

**Setup**

Setup    Wireless    Security    Applications & Gaming    Administration    Status

Basic Setup    DDNS    MAC Address Clone    Advanced Routing

**Internet Setup**  
Internet Connection Type

PPPoE

User Name:

Password:

Connect on Demand: Max Idle Time  Min.

Keep Alive: Redial Period  Sec.

Optional Settings  
(required by some ISPs)

Host Name:

Domain Name:

MTU:  Enable  Disable Size:

Speed & Duplex: Auto

**Network Setup**

Router IP

Local IP Address:  .  .  .

Subnet Mask:  .  .  .

Network Address  
Server Settings (DHCP)

Local DHCP Server:  Enable  Disable

Start IP Address:

Number of Address:

DHCP Address Range: 192.168.1.100 ~ 149

Client Lease Time:  minutes (0 means two day)

Static DNS 1:  .  .  .

Static DNS 2:  .  .  .

Static DNS 3:  .  .  .

WINS:  .  .  .

**Basic Setup**

The Basic Setup screen is where basic configuration is performed. Some ISPs (Internet Service Providers) will require that you enter the DNS information. These settings can be obtained from your ISP. After you have configured these settings, you should set a router password from the Administration->Management screen.

Completing the Internet Setup section is all that is required to set up for your specific ISP. Please look at the table below to configure the Router for your internet connection.

More...

If you're using a wireless router and have decided to turn off DHCP, also consider changing the IP subnet.

If you're deploying a wireless router, think about assigning static IP addresses for your wireless NICs and turn off DHCP. It's true that it's more of an administrative overhead to manage. Although a wireless sniffer could easily pick out IP addresses, by not passing them out, it just adds another barrier. It makes it tougher for the casual "drive by" to use your network.

Save Settings    Cancel Changes

**Welcome screen for the BEFW11S4**

## DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. You can choose which services you want to use. The two choices are as following:

DDNS.org      <http://www.dyndns.org>

TZO              <http://www.tzo.com>

Other companies like no-ip.com provide the same service for free

By default, the DDNS option is disabled.

DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before using this feature, you need to sign up for DDNS service at [www.dyndns.org](http://www.dyndns.org) or [www.tzo.com](http://www.tzo.com).

<b>DDNS Service</b>	<p>To disable DDNS Service, keep the default setting, <b>Disable</b>. To enable DDNS Service, follow these instructions:</p> <ol style="list-style-type: none"> <li>1. On the <i>DDNS</i> screen, select the DDNS service.             <ol style="list-style-type: none"> <li>A. DynDNS.org- Enter the <b>Username</b>, <b>Password</b>, and <b>Host Name</b> used when you signed up for the service.</li> <li>B. Tzo.com- Enter the <b>Email Address</b>, <b>TZO Password Key</b>, and <b>Domain Name</b> used when you signed up with the service.</li> </ol> </li> <li>2. Click the <b>Save Settings</b> button to save your changes. Click the <b>Cancel Changes</b> button to cancel unsaved changes.</li> </ol>
<b>Internet IP Address</b>	The Router's current Internet IP Address is displayed here.
<b>Status</b>	The status of the DDNS service connection is displayed here.

Check all the values and click **Save Settings** to save your settings. Click the **Cancel Changes** button to cancel your unsaved changes.

## Routing

### NAT

NAT is Network Address Translation, which allows multiple computers to share one Internet connection. You can turn off NAT by selecting the **Disable** option. By default, NAT is set to **Enable**.

### Dynamic Routing

The Dynamic Routing feature can be used to automatically adjust to physical changes in the network's layout. The Router uses the dynamic RIP protocol. It determines the route that the network packets take based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

#### To set up Dynamic Routing:

1. For the Transmit RIP Version dropdown menu, select the protocol you want to use for transmitting data on the network protocol you want for transmitting data on the network.
2. For the Receive RIP Version dropdown menu, select the protocol you want to use for receiving data from the network.
3. Click the **Save Settings** button to save your changes.

### Static Routing

When multiple routers are installed on your network, you will need to configure Static Routing. The static routing function determines the path that data follows over your network before and after it passes through the Router. You can use static routing to allow different IP domain users to access the Internet through the Router. **This is an advanced feature. Please proceed with caution.**

To set up static routing, you should add routing entries in the Router's table that tell the device where to send all incoming packets. All of your network routers should direct the default route entry to this Router.

#### To create a static route entry:

1. Select an entry from the drop down list. The router supports up to 20 static route entries.
2. Enter the following data for the static route.

Destination IP Address	Enter the network address of the remote local LAN segment. For a standard Class C IP domain, the network address is the first three fields of the Destination LAN IP, while the last field should be zero.
Subnet Mask	Enter the Subnet Mask used on the destination IP domain. For a standard class C IP domain, the Subnet Mask is 255.255.255.0.
Gateway	If this Router is used to connect your network to the Internet, then your Gateway IP is the Router's IP Address. If you have another router handling your network's Internet connection, enter the <b>IP Address</b> of

	that router instead
Hop Count	Enter the Hop Count. This is the number of hops to each node until the destination has been reached.
Interface	The Interface is the destination of the connection. For example, if you are from the local connection and you need to go out to the Internet port, then you interface is Internet.

3. Click the **Save Settings** button to save your changes. Click **Cancel Changes** to cancel your changes.

To view the current routing table, click the **Show Routing Table** button.

**To delete a static route entry:**

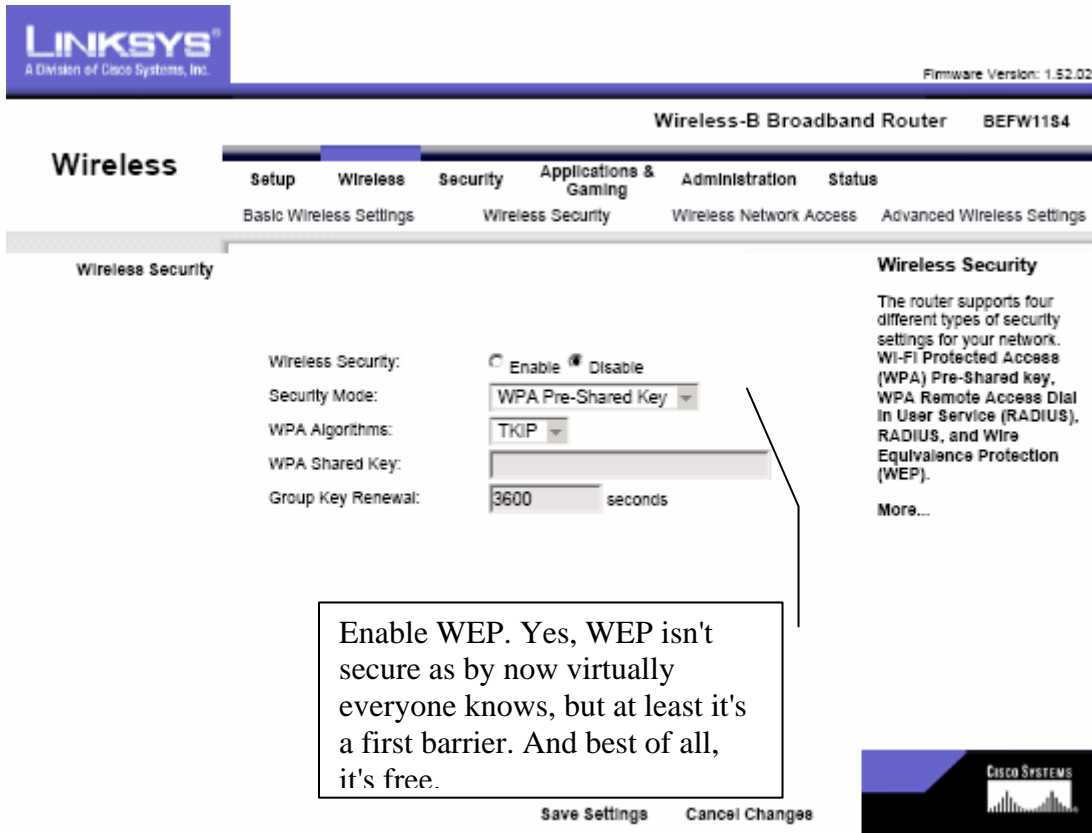
1. Select an entry from the drop-down list.
2. Click the **Delete Entry** button.
3. Click the **Save Settings** button to save your changes.

Disable "broadcast SSID". As you take your access point out of the box, broadcast SSID is enabled which means that it will accept any SSID. By disabling, the SSID configured in the client must match the SSID of the access point.

**Basic Wireless Settings**

The *Wireless* screen allows you to customize data transmission settings. In most cases, the advanced settings on this screen should remain at their default values.

<b>SSID</b>	The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. <b>Make sure this setting is the same for all devices in your wireless network. For added security, Linksys recommends that you change the default SSID (<b>linksys</b>) to a unique name of your choice.</b>
<b>SSID Broadcast</b>	When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router SSID, keep the default setting, <b>Enable</b> . If you do not want to broadcast the Router SSID, then select <b>Disable</b> .
<b>Channel</b>	Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All devices in your wireless network must use the same channel in order to function correctly.



**Wireless Security**

The router supports four different types of security settings for your network. **Wi-Fi Protected Access (WPA) Pre-Shared key, WPA Remote Access Dial In User Service (RADIUS), RADIUS, and Wire Equivalence Protection (WEP).**

To enable Security Settings, click the **Enable** radio button. Then click the **Edit Security Settings** button to configure the security settings. To disable security settings, keep the default setting, **Disable**.

**WPA Pre-Shared Key:**

There are two encryption options for WPA Pre-Shared Key, **TKIP** and **AES**. TKIP stands for Temporal Key Integrity Protocol. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. AES stands for Advanced Encryption System, which utilizes a symmetric 128-Bit block data encryption.

To use WPA Pre-Shared Key, enter a password in the **WPA Shared Key** field between 8 and 63 characters long. You may also enter a **Group Key Renewal Interval** time between 0 and 99,999 seconds.

**WPA RADIUS:**

WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS Port (default is 1812) and the shared secret from the RADIUS server.

**RADIUS:**

RADIUS utilizes either a RADIUS server for authentication or WEP for data encryption. To utilize RADIUS, enter the IP address of the RADIUS server and its shared secret. Select the desired encryption bit (64 or 128) for WEP and enter either a passphrase or a manual WEP key.

**WEP:**

There are two levels of WEP encryption, 64-bit and 128-bit. The higher the encryption bit, the more secure your network, however, speed is sacrificed at higher bit levels. To utilize WEP, select the desired encryption bit, and enter a passphrase or a WEP key in hexadecimal format.

**Wireless**

Setup Wireless Security Applications & Gaming Administration Status

Basic Wireless Settings Wireless Security Wireless Network Access Advanced Wireless Settings

**Wireless Network Access**

Allow All  
 Restrict Access

Access List:

MAC 01: 000000000000 MAC 11: 000000000000  
 MAC 02: 000000000000 MAC 12: 000000000000  
 MAC 03: 000000000000 MAC 13: 000000000000  
 MAC 04: 000000000000 MAC 14: 000000000000  
 MAC 05: 000000000000 MAC 15: 000000000000  
 MAC 06: 000000000000 MAC 16: 000000000000  
 MAC 07: 000000000000 MAC 17: 000000000000  
 MAC 08: 000000000000 MAC 18: 000000000000  
 MAC 09: 000000000000 MAC 19: 000000000000  
 MAC 10: 000000000000 MAC 20: 000000000000

Wireless Client MAC List

Save Settings Cancel Changes

**Wireless Network Access**

The Wireless Network Access screen is where you can restrict wireless access. The restriction is based on wireless device MAC address. MAC address is a unique 12 digit hexadecimal value given to each network device.

More...

Many access points allow you to control access based on the MAC address of the NIC attempting to associate with it. If the MAC address of your NIC isn't in the table of the access point, you won't associate with it.

**Wireless Network Access**

The Wireless Network Access screen is where you can restrict wireless access. The restriction is based on wireless device MAC address. MAC address is a unique 12 digit hexadecimal value given to each network device.

MAC Filter	Enable this option to allow specific network devices to gain access based on the MAC address.
MAC 01 to 20	Enter the MAC address that you want to allow access to the network.
Wireless Client MAC List	This button will show you a list of MAC address that you can select and be placed in the list of allowed wireless network devices. It is recommended that all wireless network devices be turned on to add them on the list of allowed access through wireless network.

## Wireless Client MAC List

This screen will provide a list of wireless clients currently accessing the Router. This will show **Computer Name, IP Address, MAC Address, and Enable MAC Filter**. By checking the **Enable MAC Filter**, you are granting this wireless client to gain access to the network.

For most users, the default values for the Router should be satisfactory. The Router can be used in most network environments without changing any of the values.

The screenshot displays the 'Advanced Wireless Settings' page of a Linksys BEFW11S4 router. The page title is 'Wireless' and the sub-tab is 'Advanced Wireless Settings'. The settings are as follows:

- Basic Rates: 1-2 Mbps(Default)
- Control TX Rate: 1-2-5.5-11 Mbps(Default)
- Preamble Type: Long Preamble(Default)
- Authentication Type: Auto(Default)
- Antenna Selection: Diversity(Default)
- Beacon Interval: 100 (msec, range: 1~65535, \*100)
- DTIM Interval: 1 (range: 1~255, \*1)
- Fragmentation Threshold: 2346 (range: 256~2346, \*2346)
- RTS Threshold: 2432 (range: 256~2432, \*2432)

Buttons for 'Save Settings' and 'Cancel Changes' are located at the bottom of the settings area.

### Advanced Wireless Settings

The Advanced Wireless Settings screen is where basic wireless configuration is performed.

Basic Rates	The basic transfer rates should be set depending on the speed of your wireless network. You must select 1-2 (Mbps) if you have older 802.11 compliant equipment on your network.
Control TX Rate	Select all the supported rates at which the Router will communicate with your wireless network.
Preamble Type	The preamble defines the length of the CRC block for communication between the Router and the roaming network adapter. (High network traffic areas should use the shorter preamble type.)

Authentication Type	You may choose between <b>Open System</b> , <b>Shared key</b> , or <b>Both</b> . The Authentication Type default is set to Open System, in which the sender and the recipient do not share a secret key. Each party generates its own key-pair and asks the receiver to access the randomly generated key. Once accepted, this key is used for a short time only. Then a new key is generated and agreed upon. Shared key is when both the sender and the recipient share a secret key.
Beacon Interval	This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to keep the network synchronized.
DTIM Interval	This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages.
Fragmentation Threshold	This value indicates how much of the Router's resources are devoted to recovering packet errors.
RTS Threshold	This value should remain at its default settings of 2,346. Should you encounter inconsistent data flow, only minor modifications are recommended.

For most users, the default values for the Router should be satisfactory. The Router can be used in most network environments without changing any of the values. It is recommended that these values do not change, unless you know what you are doing.

**LINKSYS**  
A Division of Cisco Systems, Inc.

Firmware Version: 1.52.02

Wireless-B Broadband Router BEFW11S4

**Security**

Setup Wireless **Security** Applications & Gaming Administration Status

Filter VPN Passthrough

**Filter IP Address Range**

NUM	Start	End
1:	192.168.1.0 ~ 0	0
2:	192.168.1.0 ~ 0	0
3:	192.168.1.0 ~ 0	0
4:	192.168.1.0 ~ 0	0
5:	192.168.1.0 ~ 0	0

**Filter Port Range**

NUM	Protocol	Start	End
1:	Both	0 ~ 0	0
2:	Both	0 ~ 0	0
3:	Both	0 ~ 0	0
4:	Both	0 ~ 0	0
5:	Both	0 ~ 0	0

**Filter MAC Address**

Edit MAC Filter Setting

**Block WAN Requests** Block Anonymous Internet Requests:  Enabled  Disabled

Filter Multicast:  Enabled  Disabled

Filter Internet NAT Redirection:  Enabled  Disabled

Filter IDENT(Port 113):  Enabled  Disabled

Save Settings Cancel Changes

**Filters**

By using the Filters screen, you can configure the Router to block specific internal users from accessing the Internet. You can set up different filters for different users based on their IP addresses, MAC addresses, and their services port numbers.

To set **Filter IP Address Range**, do the following:

1. Enter the range of IP addresses that you want to filter into the IP address range fields. The users who have these IP addresses will not be able to access the Internet.
2. Click the **Save Settings** button to save any changes.

To set **Filter Port Range**, do the following:

1. You can filter users by entering their services port numbers.

More...

CISCO SYSTEMS

**Filters**

By using the *Filters* screen, you can configure the Router to block specific internal users from accessing the Internet. You can set up different filters for different users based on their IP addresses, MAC addresses, and their services port numbers.

To set **Filter IP Address Range**, do the following:

1. Enter the range of IP addresses that you want to filter into the IP address range fields. The users who have these IP addresses will not be able to access the Internet.
2. Click the **Save Settings** button to save any changes.

To set **Filter Port Range**, do the following:

3. You can filter users by entering their services port numbers. Select the protocols and enter the range of port numbers that you want to filter in the port number range fields. The users who have these port numbers will not be able to access the Internet.
  4. Click the **Save Settings** button to save any changes.
- 

To filter MAC addresses, do the following:

1. Click the **Edit MAC Filter Settings** button to open the MAC Filter page.
  2. In the **Filtered MAC Address** dropdown menu, select the set you want to view. A total of 50 MAC address can be filtered. Filtering MAC addresses will block access to the Internet.
  3. Enter the MAC Address in the field provided to prevent this computer from getting access to the Internet.
- 

### **Block WAN Requests**

The **Block Anonymous Internet Requests** is a feature is designed to prevent intruders from attacking through the Internet. When it is Enabled, the Router will drop both the unaccepted TCP request and ICMP packets from the Internet. The hacker will not find the Router by pinging the Internet IP address. Click Disabled to allow those packets to get through.

**LINKSYS**  
A Division of Cisco Systems, Inc.

Firmware Version: 1.52.02

Wireless-B Broadband Router BEFW11S4

Applications & Gaming

Setup Wireless Security Applications & Gaming Administration Status

Port Range Forwarding Port Triggering UPnP Forwarding DMZ

Port Range Forwarding

Port Range					
Application	Start to	End	Protocol	IP Address	Enable
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>
	0 to 0	0	Both	192.168.1.0	<input type="checkbox"/>

Save Settings Cancel Changes

**Port Range Forwarding**

Port Range Forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your network, the Router can forward those requests to computers equipped to handle the requests. If, for example, you set the port number 80 (HTTP) to be forwarded to IP Address 192.168.1.2, then all HTTP requests from outside users will be forwarded to 192.168.1.2. It is recommended that the computer use static IP address.

You may use this function to establish a web server or FTP server via an IP Gateway. Be sure that you enter a valid

More...

CISCO SYSTEMS

Port Forwarding, Port Triggering, UPnP Forwarding, Essentially provide the same service. DMZ leaves open a machine to the Internet, no firewall

**Port Range Forwarding**

Port Range Forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your network, the Router can forward those requests to computers equipped to handle the requests. If, for example, you set the port number 80 (HTTP) to be forwarded to IP Address 192.168.1.2, then all HTTP requests from outside users will be forwarded to 192.168.1.2. **It is recommended that the computer use static IP address.**

You may use this function to establish a web server or FTP server via an IP Gateway. Be sure that you enter a valid IP address. (You may need to establish a static IP address with your ISP in order to properly run an Internet server.) For added security, Internet users will be able to communicate with the server, but they will not actually be connected. The packets will simply be forwarded through the Router.

To add a server using forwarding:

1. Enter an **Application** name of the service you want to forward.
2. Enter the **Port Range Start** and **End** of the service you want to forward.
3. Select the **protocol** used by the services.
4. Enter the **IP Address** of the server that you want the Internet users to access.
5. Select **Enabled** for that entry.
6. Click the **Save Settings** button to save the settings.

To delete a service entry:

1. Enter a zero number in the Port Range number and IP Address fields.
2. Uncheck the **TCP** and/or **UDP** check box and the **Enable** check box.
3. Clear the **Application** field.
4. Click the **Save Settings** button to save any changes you make.

### **Port Triggering**

Port triggering will forward port based on the incoming port specified. Check with your software application to find out what is necessary to enter in these fields.

**To add a server using forwarding:**

1. Enter an *Application* name of the service you want to forward.
2. Enter the *Trigger Range* for *Start* and *End* of the services to trigger forwarding.
3. Enter the *Forwarded Range* for *Start* and *End* of the service you want to forward.
4. Click the *Save Settings* button to save the settings.

**To delete a service entry:**

1. Enter a zero number in the *Port Range* and *Forwarded Range* field.
2. Clear the *Application* field.
3. Click the *Save Settings* button to save any changes you make.

### **UPnP Forwarding**

UPnP Forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your network, the Router can forward those requests to computers equipped to handle the requests. If, for example, you set the port number 80 (HTTP) to be forwarded to IP Address 192.168.1.2, then all HTTP requests from outside users will be forwarded to 192.168.1.2. **It is recommended that the computer use static IP address.**

You may use this function to establish a Web server or FTP server via an IP Gateway. In this format, Windows XP can be used to configure this through UPnP communication. Be sure that you enter a valid IP Address. (You may need to establish a static IP address with your ISP in order to properly run an Internet server.) For added security, Internet users will be able to communicate with the server, but they will not actually be connected. The packets will simply be forwarded through the Router.

**To add a server using forwarding:**

1. Enter an **Application** name of the service you want to forward.
2. Enter the **Ext. Port** number. Check with your service application needed for External Port used.
3. Select the **Protocol** used by the services.
4. Enter the **Int. Port** number used by the application.
5. Enter the **IP Address** of the server that you want the Internet users to access.
6. Select **Enable** for that entry.
7. Click the **Save Settings** button to save the settings.

**To delete a service entry:**

1. Enter a zero number in the **Ext. Port** and **Int. Port**, and **IP Address** from the fields.
2. Uncheck the **Enable** check box.
3. Clear the **Application** field.
4. Click the **Save Settings** button to save any changes you make.

**DMZ Host**

The DMZ Host setting can allow one local PC to be exposed to the Internet. If a local user wishes to use some special-purpose service such as an Internet game or video-conferencing, Enable **DMZ**, fill in the **IP address**, and click the **Save Settings** button. Select Disable for **DMZ**, deactivates this feature. When enabling this setting, the Router firewall protection of the DMZ Host setting can allow one local PC to be exposed to the Internet. If a local user wishes to use some special-purpose service such as an Internet game or video-conferencing, Enable **DMZ**, fill in the **IP address**, and click the **Save Settings** button. Select Disable for **DMZ**, deactivates this feature. When enabling this setting, the Router firewall protection of the local DMZ host will be disabled.

The screenshot shows the Linksys BEFWS11S4 web interface. At the top, there is a blue header with the Linksys logo and 'A Division of Cisco Systems, Inc.' on the left, and 'Firmware Version: 1.52.02' on the right. Below the header, the page title is 'Wireless-B Broadband Router BEFW11S4'. The main navigation bar includes 'Administration' (selected), 'Setup', 'Wireless', 'Security', 'Applications & Gaming', and 'Status'. Under 'Administration', there are sub-links: 'Management', 'Log', 'Factory Defaults', and 'Firmware Upgrade'. The 'Management' section is active, showing 'Local Router Access' with password fields, 'Remote Router Access' with radio buttons for 'Remote Upgrade' and 'Remote Administration' (both set to 'Disabled'), and 'UPnP' settings. The 'UPnP' section has three options: 'UPnP' (Disabled), 'Allow users to make Configuration Changes' (Enabled), and 'Allow users to Disable Internet Access' (Enabled). A 'Backup and Restore' button is visible at the bottom of the management section. A 'Save Settings' button is at the very bottom. On the right side, there is a 'Router Password' section with explanatory text. A text box on the left explains that UPnP publishes too much information and should be disabled. A callout box on the right explains that the default password should be changed because programs like NetStumbler can identify the manufacturer based on the MAC address.

UPnP publishes so much information about the router, it is best to disable it

Change the default password on your access point or wireless router. Since programs like NetStumbler identify the manufacturer based on the MAC address, it doesn't take much work to figure out what type of device it is even if you change the SSID.

## Management

### Local Router Access

Router Password	Enter the password you choose for this Router. This is needed to gain access to the Web-based Utility.
Re-enter to confirm	Enter the password chosen above to confirm that you properly entered the password.

### Remote Router Access

Remote Upgrade	This option allows for upgrading the Router's firmware from a remote location.
Remote Administration	This option allows you to access the Web-based Utility from a remote location.
Administrator Port	Enter the port number you want to use to access to the Router from a remote location.

#### To access the router from the remote location

Enter the following in the URL of your web browser:

http:// <internet IP address of the Router>:<Administrator Port>. For example, if your IP address is 1.2.3.4 and you set the administrator port number to be 5204, you would enter the following:

<http://1.2.3.4:5204/>

## UPnP

UPnP	Select <b>Enabled</b> to allow UPnP communication between the Router and the computer that is UPnP compliant. By default, UPnP is Disabled.
Allow users to make Configuration Changes	This options allows users to make changes using windows XP utilities. For example, you can make changes that are configurable through Windows XP utility.
Allow users to Disable Internet Access	This option allows users to disable Internet access by disabling network connections in Windows XP.

## Backup and Restore

Click the **Backup and Restore** button to save and reload the configuration of the Router.

Backup	To save the Router's configuration, click the <b>Backup</b> button. On the window that appears, click the <b>Save</b> button. Select the location and filename, then the <b>Save</b> button.
Restore	Click the Browse... Button and specify the location and filename of the configuration file previously saved. Click the <b>Open</b> button and the full path will appear in the prompt. Click the <b>Restore</b> button and then click the <b>Close</b> button.

Click **Save Settings** to save any changes.

### **Log Status**

the *Log* screen provides information on all the log activities. A file can also be generated to keep a permanent record of the activities by using logviewer software, which is available on the setup CD or can be downloaded from the Linksys website at [www.linksys.com](http://www.linksys.com).

### **Log**

Select **Yes** to log all the Router activities. By default, the log is Disabled.

### **Logviewer IP Address**

Enter the IP address of the PC that is running the logviewer software. To find the IP address of this computer, go to it and run *ipconfig* or *winiipcfg*. For details, refer to the User Guide.

### **Incoming log**

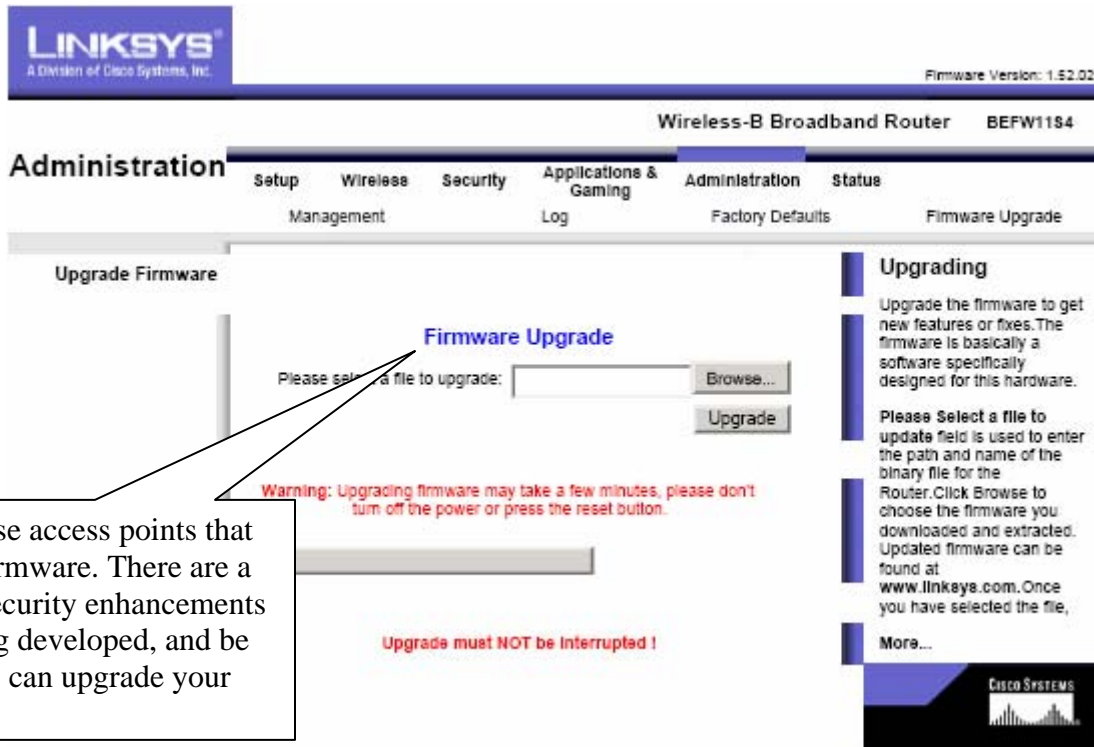
Click on this button to get a log of all incoming activities. This is useful if you are running a website or FTP server and want to keep track of who came in through the Router.

### **Outgoing log**

Click on this button to get a log of all outgoing activities. This keeps track of all the outgoing traffic and is useful for monitoring a specific website a computer went to based on the local IP address.

### **Factory Default**

Click **Yes** and **Save Settings** to reset the Router to factory defaults. You can also do this by holding the Reset button on the back of the Router for 30 seconds.



Only purchase access points that have flash firmware. There are a number of security enhancements that are being developed, and be sure that you can upgrade your access point.

**Upgrading**

Upgrade the firmware to get new features or fixes. The firmware is basically software specifically designed for this hardware.

**Please Select a file to update** field is used to enter the path and name of the binary file for the Router. Click **Browse** to choose the firmware you downloaded and extracted. Updated firmware can be found at [www.linksys.com](http://www.linksys.com). Once you have selected the file, click **Upgrade** to start upgrading. If the upgrade fails, make sure you do the following:

1. Make sure you have the correct firmware for the Router you are using.
2. Try upgrading the Router again before rebooting the computer or turn off the Router.

For details on recovering from a failed upgrade, please check the User Guide on the Setup CD-ROM for detailed information.



Firmware Version: 1.52.02

Wireless-B Broadband Router BEFW11S4

Status

- Setup
- Wireless Router
- Security
- Applications & Gaming Local Network
- Administration
- Status

Router Information

Firmware Version: 1.52.02, Apr 7 2005  
 MAC Address: 00-0F-66-B8-96-87

Internet

Configuration Type

Login Type: PPPOE  
 Login Status: Connected   
 Internet IP Address: 201.145.3.183  
 DNS 1: 151.164.17.201  
 DNS 2: 151.164.11.201  
 DNS 3: 200.33.148.196  
 MTU: 1492

Router Status

This screen provides the Router's current status information in a read-only format.

Login Type

This field shows the Internet login status. When you choose PPPoE, RAS, PPTP, or HBS as the login method, you can click the **Connect** button to log in. If you click the **Disconnect** button, the Router will not dial up again until you click the **Connect** button.

If your connection is DHCP or Static IP, the Status screen will show you the Internet IP Address, Subnet mask,

More...

Refresh



Status