4.5 Wireless LAN (2.4G) Configuration

The Wireless Broadband Router implements Access Point capability which connects wireless clients to a wired LAN. It allows wireless nodes to access network resources and share the broadband Internet connection. With the default values, the router (Access Point) can be easily associated by a wireless client. We suggest that you customize the wireless settings to prevent unauthorized association.

▶ Basic Configuration

Access Point Name: The name used for identifying the Access Point.

SSID: Service Set ID. It uniquely identifies a logical network domain name of your WLAN.

Do not broadcast SSID: If this option is disabled, the AP (also referred to as an “open” AP) will periodically broadcast its SSID to allow the wireless clients to recognize their presence. However, this creates a security hole since any wireless station with SSID set to “any” or got the broadcast may associate to your AP. It is recommended to enable this option to have your AP only accept stations whose SSIDs are the same as this AP’s.

BSSID: The MAC address of the AP.

Channel ID: The radio frequency used for communication. Select a channel out of the available cannels or use the default, **Auto**, to have the AP automatically scan and select a channel when it starts up.

▶ Advanced Configuration

We suggest you not to modify the Advanced parameters unless specific requirement is required. The parameters are described as below.

Beacon Interval: Defines the periodic interval at which the Access Point sends out a beacon.

RTS Threshold: Request to send threshold. It specifies the packet size beyond which the AP invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism.

Fragment Threshold: It determines whether packets will be fragmented and at what size. On an 802.11 wireless LAN, packets exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. On the other hand, packets smaller than the specified fragmentation threshold value are not fragmented.

DTIM Interval: Specifies the Deferred Traffic Indicator Map (DTIM) period. This value determines at which interval the AP will send its broadcast traffic. The default value is 1.

Data Rate: The default setting, **Auto**, allows the AP to automatically use the fastest possible data rate. Selecting a specific rate forces the AP to transmit at a particular speed.

Operational Mode: This item allows you to choose from these communication options:

- **Auto:** Both 802.11g draft and 802.11b clietns can communicate with this AP. The data rate will be automatically adjusted.
- **802.11g:** Only 802.11g wirless clients can communicate with the AP.
- **802.11b:** Only 802.11b clients can communicate with the AP.

4.6 Wireless LAN Security

When implementing a wireless network, it is important to secure the data transmitted over the wireless network. This Wireless Broadband Router provides a couple of approaches to protect your wireless network: WEP, MAC address access control and 802.1x.

▶ 802.1x

The 802.1X standard is designed to enhance the security of a wireless network. For more information on 802.1x, please refer to the appendix “A Implementing 802.1x”.

▶ WEP

WEP Mode: WEP (Wired Equivalent Privacy) is an authentication algorithm which encrypts your data and protects your Wireless LAN against eavesdropping.

WEP is disabled by default. If you want to protect your data when it is transferred from one station to another, you should enable this security option. For security concern, we strongly suggest you enable WEP function.

To enable WEP, select **64 bits** or **128 bits** option as the encryption algorithm. The higher the bit number, the greater the complexity and the security of the encryption.

Authentication Mode: Authentication is a process in which the AP validates if wireless clients are qualified to access the AP’s service. This happens **prior to** any wireless client can associate to an AP. The IEEE 802.11 defines two types of algorithms in authentication: the “Open System” and “Shared Key”.

- **Open System:** The authentication is done through a pseudo process, accepting all kinds of requests, mainly used in cases where connectivity is more important than security. If WEP is disabled, the Authentication Mode is set to **Open**.
- **Shared Key :** Utilizes WEP capability to further verify if a wireless client is authorized to share this AP’s resource. If the client has the wrong key or no key, it will fail authentication and will not be allowed to associate with the AP.
  This option is only available when WEP is enabled and you need to configure the WEP keys used for authentication and data encryptiong.

WEP Key Type: Select **ASCII** or **Hexadecimal** as the key format you want to use.

WEP Keys: Enter one to four WEP keys in either ASCII or Hexadecimal format as specified. The key length depends on the encryption algorithm (64 bits or 128 bits) you selected.

Note that when using Hexadecimal format, only digits 0-9 and letters A-F, a-f are allowed. Valid key length for each encryption type is as below:

	ASCII Format	HEX Format
64 Bit	5 ASCII characters	10 hexadecimal digits
128 Bit	13 ASCII characters	26 hexadecimal digits

Specifing a default key to encrypt outging data

Aside from entering your WEP keys, you should select one of the entered keys to encrypt the data before being transmitted. The AP always transmits data encrypted using this WEP Key. The key number (1,2,3,4) is also transmitted. The receiving station will use the key number to determine which key to use for decryption. If the key value does not match with the transmitting station, the decryption will fail. To ensure successful decryption, have your wireless stations set identical key tables.

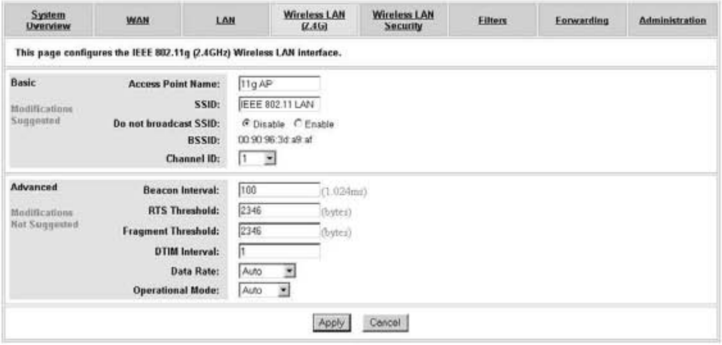
Note: All wireless stations must use identical encryption algorithm level and key values (same key position in its key table) to ensure successful data transmission.

▶ Access Control

MAC Address Access Control: This AP has the capability to control the wireless client access based on the MAC address of a wireless client. We offer you the flexibility to customize your own control policy based on these options:

- **Allow:** If selected, only the wireless client whose MAC address is in the **MAC Address List** is allowed to access this AP.
- **Deny:** If selected, only the wireless client whose MAC address is in the list cannot access this AP. Others clients are granted access.
- **Disable:** No access control. All the clients are allowed to access this AP.

When entering MAC address in the list, up to 12 MAC entries are allowed.



This page configures the IEEE 802.11g (2.4GHz) Wireless LAN interface.

Basic

Modifications Suggested

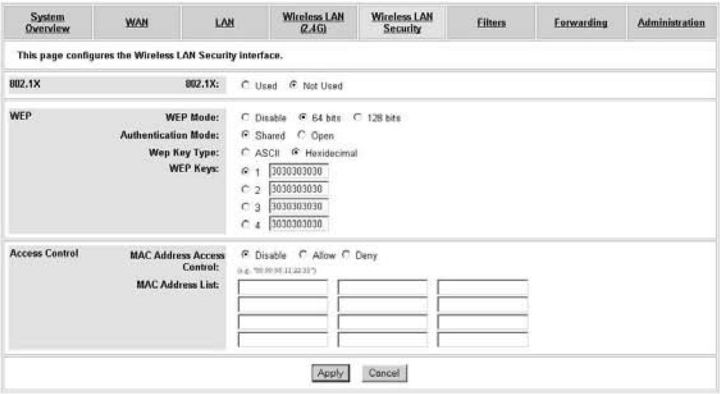
- Access Point Name: 11g AP
- SSID: IEEE 802.11 LAN
- Do not broadcast SSID: ● Disable ○ Enable
- BSSID: 00:90:96:3d:a9:af
- Channel ID: 1

Advanced

Modifications Not Suggested

- Beacon Interval: 100 (1.024ms)
- RTS Threshold: 2346 (bytes)
- Fragment Threshold: 2346 (bytes)
- DTIM Interval: 1
- Data Rate: Auto
- Operational Mode: Auto

Figure 4-13 Wireless LAN Configuration



This page configures the Wireless LAN Security interface.

802.1X

- 802.1X: ○ Used ● Not Used

WEP

- WEP Mode: ○ Disable ● 64 bits ○ 128 bits
- Authentication Mode: ● Shared ○ Open
- Wep Key Type: ○ ASCII ● Hexidecimal
- WEP Keys:
  - ● 1 3030303030
  - ○ 2 3030303030
  - ○ 3 3030303030
  - ○ 4 3030303030

Access Control

- MAC Address Access Control: ● Disable ○ Allow ○ Deny (e.g. "00:00:00:11:22:33")
- MAC Address List:

Figure 4-14 Wireless LAN Security Configuration

4.6 Filters

When your Wireless Broadband Router operates as a router, the built-in NAT function provides your LAN with the Internet access via the single public IP of the WAN port. That means all network devices are allowed to access various Internet service. Under this circumstance, network security becomes an important issue and system administrators may need to build access control to protect the network.

The filter feature serves as a basic firewall security measure for your network. When filter function is enabled, the Wireless Broadband Router inspects all data packets arrive from LAN side and determines if packets are allowed to pass through the WAN port depending on whether packets match your filter rules and whether your filter type is Listed Pass or Listed Block.

In addition to filter settings, the Filters page also allows to configure other firewall settings, including WAN Management, WAN Port Ping Reply and Report Log to TFTP Server.

Specifing Your IP Filter Rules

If you are going to specify your filter rules, follow the procedures below:

1. In the **Firewall** item, select the **Enable** option.
2. In the **Filter Type** item, select the action (**Listed Pass** or **Listed Block**) to be performed on the IP packets matching your filter rules.
3. In the four filter types, select whether to enable or disable each filter.
4. If a filter is enabled, enter the criteria in provided fields. Click **More** to add more criteria if required. See next section for more information.
5. Click **Apply** to commit your changes.

Filter Types

When setting up filter rules, you can define the Filter rules based on the LAN machine's MAC address, IP address or the protocol type of the data packet. Each filter type is described as below.

Note: Based on OSI reference model, MAC Filters demand higher priority than IP Filters while IP Filters higher than Port Filters.

MAC Filters: The MAC address of the LAN machine from which packets are allowed (or prohibited) to pass through the WAN port. Up to 12 entries are allowed.

IP Filters: The range of IP addresses of the LAN machines from which packets are allowed (or prohibited) to pass through the WAN port. You may enter the same address in both (Start and End) fields to define a single IP address. Up to 5 entries are allowed.

TCP Port Filters: Allows (or prohibits) certain LAN machine to use TCP based service in the specified port range through the WAN port. Up to 12 entries are allowed.

For example, to allow (or prohibit) local PC 192.168.1.210 to use FTP service (using TCP port 21):

IP Address	Start	End
192.168.1.210	20	21

UDP Port Filters: This field allows you to allow (or prohibit) certain LAN machine to use UDP based service in the specified port range through the WAN port. Up to 12 entries are allowed.

For example, to allow (or prohibit) local PC 192.168.1.210 to use ping service (using UDP port 53):

IP Address	Start	End
192.168.1.210	53	53

Filter Scenario of the Wireles Broadband Router

When setting up your firewall policy, note the filter scenario used by the router:

When Filter Type is ***Listed Block***:

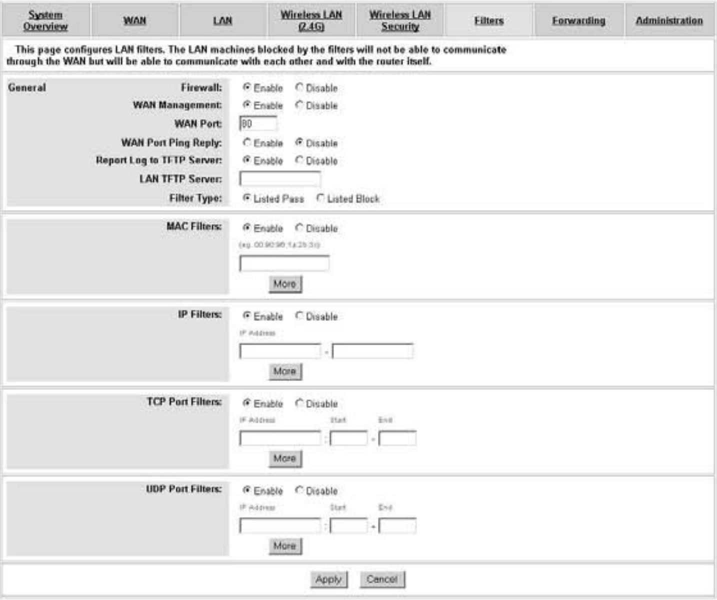
If all the filters are ***disabled***: No filter rule is specified to block any packet. All packets can pass through the WAN port. (Defaults)

If any filter is ***enabled***: only the packets matching the specified rule are blocked; other packets can pass through the WAN port.

When Filter Type is ***Listed Pass***:

If all the filters are ***disabled***: No filter rule is specified to allow any packet to pass. All packets are blocked.

If any filter is ***enabled***: Only the packets matching the specified rule can pass; other packets are blocked.



This page configures LAN filters. The LAN machines blocked by the filters will not be able to communicate through the WAN but will be able to communicate with each other and with the router itself.

General

Firewall: ● Enable ○ Disable
WAN Management: ● Enable ○ Disable
WAN Port: 80
WAN Port Ping Reply: ○ Enable ● Disable
Report Log to TFTP Server: ● Enable ○ Disable
LAN TFTP Server:
Filter Type: ● Listed Pass ○ Listed Block

MAC Filters: ● Enable ○ Disable
(eg. 00:90:96:1a:25:3i)

IP Filters: ● Enable ○ Disable
IP Address

TCP Port Filters: ● Enable ○ Disable
IP Address Start End

UDP Port Filters: ● Enable ○ Disable
IP Address Start End

Figure 4-15 Filters

Viewing Filter Log

When filter feature is enabled, the router will keep a record of the packets discarded. To view the firewall activity log, go to **System Overview** > **Firewall** > **Activity Log** and click the **Show Log** button. Filter activity log is displayed in a separate window with a maximum of 32 entries. Clicking the **Update** button allows to refresh the log with newly reported data. The log types are defined as below:

Type	Description
1	Blocked packets, from WAN side, by DoS (Deny of Service) protection mechanism.
2	Blocked packets, from LAN side, by MAC/IP/TCP/UDP filter.

Other Firewall Settings

WAN Management: Available only when Firewall is enabled. If available, this item is disabled by default that rejects any external access from the WAN port. If this option is enabled, a **WAN Port** filed is displayed with the default value 80. If required, you may enter another port number used by the external WAN access.

If WAN Management is enabled using a non-80 port, the router's HTTP service (Web Configuration Utility) will be accessible via the router's WAN port IP address following by a colon and the non-80 port:

http://<WAN IP address>:<non-80 port>

For example, if *1234* is entered, a remote user can access and configure the router at *http://203.1.2.3:1234* where 203.1.2.3 indicates the WAN port's IP address.

If WAN Management is enabled using standard port 80, no suffix is required.

If WAN Management is enabled using port 80, your publicly accessible Web server (if any) on LAN side should use a non-80

HTTP port. And you need to use the Forwarding feature to shift external HTTP requests to the non-80 port number used by the Web server on LAN side.

WAN Port Ping Reply: Available only when Firewall is enabled. If available, this setting determines if an external host will get reply when trying to ping the IP address of your WAN port. It's disabled by default.

Report Log to TFTP Server: Available only when Firewall is enabled. If available, it specifies whether to report firewall event log to your TFTP server. If enabled, a **LAN TFTP Server** field is present for you to specify the IP address of the TFTP server. All the filter logs are sent to TFTP server although only 32 entries are displayed in **Show Log** window (see **System Overview** page).

4.7 Forwarding

This page allows you to configure the Forwarding and DMZ (De-Militarized Zone) features. Unlike Filter which governs outgoing traffic, Forwarding is used to provide external access to your local machines. This is commonly used when you have publicly accessible virtual servers on your local network.

By default, forwarding entry is empty and any external access to your LAN is blocked. Once you define a forwarding entry, incoming packets (identified by its port number) that match your Forwarding criteria will be forwarded to the port range of the specified local machine. Otherwise packets are blocked. Forwarding serves as a measure of security that protects your network from hazardous packets.

However, if you designate a DMZ sever, incoming packets that do not match the forwarding criteria will be redirected to the DMZ IP address. That is, forwarding demands a higher priority than DMZ.

Setting Up Forwarding Entries

To set up your forwarding entries, enter these fields:

DMZ IP Address: DMZ setting allows a local machine to be exposed to the Internet. If you specify a DMZ host here, the incoming packets containing no port information specified in the Forwarding table are forwarded to the DMZ host.

TCP Port Forwards: In the first **Start** and **End** fields, define the port range for the incoming TCP service you want to forward. In the **IP Address** filed, enter the IP address of the virtual server to which packets are forwarded. The **Start/End** fields on right side define the port range for the TCP service on the virtual server.

For example, you have a virtual server 192.168.1.210 running FTP service and you allow external access by the setting below:

Start	End	IP Address	Start	End
20	21	192.168.1.210	20	21

UDP Port Forwards: The configuration is the same as setting TCP Port Forwards, only that the entry applies to UDP service.

When the router gets outside TCP/UDP requests destined for the WAN port, it determines whether the services are allowed according to your forwarding settings. For example, if you do not specify FTP virtual service in Forwarding table, incoming FTP requests (identified by port number in packets) are blocked or otherwise sent to DMZ host (if specified). On the other hand, if an FTP forwarding entry has been set up, the FTP requests will be able to be forwarded to the specified machine.

If you have a Web server on your network...

If you enable WAN Management (i.e., allow external access from the WAN port, see "4.6 Filters") and want to designate another Web server on your local network, take either of the procedures below to avoid port confliction:

Option 1: In Filters page, with **WAN Management** enabled, enter a port number other than 80 (for example, 1234) and reserve the number 80 for your Web server.

If any external host wants to access your Web management server through the WAN port, it should use the address below:

http://*204.71.200.143* (i.e., the WAN IP address):1234

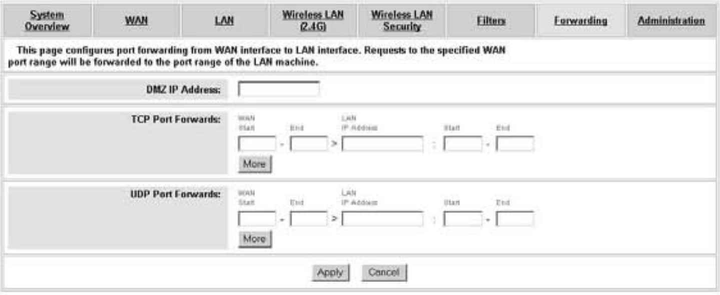
Option 2: Have **WAN Management** to use the standard port number 80 and your Web server (e.g., 192.168.1.4) to use another port number (e.g., 8080). In this case, you need to shift the incoming HTTP request (destined for local Web server) to port 8080 of your Web server, the forwarding entry may look like this:

Start	End	IP Address	Start	End
8080	8080	192.168.1.4	8080	8080

With the settings above, an external host trying to access your local Web server should use the address like this:

http://*204.71.200.143* (i.e., the WAN IP address):8080

If you do not enter the suffix ":8080", the external host's packets will contain the standard port number 80 and the router will not forward the packets since no forwarding entry matches. As a result, if a WAN computer tries to access the LAN's Web server, it will turn to access the Web service on the WAN port, i.e., the Web Configuration Utility of the router instead.



This page configures port forwarding from WAN interface to LAN interface. Requests to the specified WAN port range will be forwarded to the port range of the LAN machine.

Figure 4-16 Forwarding

4.8 Administration

▶ System Clock Configuration

Network administrators may want to synchronize date and time among network devices. This can be done by synchronizing the local clock to an available NTP server or manually specifying the date and time in this router for your network.

Option 1: Using an existing NTP server.

1. In **Set by** item, enable the **Network Time Protocol** option.
2. In **NTP Server** field, enter the IP address of the NTP server.
3. In **Update Interval** item, select your update interval as **1**, **2** or **7 days**.
4. In **Time Zone** field, select a time zone according your geographic location.

Option 2: Specifying the router as your network NTP server.

1. In **Set by** item, enable the **Manual Setup** option.
2. Manually enter the date and time information in respective fields.

▶ Management Setup

Username&Password: For administration security, specify required **User Name** and **Password** and re-enter password in corresponding field for confirmation. This setting limits your Web-based manager access to users with the correct credentials. By default, the user name is empty and the password is **admin**.

▶ Firmware Upgrade

This option allows you to upgrade the Wireless Broadband Router with new firmware. After upgrading, your customized configuration will still exist and not reset to the factory defaults. To upgrade, download required firmware file to your host PC and follow the steps below:

1. In the **Locate New Firmware** field, click **Browse** to locate the firmware file.
2. Click the **Upgrade** button to start upgrade and then wait for a few minutes as the utility prompts. You will return to the Administration page while the process is complete.

Note: Do not interrupt the upgrade process otherwise it might cause damage to your Wireless Broadband Router.

After upgrade, you can see the new firmware version in **Current Firmware version** field.

▶ User Configurations

Save Current Configurations: Allows you to save your customized settings to the device. Once your router is properly configured, you may wish to save current settings. The saved settings can be retrieved easily if required, even after you reload factory defaults.

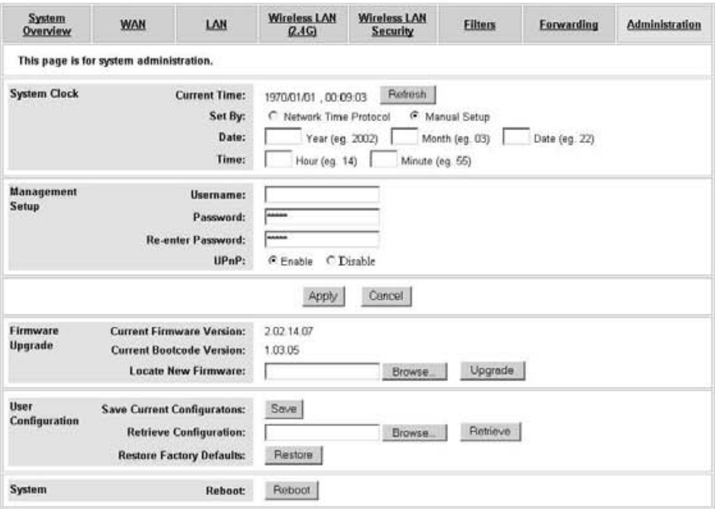
Retrieve User Configurations: If you have loaded factory defaults (either via the Load Default button on the back panel or via the Restore button in this group), you can restore your settings by clicking the **Retrieve** button.

Important: After retrieving your desired configuration file, you must reboot the device to enable the retrieved settings.

Restore Factory Defaults: To restore factory defaults, click the **Restore** button and then wait for a few seconds as the utility prompts. You will return to the Administration page while the process is complete. This feature is basically the same as resetting via the Load Default button (see “Rear Panel and Connectors”) on the device but it allows you to remotely perform the reset task.

▶ System

Reboot: This option allows to you remotely reboot the device.



This page is for system administration.

System Clock

Current Time: 1970/01/01 , 00:09:03

Set By: ○ Network Time Protocol ● Manual Setup

Date: Year (eg. 2002) Month (eg. 03) Date (eg. 22)

Time: Hour (eg. 14) Minute (eg. 55)

Management Setup

Username:

Password: ******

Re-enter Password: ******

UPnP: ● Enable ○ Disable

Firmware Upgrade

Current Firmware Version: 2.02.14.07

Current Bootcode Version: 1.03.05

Locate New Firmware:

User Configuration

Save Current Configuratons:

Retrieve Configuration:

Restore Factory Defaults:

System

Reboot:

Figure 4-17 Administration