

## 1. LINKSYS

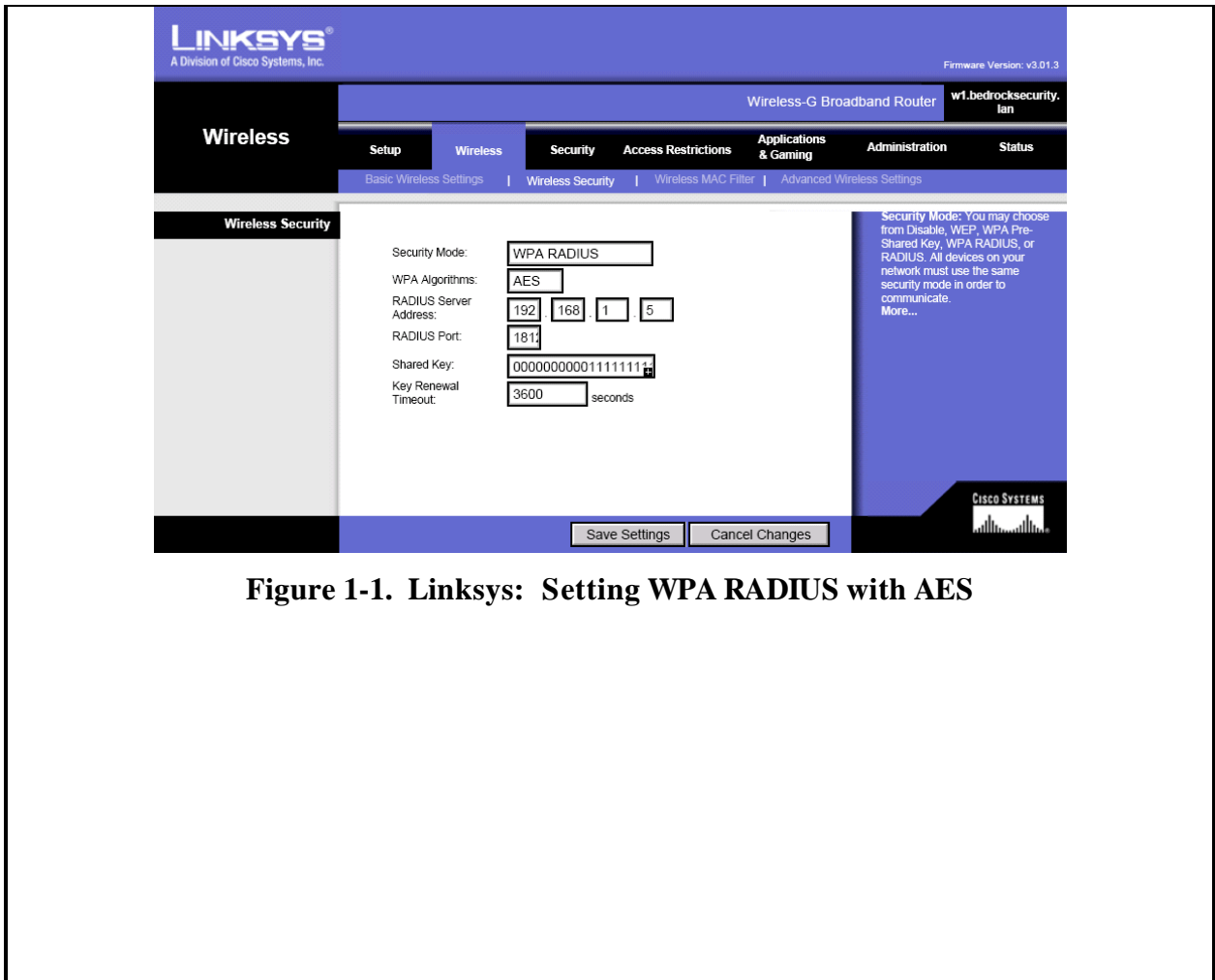
### 1.1 Product Description

The following are device specific configuration settings for the Linksys Wireless-G Broadband Router. Other Linksys wireless devices may or may not have similar capabilities. For example, the Linksys EtherFast Wireless AP + Cable/DSL Router w/4-Port Switch (BEFW11S4 v2.1; firmware 1.45.10), does **not** have similar security features. Further information may be obtained from <http://www.linksys.com/>. For similar Linksys devices, navigation through the management screens will be similar but may vary. The following equipment was used in the test case:

Device: Linksys WRT54G Wireless-G Broadband Router v2.0  
Firmware: Version 3.01.3  
Firmware Release Date: October 12, 2004

### 1.2 Configuration of Recommended Security Policies

2.3.1.010	Use layer 2 or 3 encryption with AES
<p>The Wi-Fi Alliance has certified the interoperability of the Linksys WRT54G v2 with products that support AES. Configure the Linksys WRT54G v2 to use WPA with AES, dynamic keys and RADIUS.</p> <ul style="list-style-type: none"><li>- Go to the <b>Wireless -&gt; Wireless Security</b> tab</li><li>- Select <b>WPA Radius</b> in the <b>Security Mode</b> option.</li><li>- For <b>WPA Algorithm</b> select <b>AES</b></li><li>- Enter the RADIUS Server's IP address</li><li>- Enter the RADIUS Server's authentication port: typically 1812</li><li>- Enter the Shared Key: (a random string of up to 64 characters)</li><li>- Enter the Renewal Timeout (in seconds): (3600 or less is recommended)</li><li>- Click on <b>Save Settings</b></li></ul>	



**Figure 1-1. Linksys: Setting WPA RADIUS with AES**

2.3.1.020	Choose products that support a network level security management solution. Network IDS/IPS devices may be used in conjunction with the Linksys WRT54G v2. The Linksys WRT54G v2 does not support centralized logging through SNMP, which could further enhance network intrusion detection capabilities.
-----------	--

2.3.1.030	Disable management ports on network devices when not in use.
-----------	--

The Linksys WRT54G v2 can only be configured through a web-based interface, so the HTTPS interface on the LAN side of this wireless router must remain enabled.

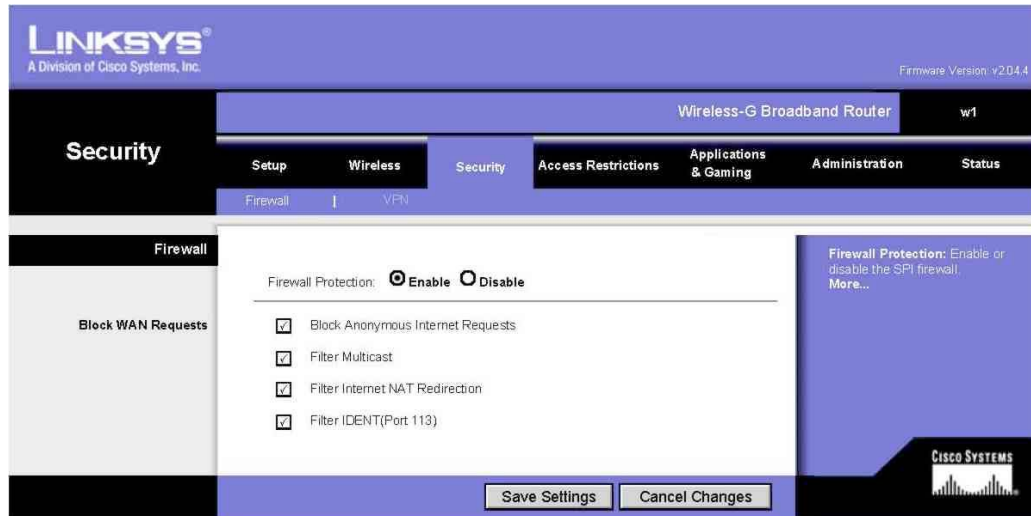
- Go to **Administration** → **Management**
- For Access Server: uncheck/disable HTTP; check/enable HTTPS
- For Remote Management: choose Disable
- For UPnP: choose Disable
- Click on **Save Settings**

The screenshot shows the Linksys WRT54G v2 web-based configuration interface. The page title is "Wireless-G Broadband Router" and the router name is "w1". The "Administration" menu is active, and the "Management" sub-menu is selected. The "Router Password" section is expanded, showing "Local Router Access" with two password input fields. Below that, the "Web Access" section has "Access Server" with "HTTP" unchecked and "HTTPS" checked, and "Wireless Access Web" with "Enable" selected. The "Remote Router Access" section has "Remote Management" with "Disable" selected, "Management Port" set to "8080", and "Use https" checked. The "UPnP" section has "UPnP" with "Disable" selected. A "Save Settings" button is at the bottom. On the right, there are help sections for "Local Router Access", "Web Access", "Remote Router Access", and "UPnP". The Cisco Systems logo is in the bottom right corner.

**Figure 1-2. Linksys: Port Management and Password Options**

Also disable (i.e. filter) services such as IDENT on the WAN interface of the Linksys WRT54G v2 (unless it is needed by your Internet Service Provider):

- Go to **Security** → **Firewall**
  - Enable: Filter IDENT (Port 113)
- Click on **Save Settings**



**Figure 1-3. Linksys: Filters**

2.3.1.040	Use OOB management across a specially configured VLAN for network administration/management
Configuration	The Linksys WRT54G v2 does not support this feature.

2.3.1.050	WLAN must have session timeout capability and must be set to 15 min or less
Configuration	The Linksys WRT54G v2 does not support this feature.

2.3.1.060	Set AP transmit power to lowest possible to attain signal strength required
Configuration	The Linksys WRT54G v2 does not support this feature. Place the device in a manner that reduces signal strength outside of the desired area.

2.3.1.070	Password-protect AP and bridges beyond manufacturer's default setting
<ul style="list-style-type: none"> <li>- Go to <b>Administration</b> → <b>Management</b> (See Figure 7-2)</li> <li>- Enter the router password</li> <li>- Confirm the router password</li> <li>- Click on <b>Save Settings</b></li> </ul>	

2.3.1.080	Change default SSID
<ul style="list-style-type: none"> <li>- Go to <b>Wireless</b> → <b>Basic Wireless Settings</b></li> <li>- Choose a SSID that is different from defaults used by wireless access points</li> <li>- Specify the SSID in <b>Wireless Network Name (SSID)</b></li> <li>- Click on <b>Save Settings</b></li> </ul>	
<p><b>Figure 1-4. Linksys: Setting SSID options</b></p>	

2.3.1.090	Disable SSID broadcast mode
<ul style="list-style-type: none"> <li>- Go to <b>Wireless</b> → <b>Basic Wireless Settings</b> (See Figure 7-4 above)</li> <li>- Disable: <b>Wireless SSID Broadcast</b></li> <li>- Click on <b>Save Settings</b></li> </ul>	

2.3.1.100 | Enable MAC address filtering

- Go to **Wireless -> Wireless MAC Filter**
- For **Wireless MAC Filter** select **Enable**
- Select **Permit only PCs listed to access the wireless network**
- Click on **Save Settings**

**Note:** Some dissimilar Linksys devices provide MAC address filters that only deny access to a specified list of MAC addresses (rather than allowing access from a specified list).



**Figure 1-5. Linksys: MAC Filter Settings**

- Click on **Edit MAC Filter List** and enter the authorized MAC addresses (s)
- Click on **Save Settings**

**MAC Address Filter List**

Enter MAC Address in this format: xxxxxxxxxxxx

**Wireless Client MAC List**

MAC 01:	00:03:2D:47:DC:AA	MAC 11:	_____
MAC 02:	00:06:EB:33:4B:A9	MAC 12:	_____
MAC 03:	00:1C:A2:5C:A9:11	MAC 13:	_____
MAC 04:	_____	MAC 14:	_____
MAC 05:	_____	MAC 15:	_____
MAC 06:	_____	MAC 16:	_____
MAC 07:	_____	MAC 17:	_____
MAC 08:	_____	MAC 18:	_____
MAC 09:	_____	MAC 19:	_____
MAC 10:	_____	MAC 20:	_____

---

MAC 21:	_____	MAC 31:	_____
MAC 22:	_____	MAC 32:	_____
MAC 23:	_____	MAC 33:	_____
MAC 24:	_____	MAC 34:	_____
MAC 25:	_____	MAC 35:	_____
MAC 26:	_____	MAC 36:	_____
MAC 27:	_____	MAC 37:	_____
MAC 28:	_____	MAC 38:	_____
MAC 29:	_____	MAC 39:	_____
MAC 30:	_____	MAC 40:	_____

**Figure 1-6. Linksys: MAC Filter List**

2.3.1.110 | Backup system configuration settings

To backup or restore the configuration go to **Administration** → **Config Management**



**Figure 1-7. Linksys: Configuration Management Settings**



### 2.3.1.120

### Enable Wireless Client Isolation

Enable wireless client isolation to prevent communication between Wireless clients associated with the Linksys WRT54G v2 (unless that functionality is required). This does not restrict communication between Wireless clients and LAN clients. Linksys refers to this feature as AP isolation.

- Go to **Wireless** → **Advanced Wireless Settings**
- For **AP Isolation** select On
- Click on **Save Settings**

The screenshot displays the Linksys WRT54G v2 Advanced Wireless Settings page. The page is titled "LINKSYS A Division of Cisco Systems, Inc." and "Wireless-G Broadband Router w1". The "Wireless" menu is selected, and the "Advanced Wireless Settings" sub-menu is active. The settings are as follows:

Setting	Value	Default
Authentication Type	Auto	Auto
Basic Rate	Default	Default
Transmission Rate	Auto	Auto
CTS Protection Mode	Disable	Disable
Frame Burst	Enable	Disable
Beacon Interval	100	100, Milliseconds, Range: 1 - 65535
DTIM Interval	1	1, Range: 1 - 255
Fragmentation Threshold	2346	2346, Range: 256 - 2346
RTS Threshold	2347	2347, Range: 0 - 2347
AP Isolation	On	Off

The "AP Isolation" setting is highlighted in blue. The page also includes a "Save Settings" button and a "Cancel Changes" button. A note on the right side of the page states: "Authentication Type: You may choose from Auto or Shared Key. Shared key authentication is more secure, but all devices on your network must also support Shared Key authentication. More..."

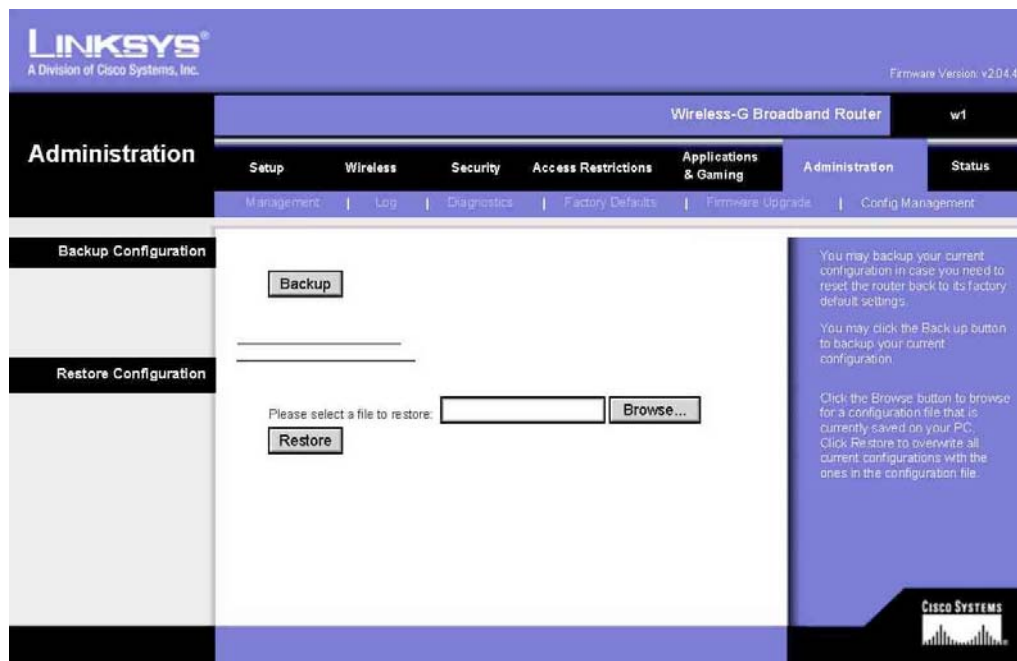
Figure 1-8. Linksys: Advanced Wireless Settings

### 2.3.1.130 Enable and configure logging

The Linksys WRT54G can log traffic on the WAN interface if you are using it in the default gateway mode (versus the router mode). This feature permits logging for local inspection but it does not permit logging to a remote server

(**Note:** Some Linksys wireless devices permit logging to a remote server).

- Go to **Administration** → **Log**
- Enable the Log
- Click on **Save Settings**



**Figure 1-9. Linksys: Backup and Restore**