Fixed Global IP

If you are connecting through a fixed (or static) IP address, perform these steps:

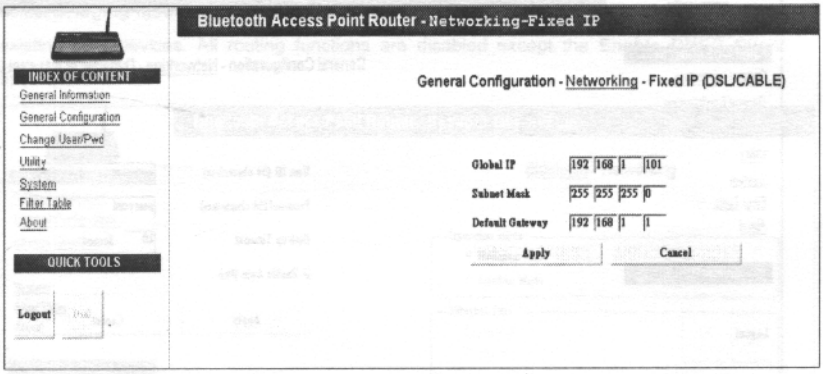

Figure 3-8

1. On the second block, select **Fixed-IP** and click the **Advanced** button. The **Fixed-IP** page appears as shown in Figure 3-8.
2. Specify the global IP address in the **Global IP** field, enter the default gateway address, and subnet mask in the following fields respectively.
3. Click the **Apply** button to save the settings and the system will automatically return to the **Networking** page.

DHCP Server

A DHCP (Dynamic Host Configuration Protocol) server automatically assigns IP addresses to each client on its network. This function is available in Routing Mode only.

- **DHCP Server -** Select the **Enable DHCP Server** option in the third box to enable the Router's DHCP server function.
- **Starting IP Address -** Click the **Advanced** button on the third block and you will enter the **DHCP Serv** page as shown in Figure 3-9. Enter the starting value (2 ~ 254) in the **Starting IP** field for the DHCP server to start with when issuing IP addresses.
- **Ending IP Address -** Enter the ending value (2 ~ 254) in the Ending IP field for the DHCP server. It is required that no more than 253 IPs are available.

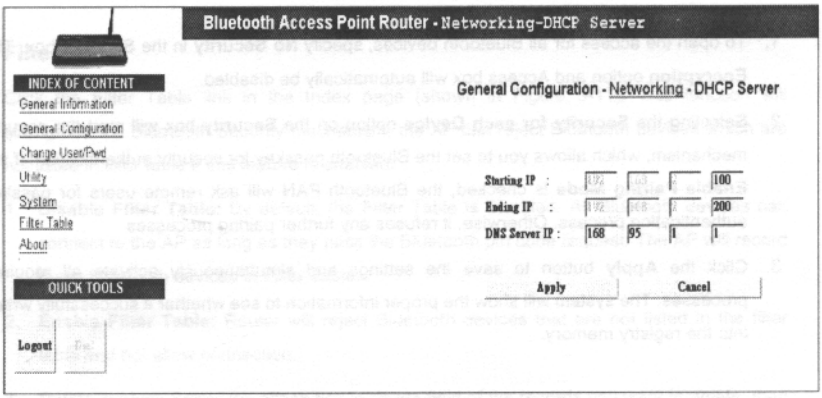

Figure 3-9

Bluetooth Security

The Bluetooth wireless connection provides a security mechanism, which enables you to keep unfriendly users from accessing the wireless network. If the security mechanism is on, the remote users need to pass the **Key** agreed by both the Bluetooth PAN and the remote user.

Click **General Configuration** link in the **Index** page and change to **Bluetooth** page as shown in Figure 3-10.

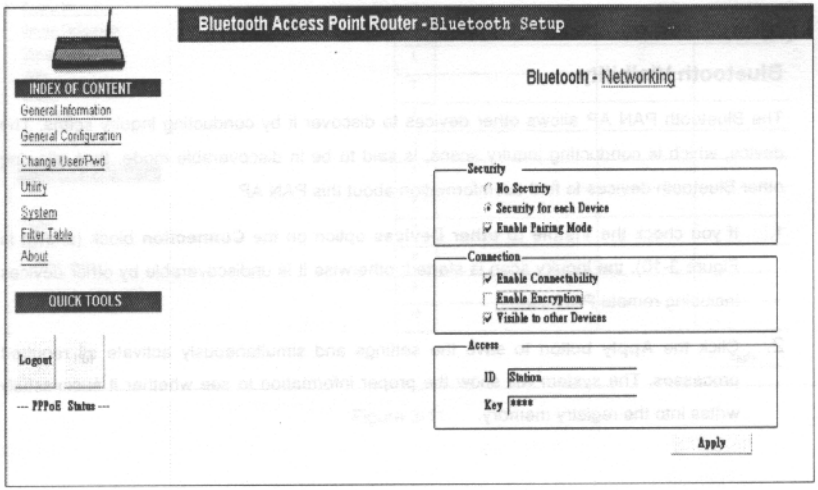

Figure 3-10

1. To open the access for all Bluetooth devices, specify **No Security** in the **Security** box. The **Encryption** option and Access box will automatically be disabled.
2. Selecting the **Security for each Device** option on the **Security** box will start the security mechanism, which allows you to set the Bluetooth passkey for security authentication. If the **Enable Pairing Mode** is checked, the Bluetooth PAN will ask remote users for passkey authentication process. Otherwise, it refuses any further pairing processes
3. Click the **Apply** button to save the settings and simultaneously activate all required processes. The system will show the proper information to see whether it successfully writes into the registry memory.

Bluetooth Connectability

1. You can check the **Enable Connectability** option in the **Connection** box (shown in Figure 3-10) to enable the paging process, or clear the option to prevent other devices from making a connection to it.
2. Click the **Apply** button to save the settings and simultaneously activate all required processes. The system will show the proper information to see whether it successfully writes into the registry memory.

Note: This function can't be disabled in Routing Mode.

Bluetooth Visibility

The Bluetooth PAN AP allows other devices to discover it by conducting inquiry scans. The device, which is conducting inquiry scans, is said to be in discoverable mode, thus allowing other Bluetooth devices to find out information about this PAN AP.

1. If you check the **Visible to other Devices** option on the **Connection** block (shown in Figure 3-10), the inquiry scan is started; otherwise it is undiscoverable by other devices including remote PAN users.
2. Click the **Apply** button to save the settings and simultaneously activate all required processes. The system will show the proper information to see whether it successfully writes into the registry memory.

Filter Table

Click the Filter Table link in the Index page (shown in Figure 3-11). This function will strengthen the Bluetooth Security mechanism; the AP can reject Bluetooth devices which are not listed in filter table if this feature is enabled.

1. **Disable Filter Table:** By default, the Filter Table is disabled. All Bluetooth devices can connect to the AP as long as they pass the Bluetooth pin code request. The AP will record these Bluetooth devices in Filter Table.
2. **Enable Filter Table:** Router will reject Bluetooth devices that are not listed in the filter table and not allow connection.
3. **Delete record:** Select the check box in delete field of the records you want to delete, then click the **Delete** button. The records will be removed from the Filter Table.
4. There can be a maximum of 50 records in this table.
5. Click the **Apply** button to save the settings and simultaneously activate all required processes. The system will show the proper information to see whether it successfully writes into the registry memory.

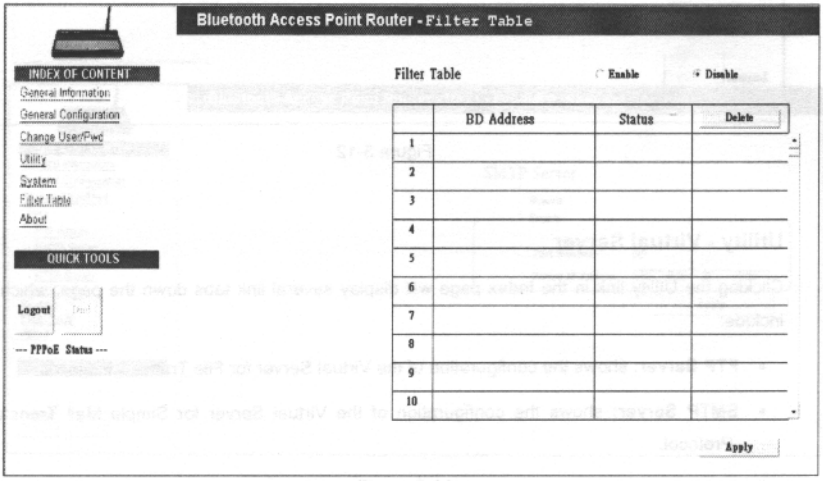

Figure 3-11

System

Click the System link in the Index page (shown in Figure 3-12) to reboot the AP or restore to the default settings.

1. **Reboot:** Click the **Reboot** button to re-boot the device.
2. **Restore to Bridging Mode default settings:** Select **Bridge,** then click the **Restore** button. The system will restore all other settings to factory default settings of Bridging Mode.
3. **Restore to Routing Mode default settings:** Select **Routing,** then click the **Restore** button. The system will restore all other settings to factory default settings of Routing Mode.

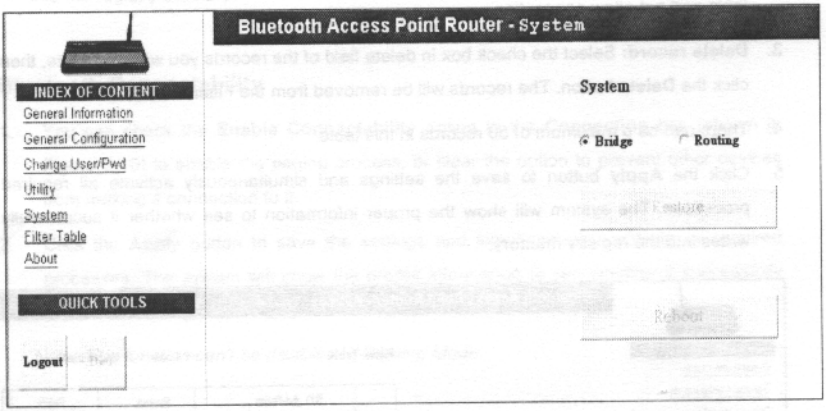

Figure 3-12

Utility - Virtual Server

Clicking the Utility link in the Index page will display several link tabs down the page, which include:

- **FTP Server:** shows the configuration of the Virtual Server for File Transfer Protocol.
- **SMTP Server:** shows the configuration of the Virtual Server for Simple Mail Transfer Protocol.
- **POP3 Server:** shows the configuration of the Virtual Server for Post Office Protocol
- **HTTP Server:** shows the configuration of the Virtual Server for Hypertext Transfer Protocol
- **MISC:** shows the default setting for other available uses of the Virtual Server.

As shown in Figures 3-13 ~ 3-17, clicking each server tab shows the default setting for the virtual FTP server. To disable the function and to prevent outside Internet access to the server, check the **Disable** option and click the **Apply** button to save the settings and simultaneously activate the required process. The system will show the proper information to see whether it successfully writes into the registry memory.

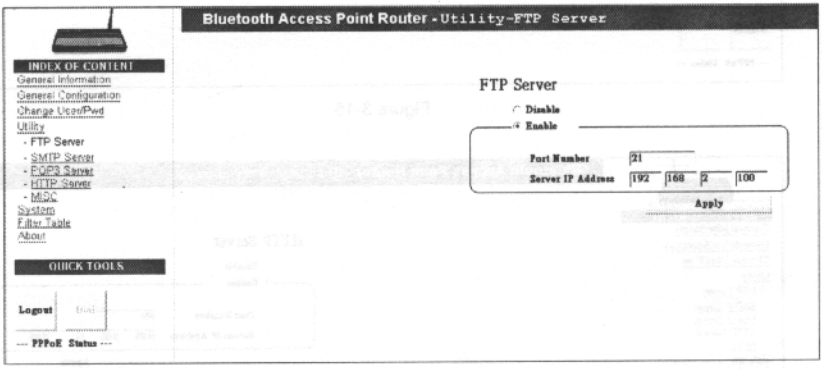

Figure 3-13

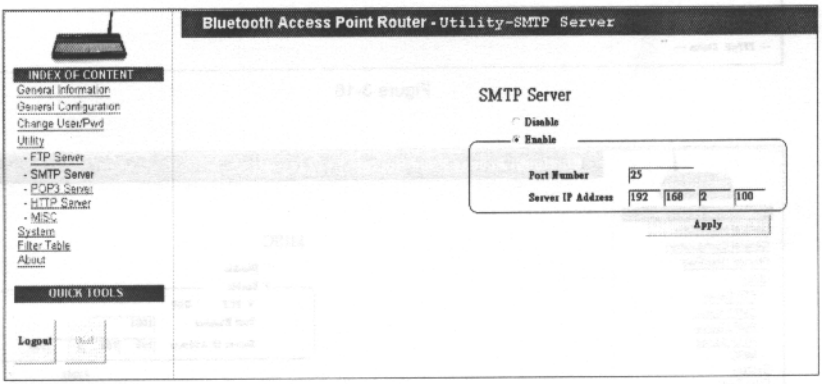

Figure 3-14

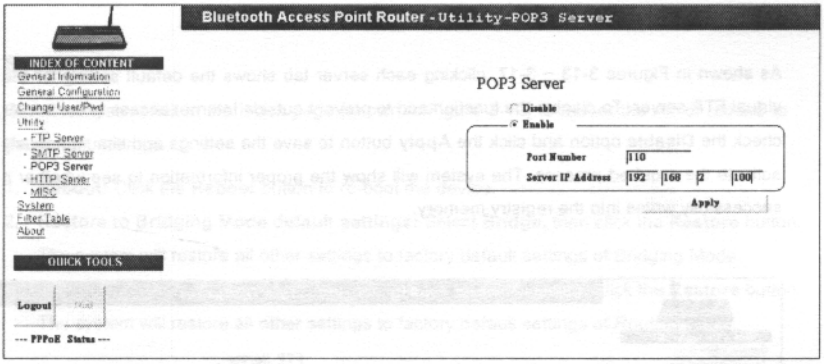

Figure 3-15

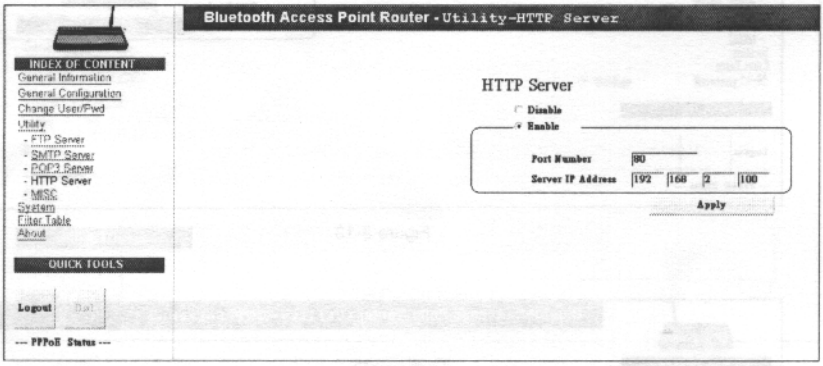

Figure 3-16

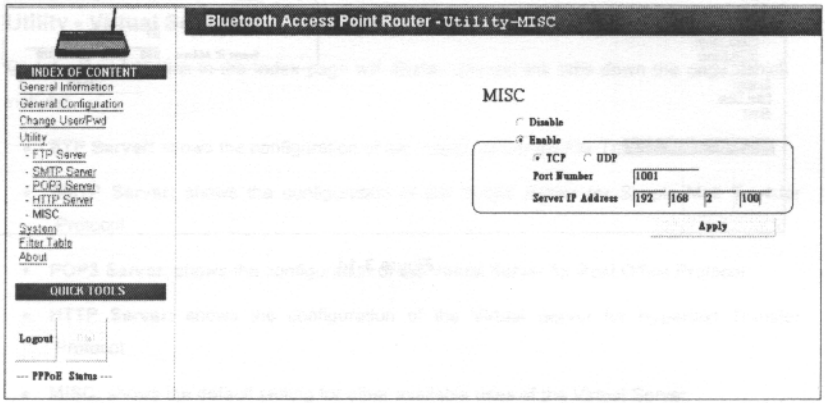

Figure 3-17