure the unit is operating in the mode you want to use.

In its default Automatic Configuration setting, the unit starts in Gateway mode if the WAN port has a valid connection. If the WAN port has no connection, it starts in Wireless Client mode.

To set the unit in Access Point mode requires manual configuration. After logging in, you must first use the Advanced Setup menu to set the mode. See "Manually Setting the Operating Mode" on page 1-3.

Accessing the Web Management Interface

The Personal Mobile Gateway has a default IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. If your PC uses DHCP or has an IP address on the same subnet (that is, the PC and Personal Mobile Gateway addresses both start 192.168.2.x), you can connect immediately to the web interface. Otherwise, you must first change your PC's IP address to be on the same subnet as the Personal Mobile Gateway.

In the web browser's address bar, type the default IP address: http://192.168.2.1.

The web browser displays the Personal Mobile Gateway's home page.

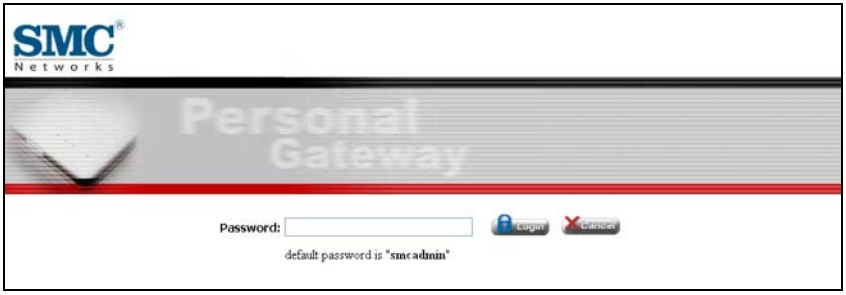

Figure 1-1. Home Page

Logging In – Type the default password "smcadmin" and click Login. For information on configuring a password, see "Administrator Settings" on page 6-4.

The Main Menu displays.

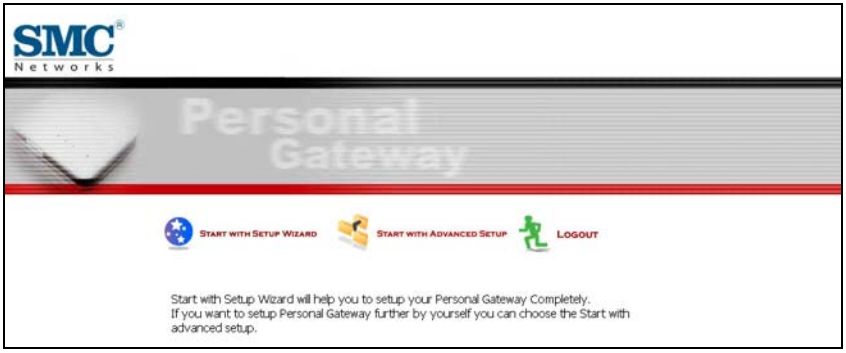

Figure 1-2. Main Menu

To configure basic settings for the current operating mode, click Start with Setup Wizard. For more information, see "Using the Setup Wizard" on page 2-1.

Alternatively, to configure more detailed settings, click Start with Advanced Setup. For more information, see "The Advanced Setup Menus" on page 1-3.

The Advanced Setup Menus

The Advanced Setup menus display only features that are valid for the Personal Mobile Gateway's current operating mode. Each menu is sumarized below with links to the relevant section in this guide where configuration parameters are described in detail.

Gateway Mode:

- **Status** – Display system information. see page 9-1
- **System** – Configure the mode and other settings. see page 6-1
- **WAN** – Configure WAN port connection settings. see page 3-3
- **LAN** – Configure LAN settings. see page 3-6
- **Wireless** – Configure wireless access settings. see page 7-1
- **VoIP** – Configure VoIP settings. see page 8-1
- **NAT** – Configure Network Address Translation settings. see page 3-7
- **Firewall** – Configure firewall settings. see page 3-10

Access Point Mode:

- **Status** – Display system information. see page 9-1
- **System** – Configure the mode and other settings. see page 6-1
- **Wireless** – Configure wireless access settings. see page 7-1
- **VoIP** – Configure VoIP settings. see page 8-1

Wireless Client Mode:

- **System** – Configure the mode and other settings. see page 4-2
- **VoIP** – Configure VoIP settings. see page 8-1

Manually Setting the Operating Mode

To set an operating mode for the Personal Mobile Gateway that is not dependent on the WAN port connection, you must access the Advanced Configuration, System, Mode Configuration page.

Note: Access Point mode can only be set through manual configuration.

Follow these steps:

1. Log into the web interface.
2. Click Start with Advanced Setup.
3. From the menu (in any mode), click System, then Mode Config.
4. Set the Mode Selection to Manual, then select the operating mode you want to use.

5. Click Apply to confirm the setting and restart the unit.

Note: Changing the Personal Mobile Gateway's operating mode always resets the unit.

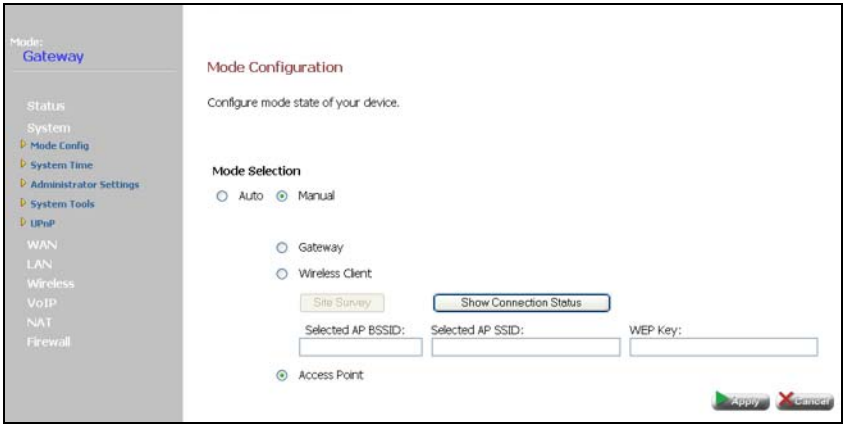

Figure 1-3. Manually Setting the Operating Mode

For more information on the Mode Configuration page, see "Mode Configuration" on page 6-2.

Chapter 2: Using the Setup Wizard

The Personal Mobile Gateway can automatically configure its operating mode for use as a gateway or wireless client. However, it still requires some manual configuration for other modes, its WAN port connection, wireless settings, and VoIP functions. The Setup Wizard takes you through the basic configuration steps for the current operating mode.

Note: The Setup Wizard steps depend on the current operating mode. You should first make sure the Personal Mobile Gateway starts in the mode that you want to use.

Launching the Setup Wizard – To perform basic configuration, click Start with Setup Wizard on the main menu.

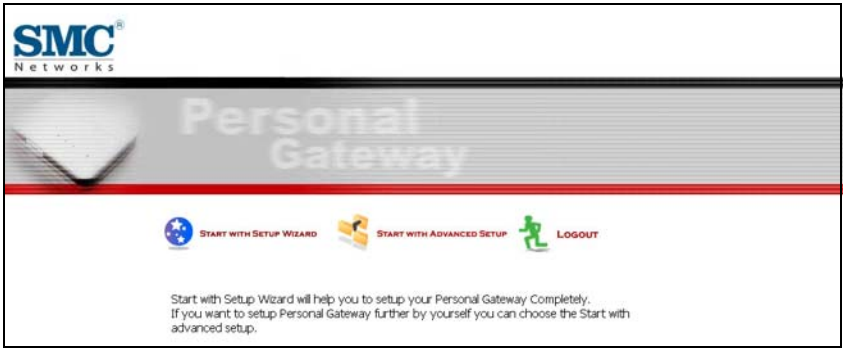

Figure 2-4. Starting the Setup Wizard

The following sections detail the necessary steps in configuring the Personal Mobile Gateway in each of its operating modes.

Gateway Mode

When configuring the unit to operate as a gateway, you will need to proceed through the following four steps:

1. **Settings** – The Settings page takes you through the wireless SSID (Service Set Identifier) configuration.

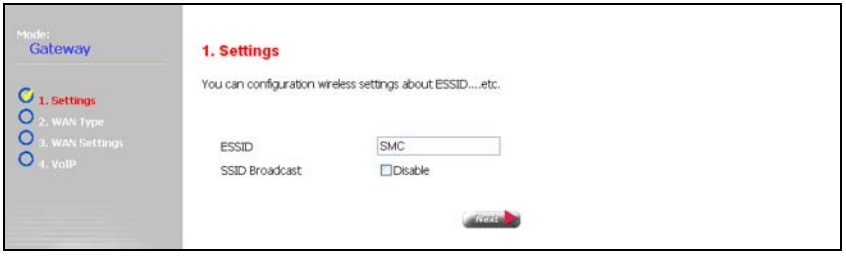

Figure 2-5. Gateway Settings

ESSID (Extended Service Set Identifier) – The ESSID is a name that uniquely identifies the wireless network provided by the Personal Mobile Gateway. Clients that want to connect to the wireless network must set their SSID to the same as that of the Personal Mobile Gateway.

SSID Broadcast – Check this box to disable broadcasting the configured ESSID. The Personal Mobile Gateway is configured by default as an "open system," which broadcasts a beacon signal including the configured ESSID. Wireless clients with a configured SSID of "ANY" can read the SSID from the beacon, and automatically set their SSID to allow immediate connection to the Personal Mobile Gateway. When disabled, the Personal Mobile Gateway does not include its ESSID in beacon messages. This provides a basic level of security, since wireless clients must be pre-configured with the ESSID to connect to the Personal Mobile Gateway.

2. **WAN Type** – The WAN Type page is for specifying the WAN port connection to your Internet service provider (ISP). When one of the four options is specified, the Wizard displays the appropriate configuration parameters.

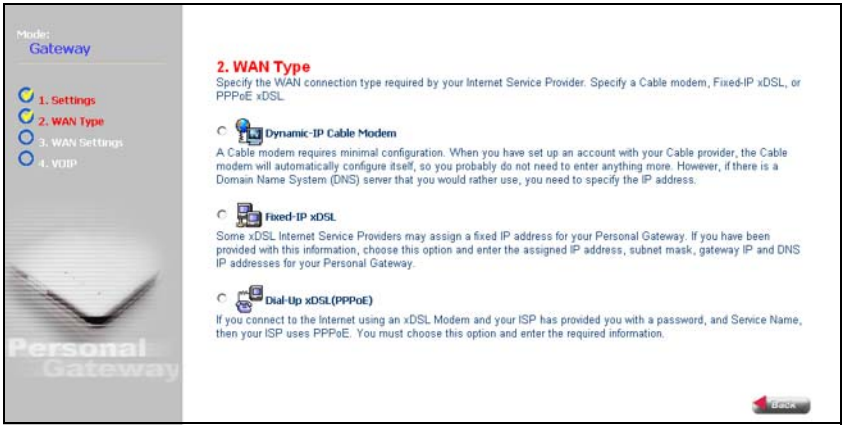

Figure 2-6. Gateway WAN Type

Dynamic-IP Cable Modem – Selects configuration for a cable modem Internet connection.

Fixed-IP xDSL – Selects configuration for a fixed IP address xDSL Internet connection.

Dial Up xDSL (PPPoE) – Selects configuration for an Internet connection using the Point-to-Point Protocol over Ethernet (PPPoE).

3. **WAN Settings** – The WAN Settings page displays the configuration settings for the WAN Type that you have selected. The following example displays a Cable Modem selection.

Figure 2-7. Gateway WAN Type - Cable Modem

For a cable modem connection, the unit requires no further configuration and prompts you to move to step four.

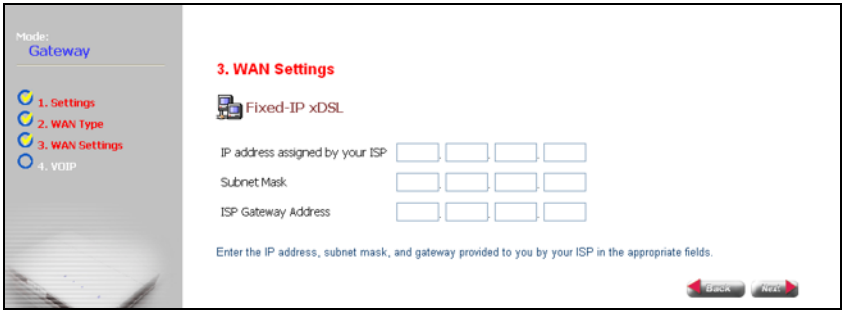

Figure 2-8. Gateway WAN Type - Fixed-IP xDSL

For a fixed IP xDSL connection, you are prompted for the following information (as supplied by your ISP):

IP Address – If your ISP has assigned you a fixed IP address, enter the address here.

Subnet Mask – Enter the subnet mask as supplied by your ISP.

ISP Gateway Address – The gateway IP address of your ISP.

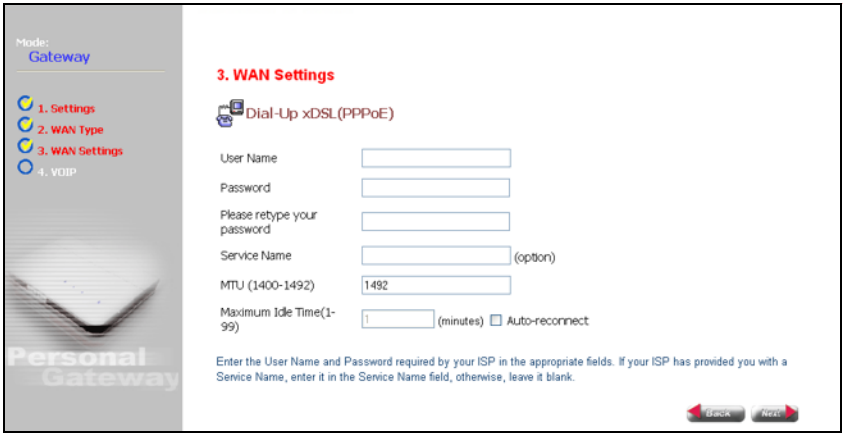

Figure 2-9. Gateway WAN Type - Dial-Up xDSL

For a dial-up xDSL (PPPoE) connection you are prompted for the following information:

User Name – Enter your user name for connecting to the xDSL service, as supplied by your ISP. (Range: 1-32 characters)

Password – Specify the password for your xDSL connection, as supplied by your ISP. (Default: No password)

Service Name – Enter the xDSL service name (if any) as supplied by your ISP.

MTU (1400~1492) – The Maximum Transmission Unit for Ethernet data transmission. Only change the default value if specifically instructed by your ISP. (Range: 1400~1492 bytes)

Maximum Idle Time (1~99) – The maximum length of inactive time the unit will stay connected to the xDSL service provider before disconnecting. This feature only works when Auto-Reconnect is selected. (Range: 1~99 minutes)

Auto-reconnect – Selecting this option prompts the unit to reconnect to the xDSL service provider after the connection has been lost.

4. **VoIP** (Voice over Internet Protocol) – The VoIP page allows you to configure SIP (Session Initiation Protocol) parameters for enabling Internet telephony.

   VoIP service providers operate SIP “proxy servers” that allow you to register your Personal Mobile Gateway on their system so that you can make telephone calls over the Internet. Your VoIP service provider will provide you with the connection details that need to be set up on the Personal Mobile Gateway to be able to use their service.

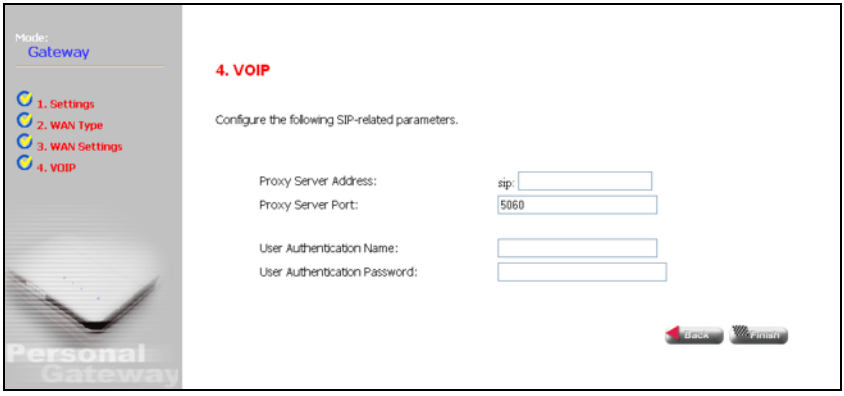

Figure 2-10. Gateway VoIP Configuration

Proxy Server Address – Address of the VoIP service provider proxy server.

Proxy Server Port – The TCP port number used by the VoIP service provider's proxy server. (Default: 5060)

User Authentication Name – An alphanumeric string that uniquely identifies the user to the SIP server, as supplied by the VoIP service provider.

User Authentication Password – An alphanumeric string that uniquely identifies the SIP user's permission rights, as supplied by the VoIP service provider.

Wireless Client Mode

When configuring the unit to operate as a wireless client, you will need to proceed through the following two steps:

1. **Settings** – The settings page takes you through the process of searching and selecting the access point to which you want to connect.

   If you know the SSID of the wireless network, you can enter it directly in the text box provided. Otherwise, you may perform a wireless scan to detect all access points that are within range, and then select the access point you want to connect to from a list.

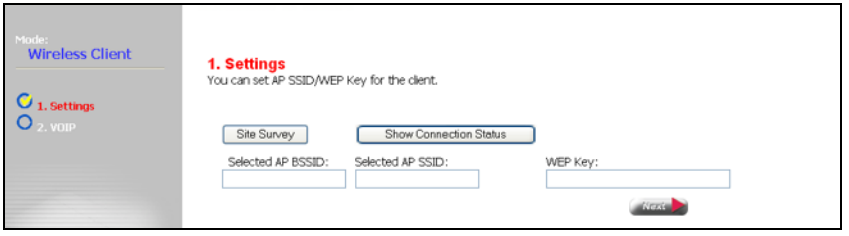

Figure 2-11. Wireless Client Settings

Site Survey – Performs a wireless scan on all channels to detect all nearby access points. A list of deteced access points is displayed from which you can select an access point to connect to.

Selected AP SSID – Enter the service set identifier of the wireless network you want to connect to. The SSID is case sensitive and can consist of up to 32 alphanumeric characters.

WEP Key – WEP (Wireless Equivalent Privacy) provides a basic level of security in wireless networks, it prevents unauthorized access by encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use an access point. If the wireless network you are connecting to uses WEP security, you need to enter the WEP key provided to you by the network operator.

Show Connection Status – Displays the connection status of the unit to the selected access point.

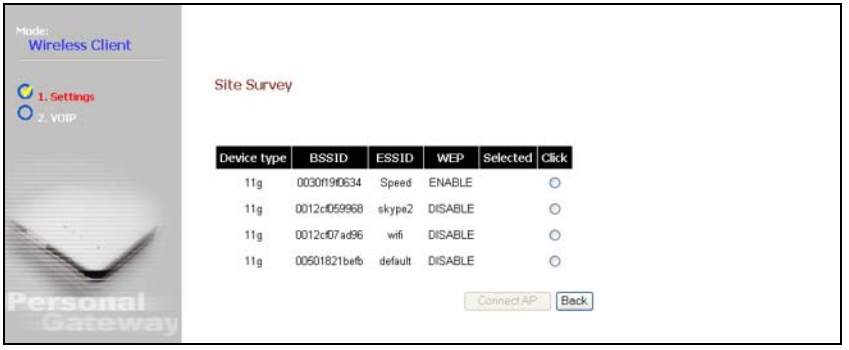

Figure 2-12. Wireless Client Site Survey

The Site Survey page displays a list of access points that are within range for connection.

Upon selection of a suitable access point, the unit asks you to confirm if you want to connect to that particular access point.

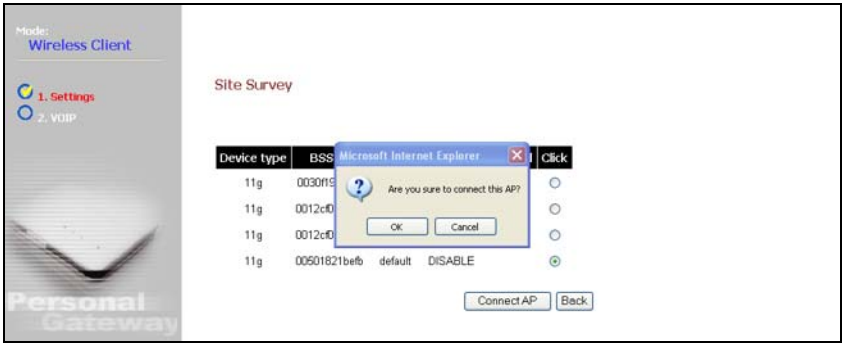

Figure 2-13. Confirm Wireless Client Connection

Clicking on Connection Status displays the status that the Personal Mobile Gateway has with the selected access point.

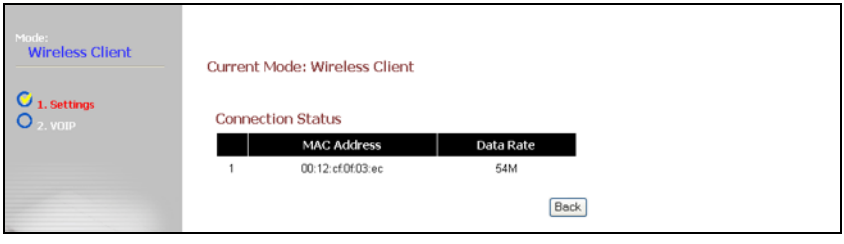

Figure 2-14. Wireless Client Connection Status

2. **VoIP** (Voice over Internet Protocol) – The VoIP page allows you to configure SIP (Session Initiation Protocol) parameters for enabling Internet telephony.

   VoIP service providers operate SIP “proxy servers” that allow you to register your Personal Mobile Gateway on their system so that you can make telephone calls over the Internet. Your VoIP service provider will provide you with the connection details that need to be set up on the Personal Mobile Gateway to be able to use their service.

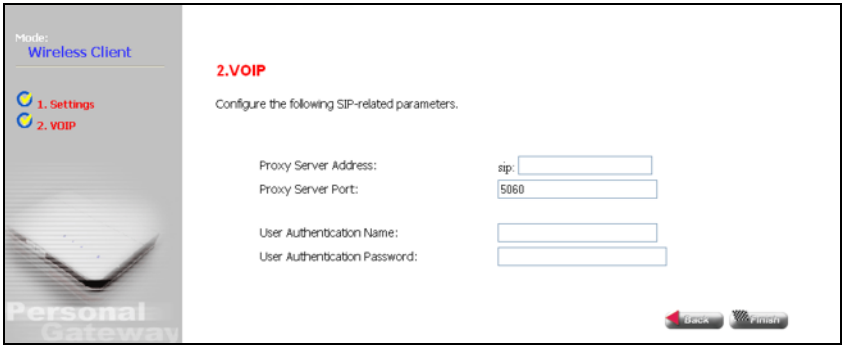

Figure 2-15. Setup Wizard VoIP Settings

Proxy Server Address – Address of the VoIP service provider proxy server.

Proxy Server Port – The TCP port number used by the VoIP service provider's proxy server. (Default: 5060)

User Authentication Name – An alphanumeric string that uniquely identifies the user to the SIP server, as supplied by the VoIP service provider.

User Authentication Password – An alphanumeric string that uniquely identifies the SIP user's permission rights, as supplied by the VoIP service provider.

Access Point Mode

When configuring the unit to operate as an access point, you need to proceed through the following two steps:

1. **Settings** – The Settings page takes you through the SSID (Service Set Identifier) configuration.

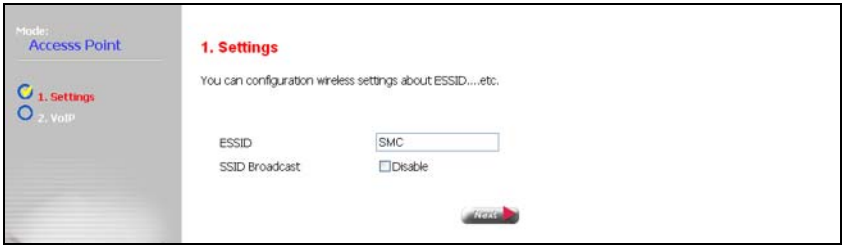

Figure 2-16. Access Point Settings

ESSID (Extended Service Set Identifier) – The ESSID is a name that uniquely identifies the wireless network provided by the Personal Mobile Gateway. Clients that want to connect to the wireless network must set their SSID to the same as that of the Personal Mobile Gateway.

SSID Broadcast – Check this box to disable broadcasting the configured ESSID. The Personal Mobile Gateway is configured by default as an “open system,” which broadcasts a beacon signal including the configured ESSID. Wireless clients with a configured SSID of “ANY” can read the SSID from the beacon, and automatically set their SSID to allow immediate connection to the Personal Mobile Gateway. When disabled, the Personal Mobile Gateway does not include its ESSID in beacon messages. This provides a basic level of security, since wireless clients must be pre-configured with the ESSID to connect to the Personal Mobile Gateway.

2. **VoIP** (Voice over Internet Protocol) – The VoIP page allows you to configure SIP (Session Initiation Protocol) parameters for enabling Internet telephony.

   VoIP service providers operate SIP “proxy servers” that allow you to register your Personal Mobile Gateway on their system so that you can make telephone calls over the Internet. Your VoIP service provider will provide you with the connection details that need to be set up on the Personal Mobile Gateway to be able to use their service.

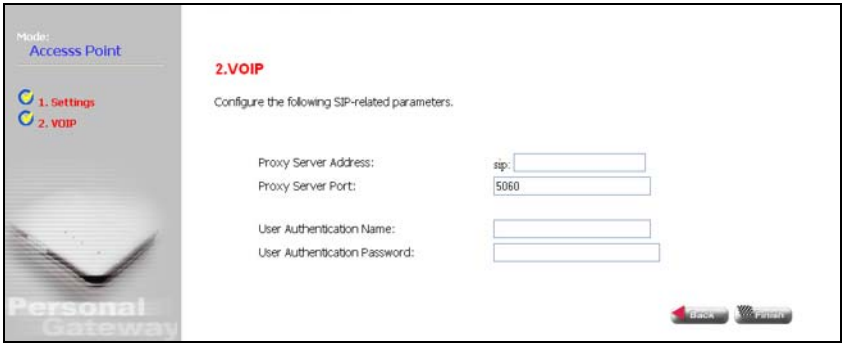

Figure 2-17. Access Point VoIP Configuration

Proxy Server Address – Address of the VoIP service provider proxy server.

Proxy Server Port – The TCP port number used by the VoIP service provider's proxy server. (Default: 5060)

User Authentication Name – An alphanumeric string that uniquely identifies the user to the SIP server, as supplied by the VoIP service provider.

User Authentication Password – An alphanumeric string that uniquely identifies the SIP user's permission rights, as supplied by the VoIP service provider.

Chapter 3: Gateway Mode

Operating in Gateway mode, the Personal Mobile Gateway provides comprehensive firewall features and NAT isolation for Internet traffic passing from the WAN port to wireless clients, or to a local network connected to the LAN port.

The DHCP server feature can assign IP addresses for up to 32 local network PCs and wireless clients. Full access point features are provided for wireless clients, with robust security options available and QoS support for voice or video traffic.

Figure 3-1. Gateway Mode Settings

The information in this chapter is organized to reflect the structure of the web screens for easy reference. Detailed information on system status, system settings, wireless settings, and VoIP are located in other chapters.

In Gateway Mode, the Advanced Setup menu includes the following options.

Table 3-1. Gateway Configuration Options

Menu	Description	Page
Status	Displays the current system status	9-1
System	Configures basic administrative settings	6-1
WAN	Sets the connection method of your Internet service provider	3-3
WAN Type	Selects the Internet connection method	3-3
Dynamic IP	Obtain an IP address automatically from your ISP	3-3
IP Settings	Set a fixed IP address provided by your ISP	3-3
PPPoE	Sets up a PPPoE connection to your ISP	3-3
DNS	Specifies DNS servers that you want to access	3-4
DDNS	Specifies a dynamic DNS service to use	3-5

Table 3-1. Gateway Configuration Options		
Menu	Description	Page
LAN	Configures IP settings for the local network	3-6
LAN Settings	Sets the unit's IP address and configures the DHCP server for the local network	3-6
Wireless	Configures wireless settings	7-1
Setting	Sets the ESSID, radio channel, and other settings	7-1
Security	Configures wireless encryption and authentication	7-4
Wireless QoS	Controls QoS for traffic prioritization	7-7
VoIP	Configures VoIP parameters	8-1
SIP Settings	Configures SIP parameters	8-2
Advanced Setting	Configures call forwarding and DTMF parameters	8-3
NAT	Shares a single ISP account with multiple users, sets up virtual servers	3-7
Virtual Server	Allows the unit to be configured as a virtual server	3-7
Port Mapping	Enables IP port mapping for special applications	3-8
DMZ	Allows clients to connect to the unit directly bypassing the firewall	3-9
Firewall	Controls access to and from the local network with various filtering options	3-10
Firewall Options	Blocks scans of the network services from an outside hacker	3-10
Client Filtering	Blocks internet access on an IP basis	3-12
MAC Control	Blocks internet access on a MAC basis	3-12

WAN

Specify the WAN connection parameters provided by your Internet Service Provider (ISP).

WAN Type

Specifies the type of WAN connection to use from a list of options. The selected option depends on the device connected to the WAN port and your specific ISP service.

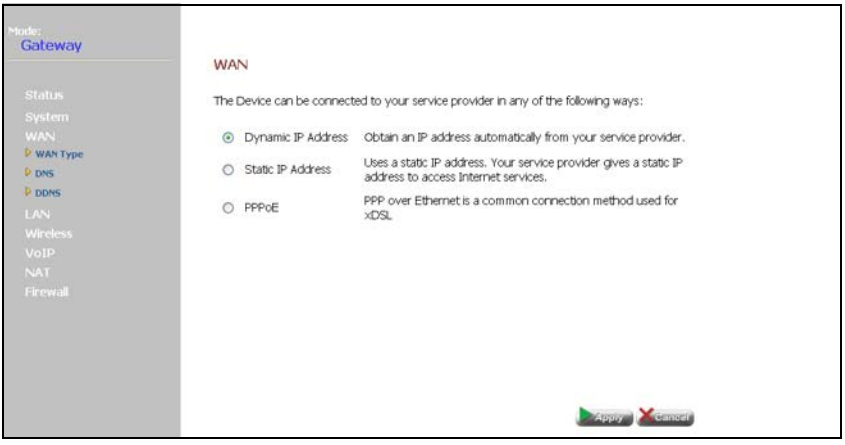

Figure 3-2. Gateway Mode WAN Type

The unit can be connected to your ISP in one of the following ways:

- **Dynamic-IP Cable Modem** – Selects configuration for a cable modem Internet connection.
- **Fixed-IP xDSL** – Selects configuration for a fixed IP address xDSL Internet connection.
- **Dial Up xDSL (PPPoE)** – Selects configuration for an Internet connection using the Point-to-Point Protocol over Ethernet (PPPoE).

DNS

DNS (Domain Name System) server addresses are usually provided by service providers, however if you want to specify certain servers, the DNS page allows you to enter primary and secodary DNS addresses.

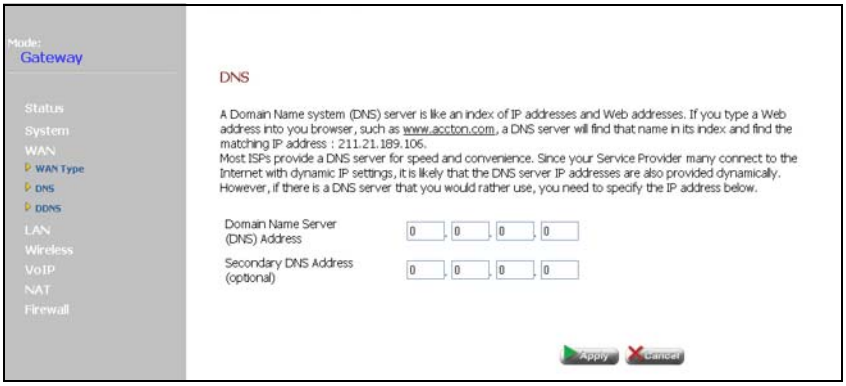

Figure 3-3. Gateway Mode DNS Setup

- **Domain Name Server (DNS) Address** – Address of the primary DNS server, specified in the form of 0.0.0.0
- **Secondary DNS Address (optional)** – Optional address of a secondary DNS server, specified in the form of 0.0.0.0

DDNS

Dynamic DNS (DDNS) provides users on the Internet with a method to tie a specific domain name to the unit's dynamically assigned IP address. DDNS allows your domain name to follow your IP address automatically by changing your DNS records when your IP address changes.

The Personal Mobile Gateway provides access to two DDNS service providers, dyndns.org and dyns.cx. To set up an DDNS account, visit the websites of these service providers at www.dyndns.org or www.dyns.cx.

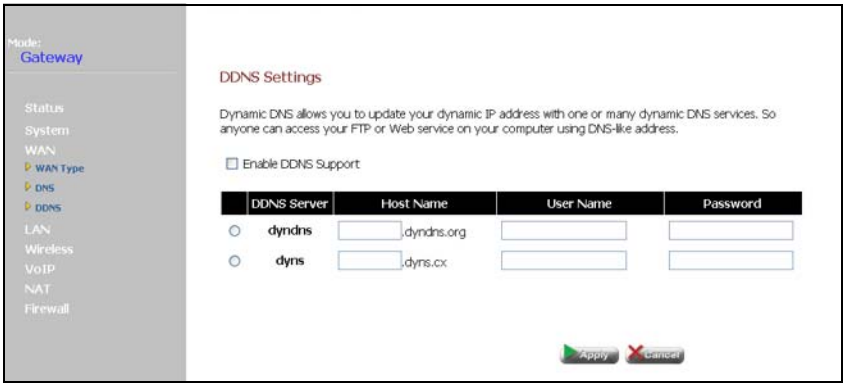

Figure 3-4. Gateway Mode Dynamic DNS Setup

- **DDNS Server** – Specifies the DDNS service provider.
- **Host Name** – Specifies the prefix to identify your presence on the DDNS server.
- **User Name** – Specifies your username for the DDNS service.
- **Password** – Specifies your password for the DDNS service.

LAN

The Personal Mobile Gateway must have a valid IP address for management using a web browser and to support other features. The unit has a default IP address of 192.168.2.1. You can use this IP address or assign another address that is compatible with your existing local network. The unit can also be enabled as a Dynamic Host Configuration Protocol (DHCP) server to allocate IP addresses to local PCs and wireless clients. The unit supports up to 32 local clients.

LAN Settings

The Personal Mobile Gateway includes a DHCP server that can assign temporary IP addresses to any attached host requesting the service. Addresses are assigned to clients from a common address pool configured on the unit. Configure an address pool by specifying start and end IP addresses. Be sure not to include the unit's IP address in the address pool range.

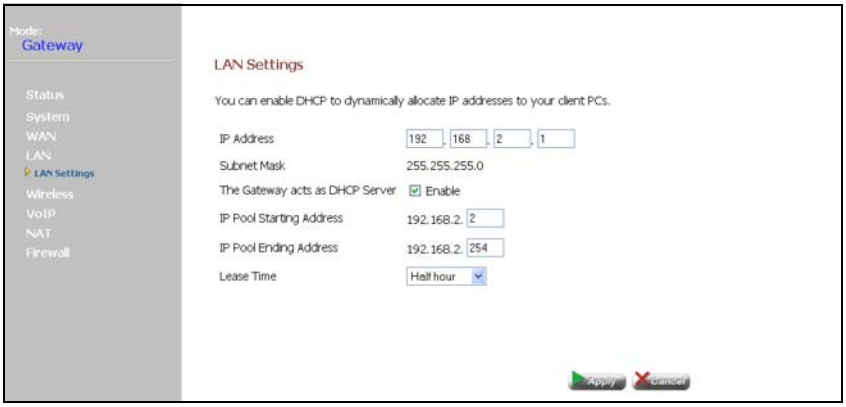

Figure 3-5. Gateway Mode LAN Settings

- **IP Address** – The IP address of the unit. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.The default setting is 192.168.2.1.
- **Subnet Mask** – Indicates the local subnet mask is fixed as 255.255.255.0.
- **The Gateway acts as DHCP Server** – Check this box to enable the DHCP server.
  - **IP Pool Starting/Ending Address** – Specifies the start and end IP address of a range that the DHCP server can allocate to DHCP clients. You can specify a single address or an address range. Note that the address pool range is always in the same subnet as the unit's IP setting.
  - **Lease Time** – Selects a time limit for the use of an IP address form the IP pool. When the time limit expires, the client has to request a new IP address.

NAT

Network Address Translation (NAT) is a standard method of mapping multiple "internal" IP addresses to one "external" IP address on devices at the edge of a network. For the Personal Mobile Gateway, the internal (local) IP addresses are the IP addresses assigned to PCs and wireless clients by the DHCP server, and the external IP address is the IP address assigned to the WAN port.

Virtual Server

Using the NAT Virtual Server feature, remote users can access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site thorugh your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.9/80, then all HTTP requests from outside users forwarded to 192.168.2.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

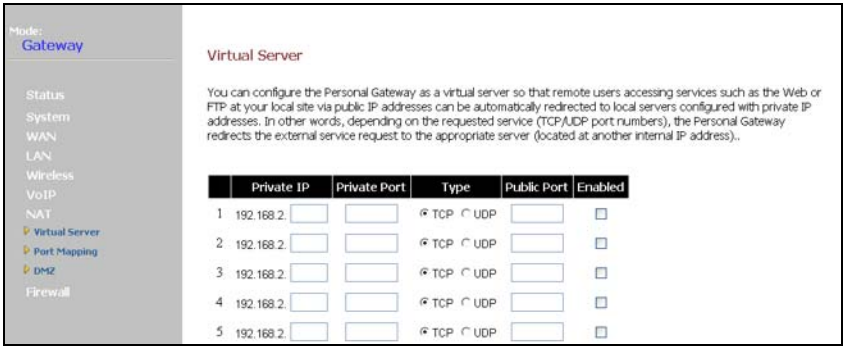

Figure 3-6. Gateway Mode Virtual Server

- **Private IP** – The IP address of the server on the local Ethernet network. The specified address must be in the same subnet as the Personal Mobile Gateway and its DHCP server address pool.
- **Private Port** – Specifies the port number used on the local server for the service.
- **Type –** Specifies the port type. (Options: TCP or UDP; Default: TCP)
- **Public Port** – Specifies the public port used for the service.
- **Enabled** – Enables the virtual server mapping on the specified ports.

Port Mapping

Some applications, such as Internet gaming, videoconferencing, Internet telephony and others, require multiple connections. These applications cannot work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use port mapping to specify the additional public ports to be opened for each application.

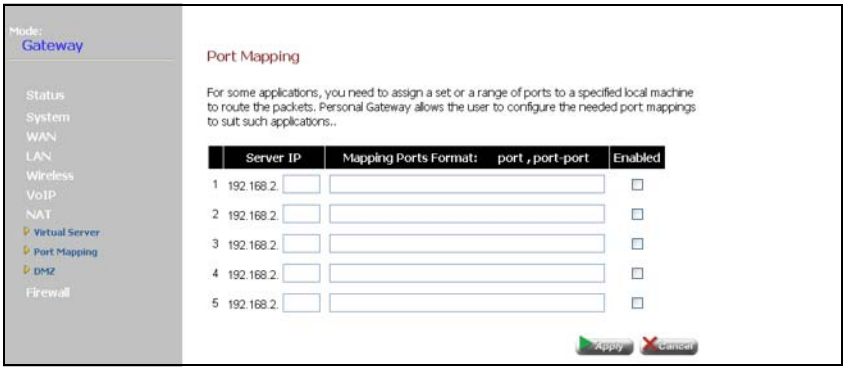

Figure 3-7. Gateway Mode Port Mapping

- **Private IP** – The IP address of the local server.
- **Mapping Ports Format: port, port-port** – Specifies the ports that the application requires. The ports may be specified individually, in a range, or a combination of both. For example, 7, 11, 57, 72-96.
- **Enabled** – Enables port mapping for the specified IP addresst.

DMZ

If you have a client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way internet access by defining a virtual-DMZ (virtual-demilitarized-zone) host.

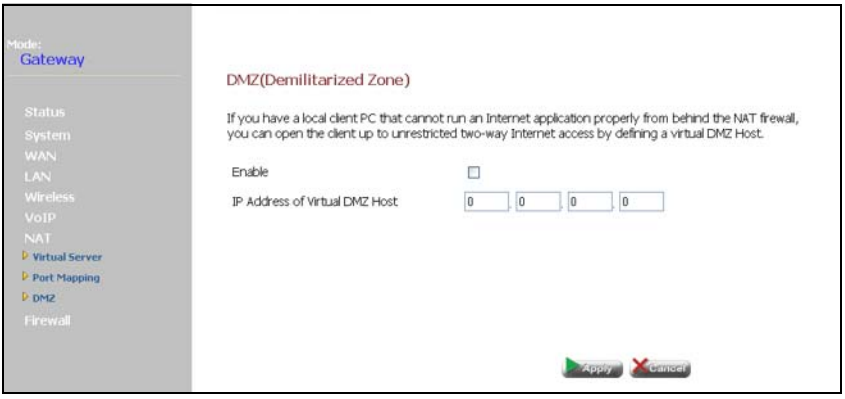

Figure 3-8. Gateway Mode DMZ

- **Enable –** Enables the feature.
- **IP Address of Virtual DMZ Host –** Specifies the IP address of the virtual DMZ host. (Default: 0.0.0.0)

Note: Adding a host to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

Firewall

The Personal Mobile Gateway provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

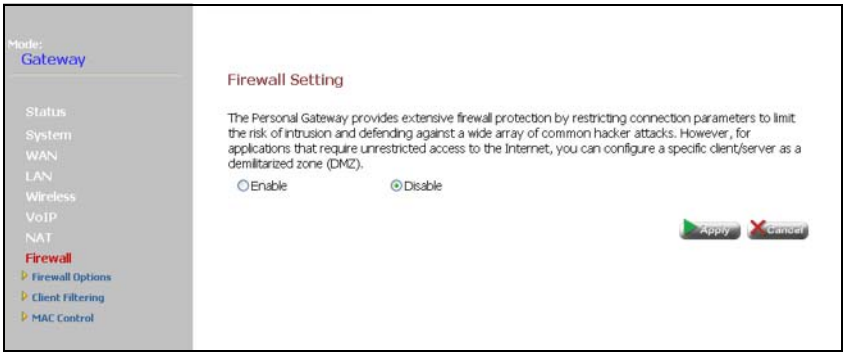

Figure 3-9. Gateway Mode Firewall Setting

- **Enable** – Enables the feature.
- **Disable** – Disables the feature.

Firewall Options

The Personal Mobile Gateway's firewall enables access control of client PCs, blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, Smurf Attack, TCP null scan, ICMP defect, and TCP SYN flooding. The firewall does not significantly affect system performance and it is best to leave it enabled to protect your network.

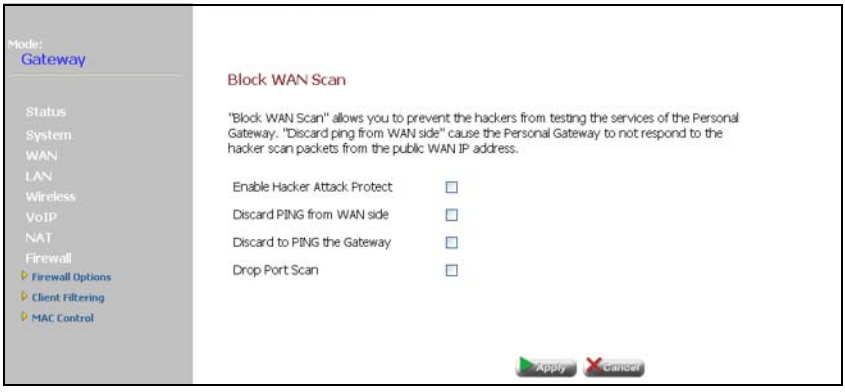

Figure 3-10. Gateway Mode Firewall Options

- **Enable Hacker Attack Protect** – Network attacks that deny access to a network device are called DoS attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The VoIP Router protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, Smurf Attack, TCP null scan, ICMP defect, and TCP SYN flooding.
- **Discard PING from WAN side** – Prevents pings on the unit's WAN port from being routed to the network.
- **Discard to PING the Gateway** – Prevents any response to a ping to the unit's IP address.
- **Drop Port Scan** – Prevents outside hackers form testing the TCP/UDP port numbers on the unit for any services.

Client Filter

You can block access to the Internet from clients on the local network by specifying IP addresses, port numbers and types.

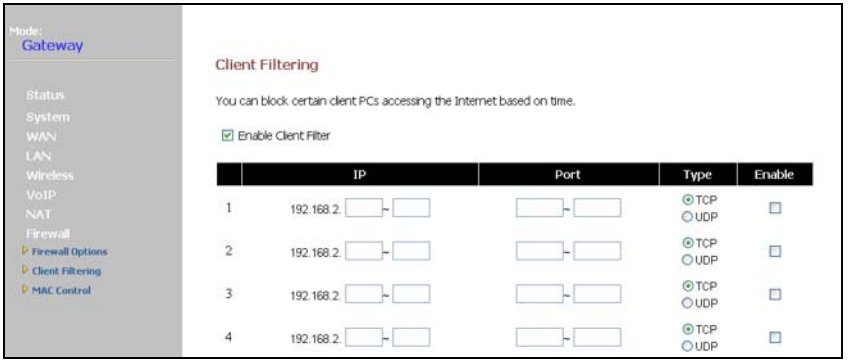

Figure 3-11. Gateway Mode Client Filter

- **Enable Client Filter** – Enables the feature.
- **IP** – Specifies an IP address or range on the local network.
- **Port** – Specifies a port number range to filter.
- **Type** – Specifies the connection type. (Default: TCP)
- **Enable** – Enables filtering for the table entry.

MAC Control

You can block access to the Internet from clients on the local network by MAC addresses.

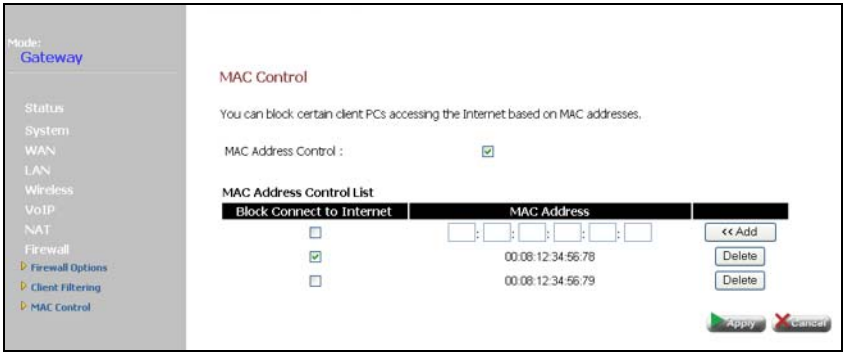

Figure 3-12. Gateway Mode MAC Control

- **MAC Address Control** – Enables the feature.
- **Block Connect to Internet** – Blocks Internet access for the scpecified MAC address.
- **MAC Address** – Specifies a local PC MAC address.
- **Add** – Adds a MAC address to the filter table.
- **Delete** – Removes a MAC address from the filter table.

Chapter 4: Wireless Client Mode

Operating in Wireless Client mode, the Personal Mobile Gateway can connect to an 802.11b/g wireless network and forward traffic from an attached PC.

To access a wireless network in Wireless Client mode, connect your PC to the LAN port and then set your PC's network connection to DHCP. In Wireless Client mode, the Personal Mobile Gateway acts as a DHCP server to assign IP address settings to one client connected on the LAN port. Use the default IP address, 192.168.2.1, to access the web management interface. Using the Setup Wizard or from the Mode Config page, you can then set up a connection to a nearby access point. See "Connecting to an Access Point" on page 4-3.

Figure 4-1. Wireless Client Settings

The information in this chapter is organized to reflect the structure of the web interface pages for easy reference. All VoIP configuration information is located in Chapter 5.

The Advanced Configuration pages include the following options.

Table 4-1. Wireless Client Configuration Options

Menu	Description	Page
System	Configures basic administrative and client access	6-1
Mode Config	Sets up a client connection with a wireless network	4-2
User Settings	Configures user password for management access	4-5
System Tools	Allows you to restore the factory default settings, or store your own setting	4-6
System Status	Displays current system information	4-7
System Log	Displays system log events	4-9
VoIP	Configures VoIP parameters	8-1
SIP Settings	Configures SIP parameters	8-2
Advanced Setting	Configures call forwarding, and DTMF parameters	8-3

Mode Configuration

When operating in Wireless Client mode, you must set a Service Set Identification (SSID) to identify the wireless network service to which you want to connect. First perform a site survey to find available nearby access points, then select the wireless network service you want to use from the displayed list. If the wireless network uses WEP security, enter the WEP key provided by the service operator.

Figure 4-2. Wireless Client Mode Configuration

Mode Selection – Allows you to select Auto configuration (2 operating modes) or Manual configuration (3 operating modes). (Default: Auto)

- **Auto** – The unit automatically selects the operating mode depending on the WAN port status.
  - With no link on the WAN port, the unit starts up in Wireless Client mode.
  - With a link on the WAN port, the unit starts up in Gateway mode.
- **Manual** – Allows you to manually select the mode in which the unit operates:
  - **Gateway** – The unit operates as a secure Internet gateway between a WAN port connection and a wired LAN or wireless devices.
  - **Wireless Client** – The unit operates as a wireless client to connect to nearby access points:
    - **Site Survey** – Performs a wireless scan on all channels to detect all nearby access points. A list of deteced access points is displayed from which you can select an access point to connect to.
    - **Selected AP SSID** – Enter the service set identifier of the wireless network you want to connect to. The SSID is case sensitive and can consist of up to 32 alphanumeric characters.
    - **WEP Key** – WEP (Wireless Equivalent Privacy) provides a basic level of security in wireless networks, it prevents unauthorized access by encrypting

data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use an access point. If the wireless network you are connecting to uses WEP security, you need to enter the WEP key provided to you by the network operator.

- **Show Connection Status** – Displays the connection status of the unit and the selected access point.

- **Access Point** – The unit operates as an access point that passes data between a wired network and wireless clients.

Connecting to an Access Point

To set up a wireless client connection to an access point, perform the following steps:

1. On the Mode Config page, click the Site Survey button.
2. Wait about six to ten seconds for the radio scan to complete. When the scan completes, a list of detected access points is displayed.

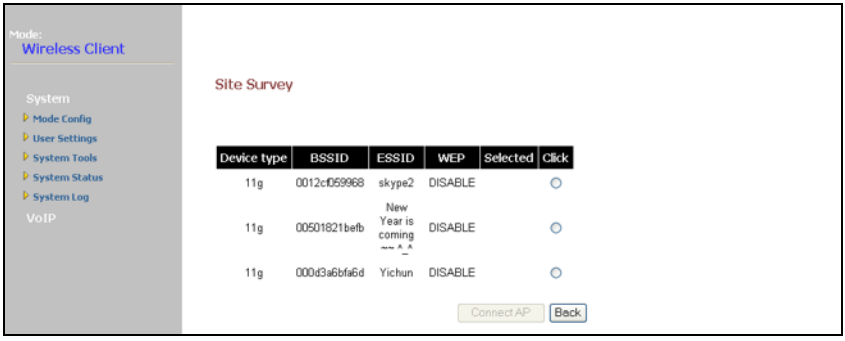

Figure 4-3. Wireless Client Site Survey

3. From the displayed list, select the wireless network ESSID you want to connect to by clicking the radio button.
4. Click the Connect AP button. A message displays to confirm if you want to connect to that particular access point. Click OK to complete the connection and return to the Mode Config page.

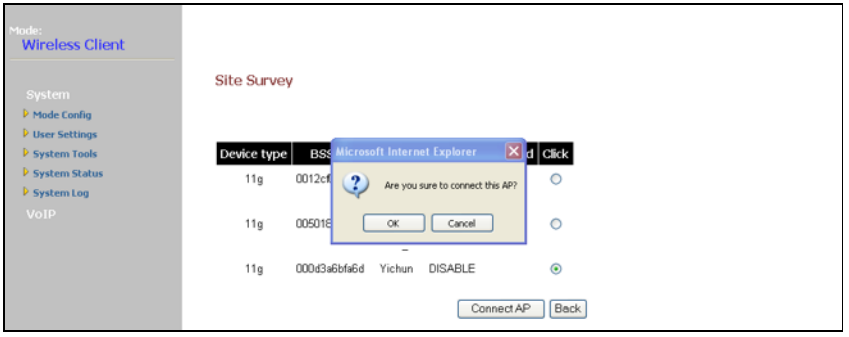

Figure 4-4. Confirm Wireless Client Connection

5. From the Mode Config page, click Show Connection Status to confirm the client connection.

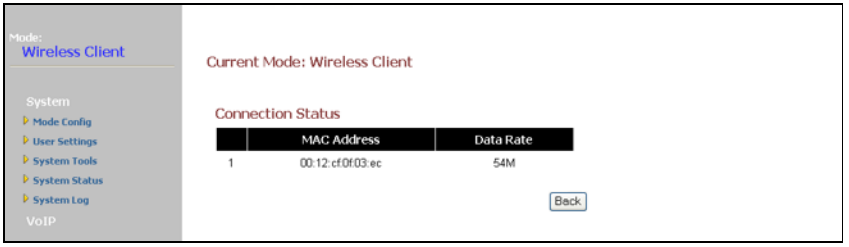

Figure 4-5. Wireless Client Connection Status

User Settings

The User Settings page allows you to change the web interface management access password and set the interface logout time.

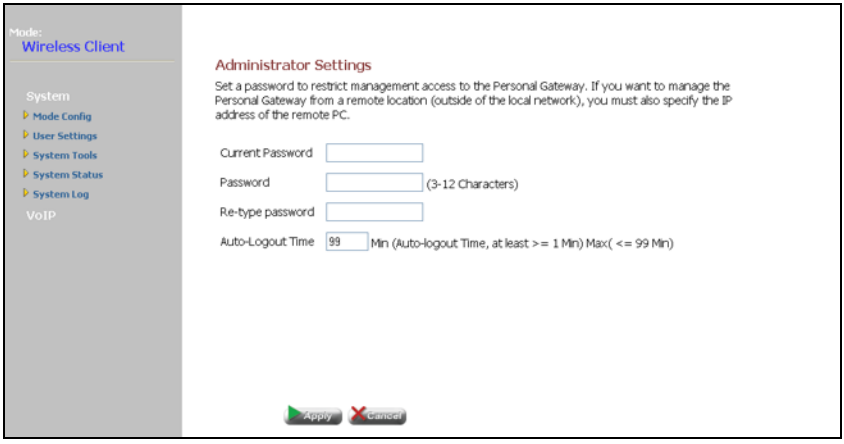

Figure 4-6. Wireless Client User Settings

- **Current Password** – Type your current password. (Default: smcadmin)
- **Password** – Type a new password. (Range: 3~12 characters)
- **Re-type Password** – Type the new password again to confirms it.
- **Auto-Logout Time** – Sets the time of no user activity after which the unit terminates a web management session. (Default: 30 minutes; Range: 1~99 minutes)

System Tools

The System Tools page allows you to upload new runtime code to the unit, restore factory default settings, save and restore the unit's configuration settings, and to reset the unit.

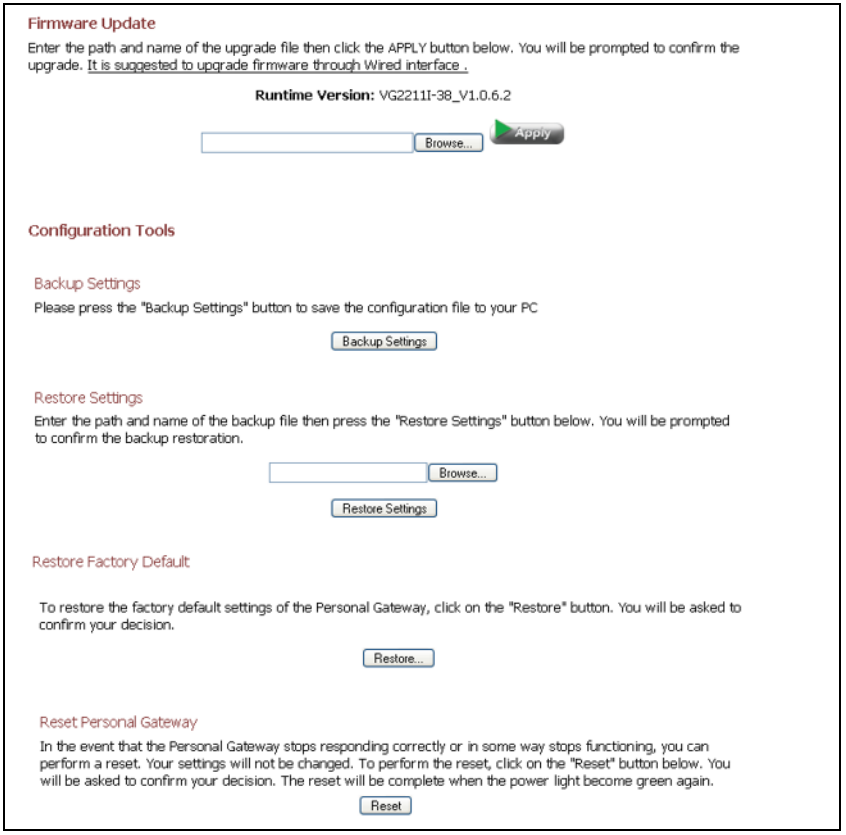

Figure 4-7. Wireless Client Configuration Tools

- **Firmware Update** – Downloads an operation code file from the web management station to the Personal Mobile Gateway using HTTP. Use the Browse button to locate the software code file locally on the management station. Click Apply to proceed.
- **Configuration Tools:**
  - **Backup Settings** – Saves the current configuration settings to a file on the web management station.
  - **Restore Settings** – Restores a saved configuration file to the unit.

- **Restore Factory Default** – Resets the unit to its factory default settings.
- **Reset Personal Gateway** – Allows the user to reboot the unit.

System Status

The system status page displays connectivity status information for the unit's wireless, WAN, and LAN interfaces, as well as firmware and hardware version numbers.

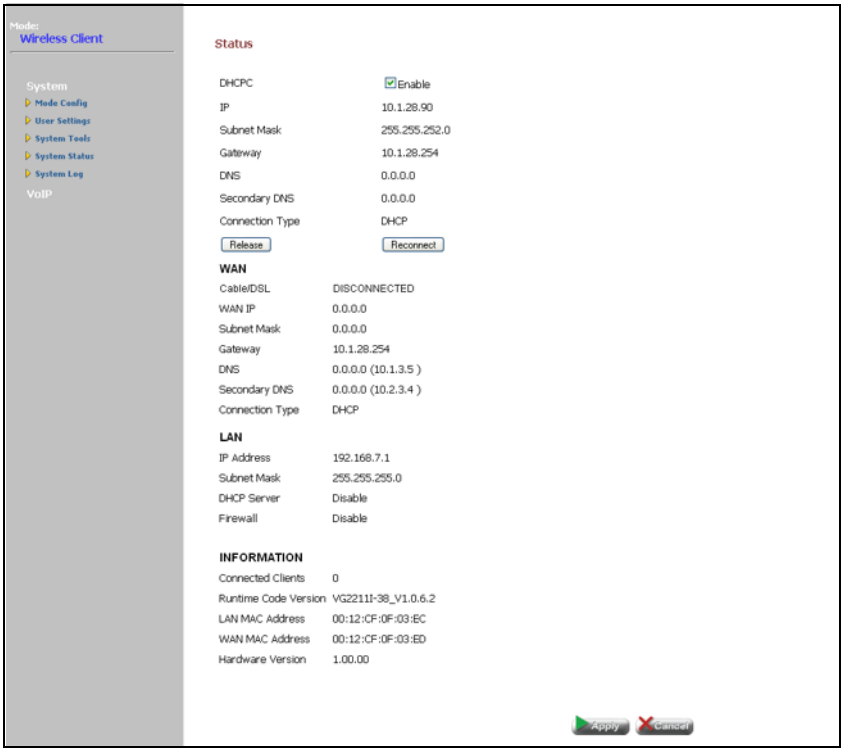

Figure 4-8. Wireless Client System Status

- **DHCPC** – Enables the DHCP client for the unit. In Wireless Client mode, the Personal Mobile Gateway requests an IP address from the wireless network's DHCP server. This IP address is used by the unit to route traffic from the connected PC. It is required to keep this option enabled for Wireless Client mode to operate.
- **IP** – Displays the IP address assigned by DHCP.
- **Subnet Mask** – Displays the subnet mask provided by DHCP.
- **Gateway** – Displays the gateway address provided by DHCP.

- **DNS** – Displays a configured DNS address. The DNS IP can only be configured when in Gateway mode.
- **Secondary DNS** – Displays a configured secondary DNS address. The secondary DNS IP can only be configured when in Gateway mode.
- **Connection Type** – Displays the connection type for the wireless interface (always DHCP for Wireless Client mode).
- **Release** – Releases the current IP address information.
- **Reconnect** – Initiates a new DHCP client request for an IP address.

WAN – Displays the WAN connection type and status:

- **Cable/DSL** – Displays connections status. Always displays “DISCONNECTED” in Wireless Client mode.
- **WAN IP** – Displays the IP address assigned to the WAN port. Displays “0.0.0.0” since there is usually no WAN port connection in Wireless Client mode.
- **Subnet Mask** – Displays the WAN subnet mask.
- **Gateway** – Displays the WAN gateway address.
- **DNS** – Displays a configured DNS address and any DNS address assigned by DHCP.
- **Secondary DNS** – Displays a configured secondary DNS address and any secondary DNS address assigned by DHCP.
- **Connection Type** – Displays the connection type for the WAN port (always DHCP for Wireless Client mode).

LAN – Display system IP settings, as well as DHCP, NAT and firewall status:

- **IP Address** – Displays the LAN port IP address. The IP address can only be configured when in Gateway mode.
- **Subnet Mask** – Displays the LAN port subnet mask.
- **DHCP Server** – Displays the LAN port DHCP server status. Displays “Disable” in Wireless Client mode. In effect, one DHCP client is supported, but the server and address pool cannot be configured.
- **Firewall** – Displays the firewall status. Wireless Client mode does not support any firewall features.

Information – Displays the number of connected clients as well as the unit’s hardware and firmware version numbers:

- **Connected Clients** – Displays the number of connected clients, if any.
- **Runtime Code Version** – Displays the runtime code version.
- **LAN MAC Address** – Displays the LAN MAC address.
- **WAN MAC Address** – Displays WAN MAC address.
- **Hardware Version** – Displays the hardware version number.

System Log

The System Log page displays Personal Mobile Gateway system events.

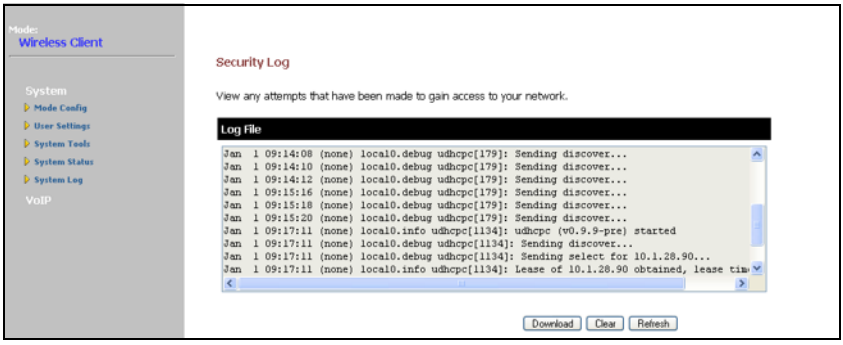

Figure 4-9. Wireless Client System Log

Chapter 5: Access Point Mode

Operating in Access Point mode, the Personal Mobile Gateway provides 802.11b/g connectivity for wireless clients, with robust security options available and QoS support for voice or video traffic.

In Access Point mode, the WAN and LAN ports act like two normal Ethernet switch ports. There are no firewall or NAT features for traffic passing between the WAN and LAN ports or wireless clients. There is also no DHCP server to assign IP addresses to connected clients. A configured DHCP server must exist on the connected local network to provide IP addresses to clients.

To access the web management interface in Access Point mode, connect directly to the unit and used the default IP address, 192.168.2.1. Alternatively, if you want to set an IP address that is compatible with the local network, use Gateway mode to configure a fixed IP address first, then change back to Access Point mode.

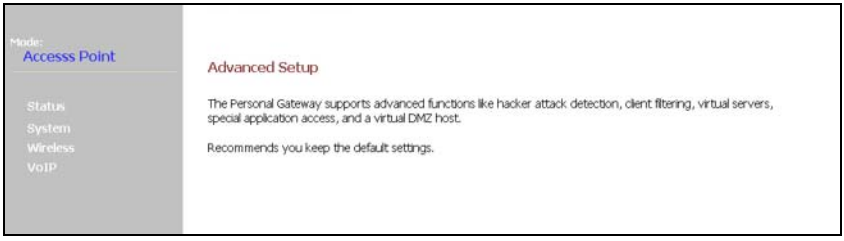

Figure 5-1. Access Point Mode Settings

Access Point mode configuration parameters are described in the relevant chapter of this guide. See the page references below to locate feature information.

Table 5-1. Access Point Configuration Options

Menu	Description	Page
Status	Displays current system information	9-1
System	Configures basic administrative and client access	6-1
Wireless	Configures wireless connectivity	7-1
Setting	Configures the ESSID and other radio parameters	7-1
Security	Configures wireless encryption and authentication	7-4
Wireless QoS	Controls QoS for traffic prioritization	7-7

Table 5-1. Access Point Configuration Options		
Menu	Description	Page
VoIP	Configures VoIP parameters	8-1
SIP Settings	Configures SIP parameters	8-2
Advanced Setting	Configures call forwarding, and DTMF parameters	8-3

Chapter 6: System Settings

The Personal Mobile Gateway's Advanced Setup System settings menu provides the same configuration options in both Gateway and Access Point mode. These settings allow you to change the operating mode, set the system time, configure a management access password, and upgrade the system software.

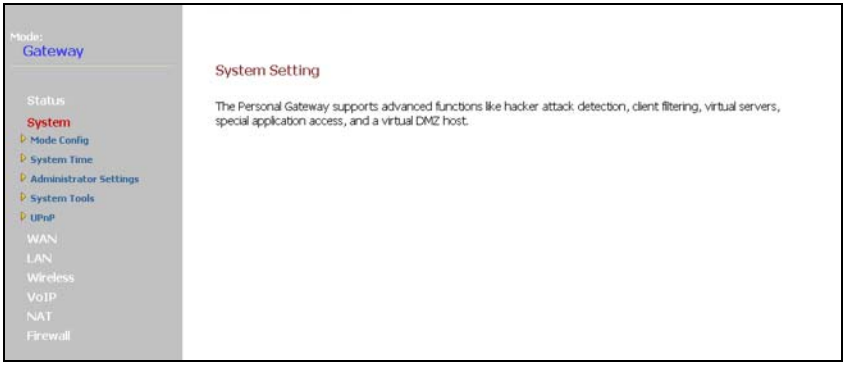

Figure 6-1. System Settings

The information in this chapter is organized to reflect the structure of the System Setting web pages for easy reference. However, it is recommended that you configure a user password as the first step under "Administrator Settings" on page 6-4 to control management access to this device.

The System Setting pages include the following options.

Table 6-1. System Setting

Menu	Description	Page
Mode Config	Allows you to set automatic, or manual configuration	6-2
System Time	Configures the system time settings for syncing with an SNTP server	6-3
Administrator Settings	Configures user password for management access; and remote system management	6-4
Configuration Tools	Allows you to restore the factory default settings, or store your own setting	6-6
UPnP	Provides inter connectivity between Universal Plug and Play devices	6-7

Mode Configuration

The Mode Configuration parameters for the unit can be left at their default settings (Auto). However, manually selecting the manner in which the unit operates allows you to select Access Point mode and configure a greater range of parameters.

When operating in Wireless Client mode, you should set a Service Set Identification (SSID) to identify the wireless network service to which you want to connect. Only clients with the same SSID can associate with a wireless network.

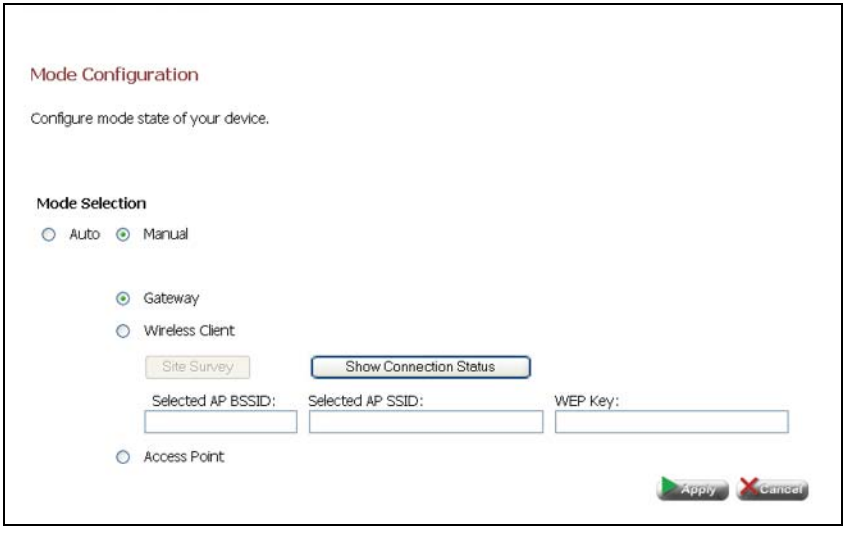

Figure 6-2. Mode Configuration

Mode Selection – Allows you to select Auto configuration (2 operating modes) or Manual configuration (3 operating modes). (Default: Auto)

- **Auto** – The unit automatically selects the operating mode depending on the WAN port status.
  - With no link on the WAN port, the unit starts up in Wireless Client mode.
  - With a link on the WAN port, the unit starts up in Gateway mode.
- **Manual** – Allows you to manually select the mode in which the unit operates:
  - **Gateway** – The unit operates as a secure Internet gateway between a WAN port connection and a wired LAN or wireless devices.
  - **Wireless Client** – The unit operates as a wireless client to connect to nearby access points:
    - **Site Survey** – Performs a wireless scan of the area to detect access points.
    - **Selected AP SSID** – The SSID of the selected access point.
    - **WEP Key** – The WEP key used for the selected access point.

- **Show Connection Status** – Displays the connection status of the unit and the selected access point.

- **Access Point** – The unit operates as an access point that passes data between a wired network and wireless clients.

System Time

The Personal Mobile Gateway uses the Simple Network Time Protocol (SNTP) to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the device enables the system log to record meaningful dates and times for event entries.

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must select your time zone.

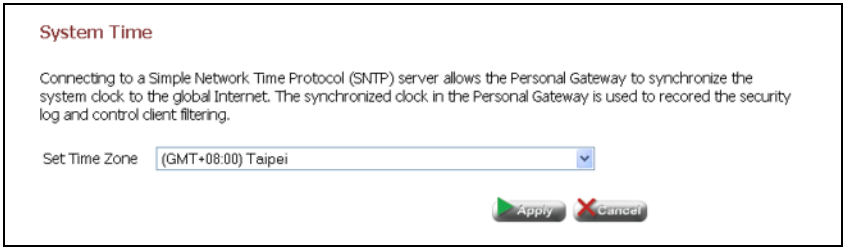

Figure 6-3. System Time

Administrator Settings

The Administrator Settings page allows you to change the default password, set a remote management IP address, and configure email alerts.

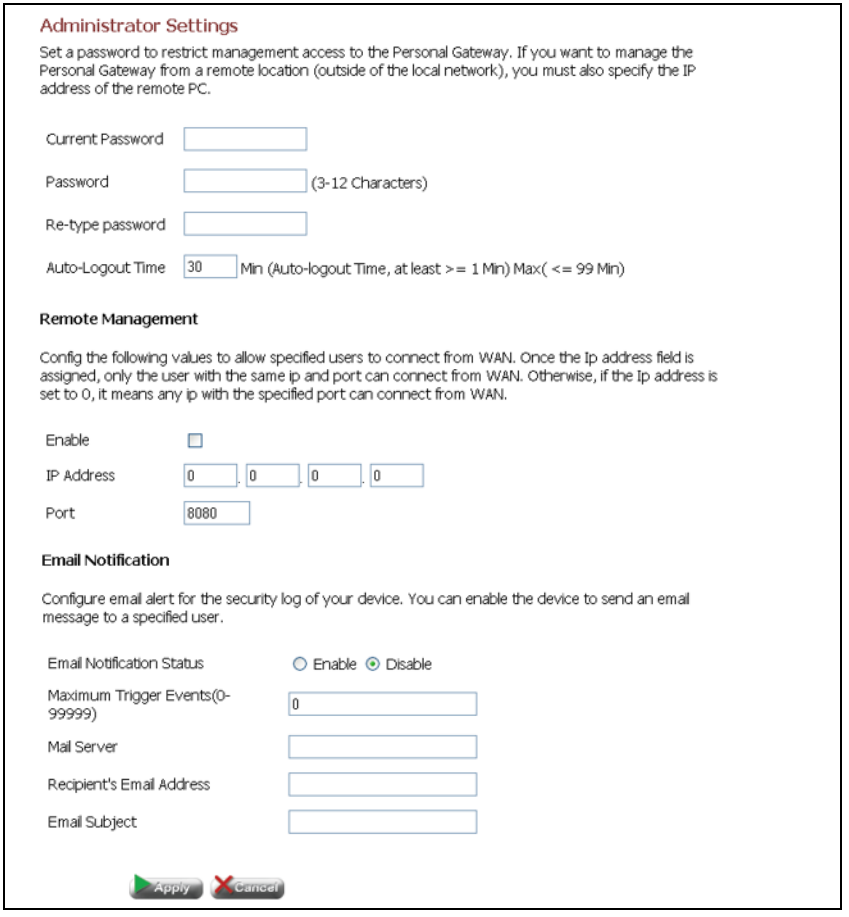

Figure 6-4. Administrator Settings

- **Administrator Settings** – Use the administrator settings to change the password and control the auto-logout time.
  - **Current Password** – Prompts you to enter your current password. (Default: smcadmin)
  - **Password** – Prompts you to enter a new password. (Range: 3~12 characters)
  - **Auto-Logout Time** – The time of non-activity after which the unit terminates a web management session. (Default: 30 minutes; Range: 1~99 minutes)

- **Remote Management** – By default, management access is only available to users on your local network, that is, those connected to the LAN port or wireless clients. However, you can also manage the unit from a remote host through the WAN port by entering a specific IP address or range of addresses that are allowed access.
  - **Enable** – Enables remote management.
  - **IP Address** – Specifies an IP address or address range that can be used for remote management. Note that a “0” in the IP address means that any host is permitted. For example, an IP address specified as 212.120.68.0 means that any host with an IP address in the range 212,120,68.1 to 212,120,68.255 will be able to manage remotely. If you check Enable and leave the IP address as 0.0.0.0, any host can manage the unit remotely.
  - **Port** – Specifies the TCP port to use for remote management. The remote management port must be specified in the address field of your web browser, for example, 212.220.168.20:8080.
- **Email Notification** – Enabling Email alerts for security logging of the unit.
  - **Email Notification Status** – Enables/disables email notifications.
  - **Maximum Trigger Events** – Sends an email message if the number of events exceeds this value.
  - **Mail Server** – The address of the mail server. Specified in the form of mail.something.com.
  - **Recipient’s Email Address** – The email address to send the alert message to. Specified in the form of someone@something.com
  - **Email Subject** – Allows the user to name the subject of the alert message.

Configuration Tools

The Configurations Tools page allows you to upload new runtime code to the unit, restore factory default settings, save and restore the unit's configuration settings, and to reset the unit.

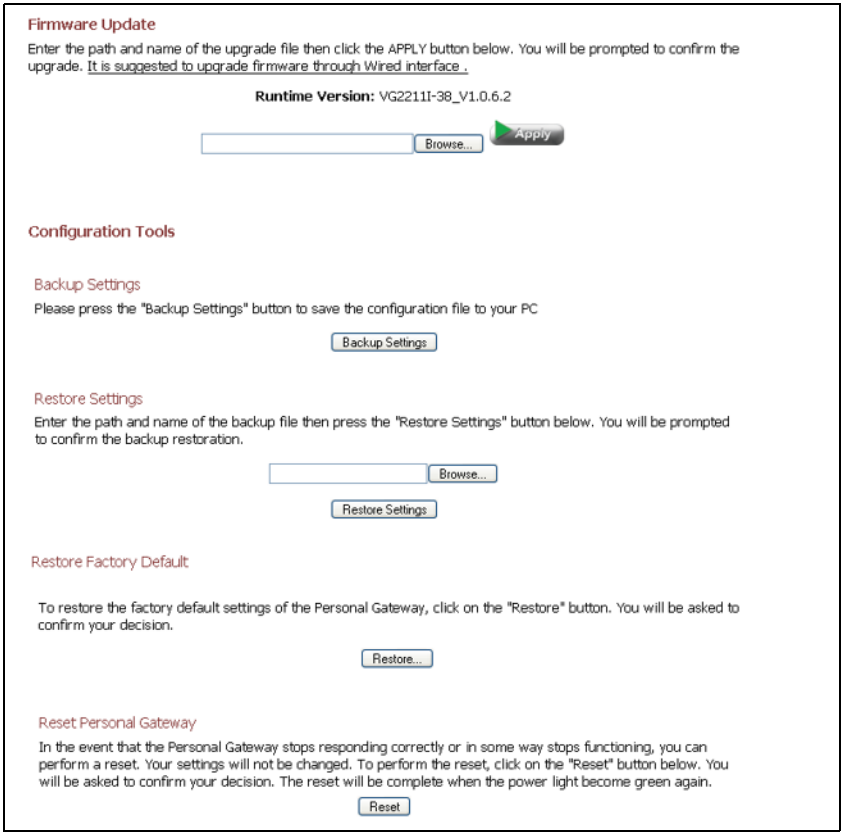

Figure 6-5. Configuration Tools

- **Firmware Update** – Downloads an operation code file from the web management station to the Personal Mobile Gateway using HTTP. Use the Browse button to locate the code file locally on the management station and click Apply to proceed.
- **Configuration Tools:**
  - **Backup Settings** – Saves the current configuration settings to a file on the web management station.
  - **Restore Settings** – Restores a saved configuration file to the unit.
- **Restore Factory Default** – Resets the unit to its factory default settings.
- **Reset Personal Gateway** – Allows the user to reboot the unit.

UPnP Settings

UPnP (Universal Plug and Play Forum) provides inter-connectivity between devices supported by the same standard.

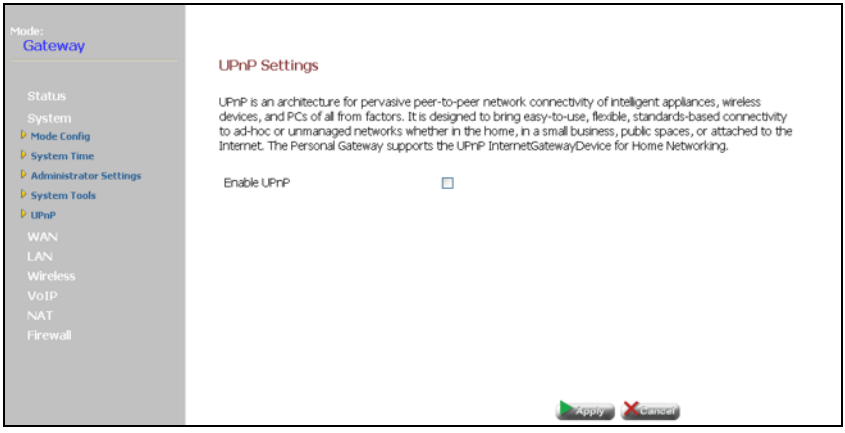

Figure 6-6. UPnP Settings

- **Enable UPnP** – Enables UPnP support for the device.

Chapter 7: Wireless Settings

The Personal Mobile Gateway includes an IEEE 802.11g radio interface for wireless communications. The Wireless set up pages include configuration options for the radio signal characteristics, wireless security, and Quality of Service (QoS) features.

The configuration of wireless settings is available in Gateway Mode and Access Point Mode only.

The Wireless configuration pages include the following options.

Table 7-1. Wireless Settings

Menu	Description	Page
Settings	Allows you configure basic radio parameters	7-1
Security	Configures wireless security features	7-4
Wireless QoS	Configures Quality of Service (QoS) for wireless traffic	7-7

Wireless Settings

From the Wireless menu, click on Settings to configure the unit's radio interface. The unit's radio can operate in three modes, IEEE, 802.11b & g, 802.11g only, and 802.11b only.

The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

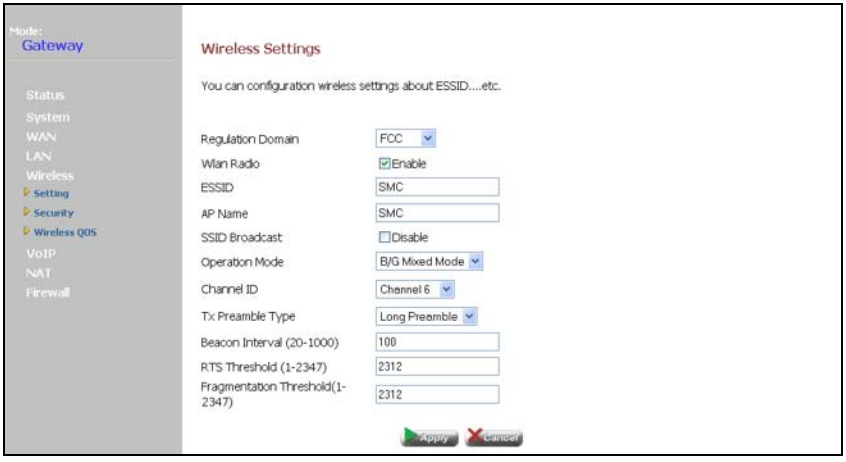

Figure 7-7. Wireless Settings

- **Regulation Domain** – Indicates the unit's regulatory domain setting. Units intended for use in the United States are configured to use only radio channels 1-11 at certain transmit power levels, as defined by FCC (Federal Communications Commission) regulations. Setting this parameter to ETSI (Europe) or Japan allows other appropriate channels and power levels to be used. (Default: FCC)
- **Wlan Radio** – Enables the wireless interface.
- **ESSID** – The Service Set ID. This should be set to the same value as other wireless devices in your network. The SSID is case sensitive and can consist of up to 32 alphanumeric characters. (Default: SMC)
- **AP Name** – A descriptive name given to the unit for identification purposes on the network. (Default: SMC)
- **SSID Broadcast** – Check this box to disable broadcasting the configured ESSID. The Personal Mobile Gateway is configured by default as an "open system," which broadcasts a beacon signal including the configured ESSID. Wireless clients with a configured SSID of "ANY" can read the SSID from the beacon, and automatically set their SSID to allow immediate connection to the Personal Mobile Gateway. When disabled, the Personal Mobile Gateway does not include its ESSID in beacon messages. This provides a basic level of security, since wireless clients must be pre-configured with the ESSID to connect to the Personal Mobile Gateway.
- **Operation Mode** – Selects the operating mode for the 802.11g radio. (Default: B/G Mixed Mode)
  - **B/G Mixed Mode**: Both 802.11b and 802.11g clients can communicate with the unit (up to 54 Mbps).
  - **G Only Mode**: Only 802.11g clients can communicate with the unit (up to 54 Mbps).

- **B Only Mode**: Both 802.11b and 802.11g clients can communicate with the unit, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).

- **Channel ID –** The radio channel used by the unit and its clients to communicate with each other. This channel must be the same on the unit and all of its wireless clients. The available channel settings are limited by local regulations. (Default: 6; Range: 1-14)

Note: If you experience poor performance, you may be encountering interference from another wireless device. Try changing the channel, as this may eliminate interference and increase performance. Channels 1, 6, and 11, as the three non-overlapping channels in the 2.4 GHz range, are preferred. (Default; Auto)

- **Tx Preamble Type –** IEEE 802.11 frames begin with an alternating pattern of 1s and 0s called the preamble, which tells receiving stations that a frame is arriving. This provides time for the receiving station to synchronize to the incoming data stream. This parameter sets the length of the signal preamble that is used at the start of a data transmission. Using a short preamble (96 microseconds) instead of a long preamble (192 microseconds) can increase data throughput on the unit, but requires that all clients can support a short preamble. (Default: Long Preamble)
  - **Short Preamble:** Sets the preamble to short for increased througput.
  - **Long Preamble:** Sets the preamble to long. Using a long preamble ensures the unit can support all 802.11b and 802.11g clients.
  - **Auto:** Sets the preamble according to the capability of clients that are currently asscociated. Uses a short preamble if all associated clients can support it, otherwise a long preamble is used.
- **Beacon Interval (20~1000) –** Sets the interval at which Beacon frames are transmitted from the unit. The Beacon Interval unit is measured in TU, which corresponds to 1024 microseconds. The beacon signals allow wireless clients to maintain contact with the unit. They may also carry power-management information. (Range: 20-1000 TUs; Default: 100 TUs)
- **RTS Threshold (0~2347) –** Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending the data frame. The unit sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the unit that it can start sending data. If the RTS threshold is set to 0, the unit always sends RTS signals. If set to 2347, the unit never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled. Units contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 0-2347 bytes: Default: 2347 bytes)
- **Fragmentation Threshold (0~2347) –** Configures the minimum packet size that can be fragmented when passing through the unit. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization,

try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Range: 256-2346 bytes; Default: 2346 bytes)

Wireless Security

The Personal Mobile Gateway's wireless interface is configured by default as an "open system," which broadcasts a beacon signal including the configured SSID. Wireless clients with a configured SSID of "ANY" can read the SSID from the beacon, and automatically set their SSID to allow immediate connection to the wireless network.

To improve wireless network security, you have to implement two main functions:

- Authentication – It must be verified that clients attempting to connect to the network are authorized users.
- Traffic Encryption – Data passing between the unit and clients must be protected from interception and evesdropping.

For a more secure network, the access point can implement one or a combination of the following security mechanisms:

- Wired Equivalent Privacy (WEP)
- IEEE 802.1X
- Wi-Fi Protected Access (WPA) or WPA2

The security mechanisms that may be employed depend on the level of security required, the network and management resources available, and the software support provided on wireless clients.

To configure wireless security click on Security.

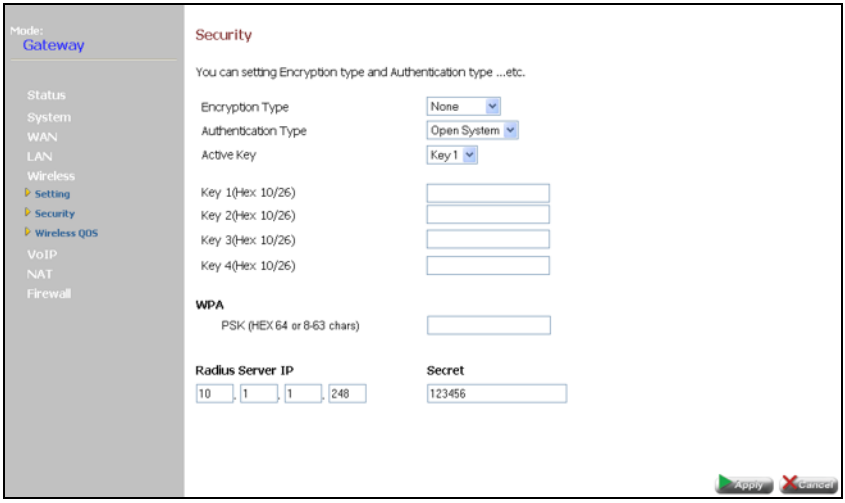

Figure 7-8. Wireless Security

- **Encryption Type** – Selects the data encryption method to use:
  - **None** – No data encryption is used.
  - **Share** – Use a WEP share key for encryption. If you choose to use WEP shared keys, be sure to define at least one static WEP key. Also, be sure that the WEP shared keys are the same for each client in the wireless network.
  - **802.11X** – Use IEEE 802.1X (802.1X) for user authentication and distributing dynamically generated encryption keys. IEEE 802.1X is a standard framework for network access control that uses a RADIUS server on the local network for user authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, usernames and passwords, or other) from the client to the RADIUS server. The unit supports TLS (Transport Layer Security) as its EAP type.
  - **TKIP** – Use Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.
  - **AES** – Use Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.
  - **TKIP/AES** – Use both TKIP and AES keys for encryption. WPA2 defines a transitional mode of operation for networks moving from WPA security to WPA2.

WPA2 Mixed Mode allows both WPA and WPA2 clients to associate to a common SSID interface. In mixed mode, the unicast encryption cipher (TKIP or AES-CCMP) is negotiated for each client.

- **Authentication Type** – The authentication types available depend on the selected encryption type. By first selecting the encryption type, only valid authentication types are then displayed.
  - **Open System** – No user authentication is used.
  - **Shared Key** – Use a WEP share key for authentication. If you choose to use WEP shared keys, be sure to define at least one static WEP key. Also, be sure that the WEP shared keys are the same for each client in the wireless network.
  - **Auto Switch** – Allows support of clients using a static WEP key or no keys.
  - **WPA-TLS** – The WPA enterprise mode that uses IEEE 802.1X and EAP-TLS to authenticate users and to dynamically distribute encryption keys to clients. Either TKIP or AES can be used as the encryption cipher. Requires a RADIUS server to be configured and available in the wired network.
  - **WPA-PSK** – The WPA Pre-shared Key (PSK) mode for small networks that uses a common password string that is manually distributed. Requires the PSK pass-phrase string to be entered. All wireless clients must be configured with the same key to communicate with the unit. Either TKIP or AES can be used as the encryption cipher.
  - **WPA2-TLS** – The WPA2 enterprise mode that uses IEEE 802.1X and EAP-TLS to authenticate users and to dynamically distribute encryption keys to clients. Either TKIP or AES can be used as the encryption cipher. Requires a RADIUS server to be configured and available in the wired network.
  - **WPA2-PSK** – The WPA2 Pre-shared Key (PSK) mode for small networks that uses a common password string that is manually distributed. Requires the PSK pass-phrase string to be entered. All wireless clients must be configured with the same key to communicate with the unit. Either TKIP or AES can be used as the encryption cipher.
- **Active Key / Key 1-4** – If you select Shared Key encryption or authentication, configure at least one shared key by entering 10 (64-bit) or 26 (128-bit) hexadecimal characters (0~9, A~F). Then select the active transmit key to use for encryption.

Note: All wireless devices must be configured with the same Key ID values to communicate with the unit.

- **Radius Server IP** – IP address of the Remote Authentication Dial-in User Service (RADIUS) server. A RADIUS server must be specified for the unit when you implement 802.1X, WPA-TLS, or WPA2-TLS security.
  - **Secret** – A shared text string used to encrypt messages between the unit and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

Wireless QoS

Wireless networks offer an equal opportunity for all devices to transmit data from any type of application. Although this is acceptable for most applications, multimedia applications (with audio and video) are particularly sensitive to the delay and throughput variations that result from this equal opportunity wireless access method. For multimedia applications to run well over a wireless network, a Quality of Service (QoS) mechanism is required to prioritize traffic types and provide an enhanced opportunity wireless access method.

The Personal Mobile Gateway implements QoS using the Wi-Fi Multimedia (WMM) standard. Using WMM, the access point is able to prioritize traffic and optimize performance when multiple applications compete for wireless network bandwidth at the same time. WMM employs techniques that are a subset of the developing IEEE 802.11e QoS standard and it enables the access point to interoperate with both WMM-enabled clients and other devices that may lack any WMM functionality.

Figure 7-9. Wireless QoS Settings

- **Enable QoS –** Check this box to enable WMM QoS on the unit.

Chapter 8: VoIP Settings

VoIP stands for Voice over Internet Protocol. By using VoIP technology you can effectively use the internet to make phone calls. This is done by placing the voice calls on the network by encrypting a voice call into data packets at one end and then decrypting it back into voice calls at the other end. This encryption and decryption is from a analog signal (your voice) into a digital signal (data packets) and then back into an analog signal.

The Pesonal Mobile Gateway uses Session Initiation Protocol (SIP) as the control mechanism that sets up, initiates, and terminates calls between a caller and a called party. The SIP messaging makes use of “Proxy,” “Redirect,” and “Registration” servers to process call requests and find the location of called parties across the Internet. When SIP has set up a call between two parties, the actual voice communication is a direct peer-to-peer connection using the standard Real-Time Protocol (RTP), which streams the encoded voice data across the network.

You can make VoIP calls by using a regular phone with the Personal Mobile Gateway. You can also make VoIP calls from your computer using a VoIP application with a simple microphone and computer speakers. However, using IP telephones or VoIP boxes provides an experience identical to normal telephoning. Many manufacturers are designing phones which are specially meant to work with this technology, called a SIP phone.

The configuration of VoIP settings is available in all operating modes.

The VoIP configuration pages include the following options.

Table 8-1. VoIP Settings

Menu	Description	Page
SIP Settings	Configures SIP parameters	8-2
Advanced Settings	Configures call forwarding and DTMF parameters	8-3

SIP Settings

To enter the SIP configuration page, click SIP Settings.

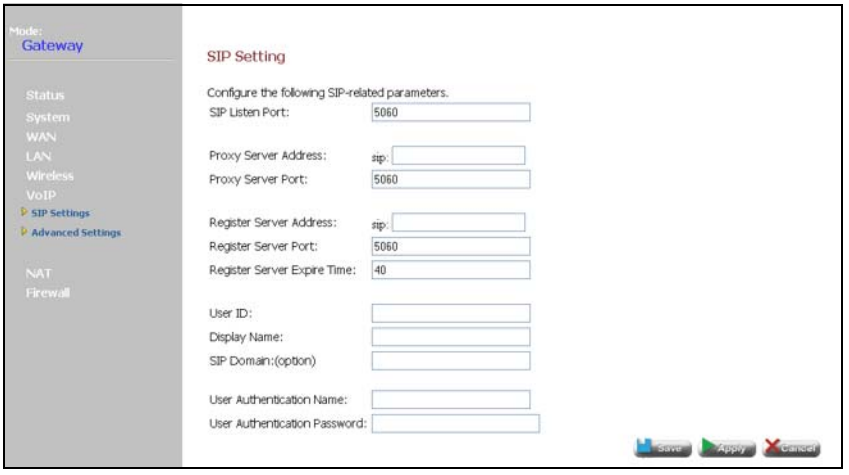

Figure 8-10. VoIP SIP Settings

- **SIP Listen Port** – The port on which the unit will listen and transmit voice-data traffic, as specified by your VoIP provider.
- **Proxy Server Address –** Address of the VoIP service provider proxy server.
- **Proxy Server Port –** The TCP port number used by the VoIP service provider's proxy server.
- **Register Server Address –** IP address of SIP registrar server. A registrar is a server that accepts register requests and places the information it receives in those requests into the location service for the domain it handles.
- **Register Server Port –** The TCP port number used by the VoIP service provider's register server.
- **Register Server Expire Time –** The time the unit waits for a response from the registrar server.
- **SIP Domain –** The address of the SIP domain. This can be in the form of an IP address or a URL, as specified by your VoIP provider.
- **User Authentication Name –** An alphanumeric string that uniquely identifies the user to the SIP server.
- **User Authentication Password –** An alphanumeric string that uniquely identifies the SIP user's permission rights.

VoIP Advanced Settings

To enter the advanced VoIP configuration page, click Advanced Settings.

STUN (Simple Traversal of UDP through NAT (Network Address Translation)) is a protocol for assisting devices behind a NAT firewall or router with their packet routing.

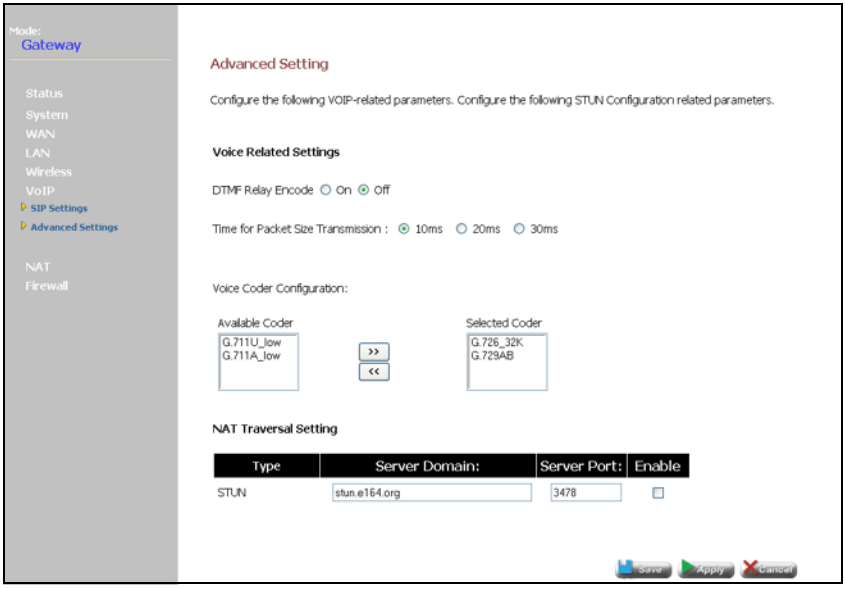

Figure 8-11. VoIP Advanced Settings

- **DTMF Relay Encode** – Enables/disables the sending of dual-tone multi-frequency (touch tone) phone signals over the VoIP connection.
- **Time for Packet Size Transmission** – Specifies a maximum amount of time for transmission of a data packet. (Default: 10ms)
- **Voice Coder Configuration**:
  - **Available Decoder** – Provides a list of available decoders.
  - **Selected Decoder** – Displays selected decoders.
- **NAT Traversal Setting:**
  - **Type** – Defines the NAT traversal setting. (Default: STUN)
  - **Server Domain** – Specifies the domain of the STUN server.
  - **Server Port** – Specifies the port used by the server.
  - **Enable –** Enables the feature

Chapter 9: Status Information

The Personal Mobile Gateway includes status information pages for details on the unit's current settings, event logs, and DHCP clients.

The status information described in this chapter applies to Gateway Mode and Access Point Mode only.

Figure 9-1. Status Menu

The Status pages include the following:

Table 9-1. Status Information

Menu	Description	Page
System Status	Displays WAN and LAN interface information and other system details	9-2
System Log	Displays event log entries	9-3
DHCP Client List	Displays connected DHCP clients that have been assigned IP addresses by the DHCP server	9-4

System Status

The system status page displays connectivity status information for the unit's WAN and LAN interfaces, firmware and hardware version numbers, and the number of clients connected to your network.

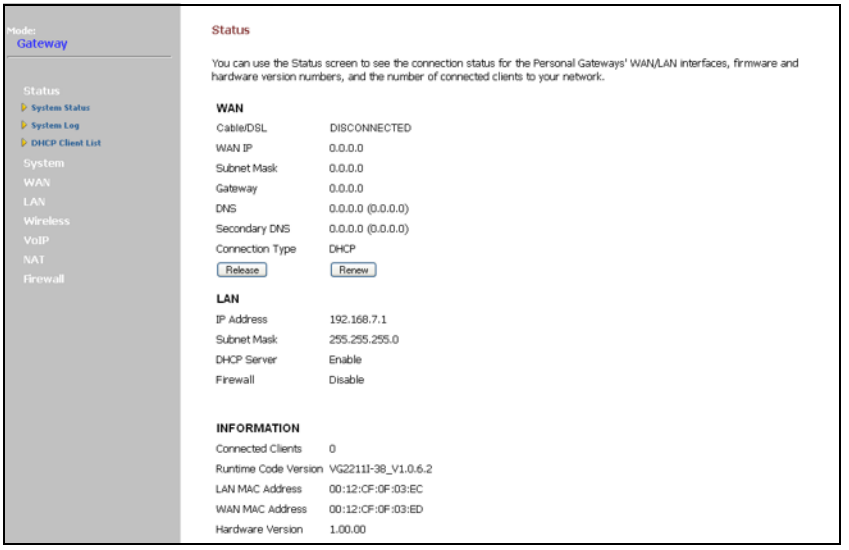

Figure 9-2. System Status Information

WAN – Displays WAN connection type and status:

- **Cable/DSL** – Displays connections status.
- **WAN IP** – Displays the WAN IP address provided by the ISP.
- **Subnet Mask** – Displays the WAN subnet mask.
- **Gateway** – Displays the WAN gateway address.
- **DNS** – Displays the WAN DNS address.
- **Secondary DNS** – Displays the secondary DNS address.
- **Connection Type** – Displays the connection type for the WAN.
- **Release** – Releases the current IP address information.
- **Renew** – Initiates a new DHCP client request for an IP address.

LAN – Display system IP settings, as well as DHCP, NAT and firewall status:

- **IP Address** – Displays the unit's IP address.
- **Subnet Mask** – Displays the subnet mask.
- **DHCP Server** – Displays the DHCP server status.
- **Firewall** – Displays the firewall status.

Information – Displays the number of connected clients as well as the unit's hardware and firmware version numbers:

- **Connected Clients** – Displays the number of connected clients, if any.
- **Runtime Code Version** – Displays the runtime code version.
- **LAN MAC Address** – Displays the LAN MAC address.
- **WAN MAC Address** – Displays WAN MAC address.
- **Hardware Version** – Displays the hardware version number.

System Log

The Security Log page displays Personal Mobile Gateway system events.

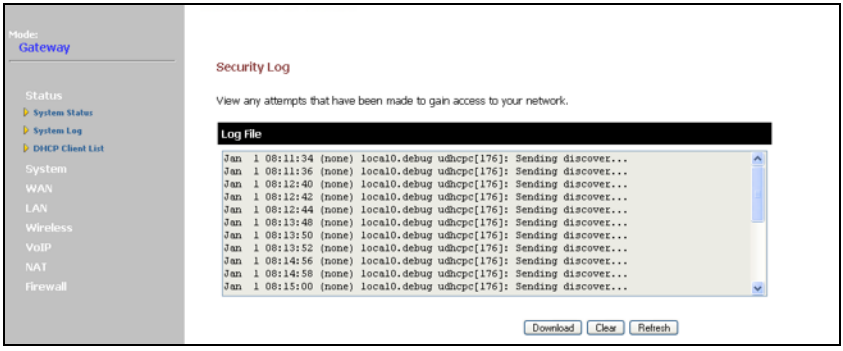

Figure 9-3. System Log

DHCP Client List

The DHCP Client List page allows you to see what devices are currently connected to the unit and have been assigned an IP address by the DHCP server.

Figure 9-4. DHCP Client List

Glossary

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

Access Point

An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

Ad Hoc

A group of computers connected as an independent wireless network, without an access point.

Advanced Encryption Standard (AES)

An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

Authentication

The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Backbone

The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Basic Service Set (BSS)

A set of 802.11-compliant stations and an access point that operate as a fully-connected wireless network.

Beacon

A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

Broadcast Key

Broadcast keys are sent to stations using 802.1X dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance.

Dynamic Host Configuration Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption

Data passing between the access point and clients can use encryption to protect from interception and evesdropping.

Extended Service Set (ESS)

More than one wireless cell can be configured with the same Service Set Identifier to allow mobile users can roam between different cells with the Extended Service Set.

Extensible Authentication Protocol (EAP)

An authentication protocol used to authenticate network clients. EAP is combined with IEEE 802.1X port authentication and a RADIUS authentication server to provide “mutual authentication” between a client, the access point, and the a RADIUS server

Ethernet

A popular local area data communications network, which accepts transmission from computers and terminals.

File Transfer Protocol (FTP)

A TCP/IP protocol used for file transfer.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard used to transmit and receive all data over the World Wide Web.

IEEE 802.11b

A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11g

A wireless standard that supports wireless communications in the 2.4 GHz band using using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.1X

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

Infrastructure

An integrated wireless and wired LAN is called an infrastructure configuration.

Inter Access Point Protocol (IAPP)

A protocol that specifies the wireless signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points.

Local Area Network (LAN)

A group of interconnected computer and support devices.

MAC Address

The physical layer address used to uniquely identify network nodes.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open System

A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

Orthogonal Frequency Division Multiplexing (ODFM)

OFDM/ allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

Power over Ethernet (PoE)

A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in the locating of access point's and network devices, and significantly decreased installation costs.

RADIUS

A logon authentication protocol that uses software running on a central server to control access to the network.

Roaming

A wireless LAN mobile user moves around an ESS and maintains a continuous connection to the infrastructure network.

RTS Threshold

Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem.” If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

Service Set Identifier (SSID)

An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

Session Key

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Shared Key

A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Temporal Key Integrity Protocol (TKIP)

A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Wi-Fi Protected Access

WPA employs 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

Wired Equivalent Privacy (WEP)

WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA Pre-shared Key (PSK)

PSK can be used for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access.

Index

Index

Model Number: SMCWTVG
Pub. Number: 149xxxxxxxxxxx, E012006-R01