CHAPTER 5

Broadband Routers and Firewalls

Depending on the report you want to accept, between 53 percent and 62 percent of Internet access in the United States is provided by broadband connections. Outside the United States, broadband access percentages can exceed 75 percent of all Internet access methods (http://www.websiteoptimization.com/bw/0511/).

Although broadband Internet access provides for increased download speeds and an explosion of Internet-based services and resources, it also introduces some unique problems to the small office/home office (SOHO) and home user markets. With dialup connections, the need to protect the resources accessing the Internet is not considered as critical, because systems are rarely left connected to the Internet all the time. Rather, users dial the computer into a service provider, do what they need on the Internet, and then hang up the modem, thus protecting the system with the most secure of "firewalls" by disconnecting it from the network.

With most broadband connections, however, the Internet connection is always on; and if the computer is left on, the computer remains always vulnerable to attack. Of course, this scenario is nothing new to the corporate arena, where always-on Internet connections are normal, but it presents a whole new issue of how to secure environments that are often out of the control of the IT department and frequently do not have people with the technical expertise to deal with security issues at the location where the resources are.

Many home users and hobbyists also want to take advantage of the increased speed and better functionality that a broadband connection provides, but want to ensure that their systems are as secure as possible. They have neither the technical expertise nor desire to secure their computers properly, but at the same time they want something that they can place between their computer and the network and be relatively certain that their computer will be protected.

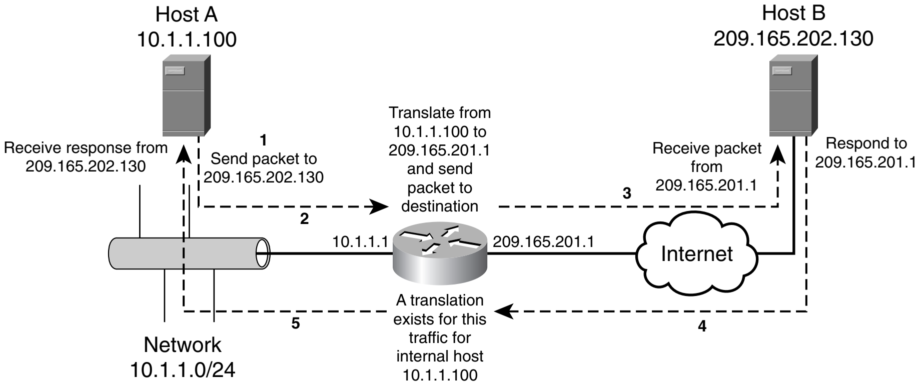
How Broadband Routers and Firewalls Work

Many broadband routers and firewalls function primarily through the use of Network Address Translation (NAT) to hide the internal systems behind a single external IP address. These so-called "NAT routers" or "NAT firewalls" do an adequate job of hiding resources from casual attack methods, but they do not perform advanced firewall functions; therefore, it is really a bit of a misnomer to call them firewalls, at least in the sense that firewalls such as the Cisco

Secure PIX Firewall, Microsoft ISA Server, and Check Point Firewall-1 products are considered firewalls. Rather, many broadband routers and firewalls are just NAT-based packet-filtering routers providing a degree of privacy, but they typically lack advanced firewall features such as stateful packet inspection (SPI), proxying of data, or deep packet inspection.

Figure 5-1 shows the NAT process.

Figure 5-1 *How NAT Works*


Host A
10.1.1.100
Host B
209.165.202.130
Receive response from 209.165.202.130
1
Send packet to 209.165.202.130
2
Translate from 10.1.1.100 to 209.165.201.1 and send packet to destination
Receive packet from 209.165.201.1
3
Respond to 209.165.201.1
10.1.1.1
209.165.201.1
Internet
A translation exists for this traffic for internal host 10.1.1.100
5
4
Network
10.1.1.0/24

The steps numbered in Figure 5-1 can be further explained as follows:

1. The client initiates a connection to an external host (HostB).
2. The broadband router/firewall receives the request and translates the request from the internal IP address to the address of the router/firewall's external interface. The router/firewall keeps track of this translation in a translation table.
3. The packets are delivered to the external destination (HostB), which believes that the packets originated from the external IP address of the router/firewall. The external host (HostB) responds accordingly to the external IP address of the router/firewall.
4. When the router/firewall receives the response from the external host, it checks its translation table for a matching outbound request.
5. If it finds one, the router/firewall repackages the packet and delivers it to the internal host (HostA), which thinks that the response is from the external host (HostB).

In addition, most broadband routers/firewalls are designed not to permit any unsolicited packets from an external host to be delivered to an internal host.

Although this is generally an adequate level of protection for most home environments, it is important to understand that reliance on NAT alone to protect hosts is a false sense of security because NAT does not guarantee security in and of itself, as noted in RFC 2663 Section 9.0. For example, NAT devices are as susceptible to targeted attacks, such as denial-of-service (DoS) attacks, as non-NAT devices. NAT also provides for no actual filtering of packets leaving the internal network; instead, it permits all outbound traffic as long as it can be translated accordingly. Although it is a subtle difference, NAT provides more privacy than it does security.

Therefore, only when used in conjunction with other technologies can NAT serve as an effective security mechanism. The best broadband routers/firewalls (for example, many of the Linksys broadband firewalls) include application-level filtering, deep packet inspection, SPI, firewall hardening, and NAT.

Linksys Broadband Routers/Firewalls

Linksys makes a number of broadband routers (with basic firewall functionality) and broadband firewalls (with advanced firewall functionality) for both wired and wireless networks. Most of the wired products begin with a model number of BEF; most of the wireless products begin with a model number of WRT. The Linksys broadband routers/firewalls are designed with the home user in mind, and therefore are designed with simplicity of implementation in mind. All function as NAT routers, and some models and versions also provide stateful packet inspection in addition to NAT; unfortunately, Linksys does not do a good job of specifying which models and versions of firmware have this functionality. This difficulty is compounded by the fact that SPI was removed from some versions of firmware, so literally the same hardware with different versions of firmware may or may not support SPI.

This chapter examines the Linksys BEFSR41v4 EtherFast Cable/DSL Router with 4-Port Switch. The BEFSR41v4 is designed primarily for the home and small office user, and as a result has a relatively basic and simple-to-implement feature set. For ease of review, the features have been categorized as follows for the discussion that follows:

- Security and filtering features
- Routing features
- Management and administration features
- Miscellaneous features

Security and Filtering Features

The BEFSR41v4 is a basic NAT router (with firewall functionality) that can perform basic port filtering to allow traffic both coming into and going out of the protected network to be filtered. Unlike many firewalls that take a “block all, permit only” minimalist approach to filtering outbound traffic, the Linksys is just the opposite, instead taking the approach of “permit all outbound, block only.” The idea is that it is easier to block a couple of ports or IP addresses than it is to identify the ports or IP addresses that should be permitted.

Inbound traffic still adheres to the minimalist filtering policy, blocking all traffic to all ports unless you otherwise configure the router to permit the traffic. Unfortunately, filtering incoming traffic can only be done based on the destination port number, so it is not possible to permit only certain external hosts to access the protected resources. Either the entire Internet can access the resources or none of the Internet can.

The BEFSR41v4 also supports the concept of a demilitarized zone (DMZ) system. The DMZ functions by effectively taking a host from the internal network and using NAT to expose it in an unfiltered fashion to the Internet. This exposure allows any Internet host to fully connect to and access the host in an unrestricted and nonfirewalled manner. In general, a DMZ is a bad idea; however, some circumstances, particularly when attempting to run gaming applications and such, require connectivity to the system that the Linksys filtering rules are not capable of easily or properly supporting. Consequently, a DMZ provides a simple, albeit entirely insecure method of making sure that the host can be accessed by Internet hosts.

Because Linksys routers utilize NAT, some protocols such as IPSec, PPP over Ethernet (PPPoE) passthrough, and Point-to-Point Tunneling Protocol (PPTP) fail to function properly. This failure results because NAT changes the source address of packets that are translated through the router, causing the destination host for those packets to believe that the data has been compromised (which strictly speaking, it has). To facilitate using these protocols through a Linksys router/ firewall, Linksys supports what is known as virtual private network (VPN) passthrough. VPN passthrough allows traffic in a VPN tunnel to pass through the router/firewall by essentially encapsulating the entire VPN packet in another packet, typically User Datagram Protocol (UDP). The router can then perform the NAT translation on that UDP packet, never actually changing the contents of the VPN packet. If you want to allow VPN traffic to pass through the router, you must enable VPN passthrough.

Routing Features

Because the BEFSR41v4 is targeted at the small office as well as the home user market, it supports some basic routing capabilities to allow it to be deployed in an environment with multiple internal subnets. In addition to being able to configure static routes, the router also supports RIP versions 1 and 2. Although RIP can prove adequate for small environments, the implementation of RIP on the router is extremely basic and lacks any kind of security functions; therefore, you should strongly consider whether this router is the appropriate firewall solution for you if you need the firewall to provide advanced routing functionality. In such cases, a more robust firewall such as the Cisco Secure PIX Firewall might be a better solution.

Management and Administration Features

Most Linksys network devices use a web-based management interface that uses HTTP as the transport protocol. Unfortunately, HTTP does not provide for encryption or security of the data being transported, so you should use caution with regard to the passwords you configure for the router, because they can relatively easily be captured using a network sniffer. By default, the router does not allow management access to the external interface, and although it can be permitted, it is generally a bad idea to do so.

The security model employed by Linksys is a simple shared password security model. All users log in using the same username and password to perform any management functions, and all authenticated users have the same rights.

The Linksys routers also typically provide basic syslog functionality, allowing the router to send events to a syslog server on the same subnet as the internal interface, as well as their own internal log-viewing software known as Log Viewer (which you can find at ftp://ftp.linksys.com/pub/befsr41/).

Miscellaneous Features

Because most home users do not have a Dynamic Host Configuration Protocol (DHCP) server on their home network, most Linksys routers feature DHCP server functionality built in to the router and enabled by default. This functionality allows a user to simply plug a computer into one of the router's switch ports, obtain an IP address that is valid for the router (typically on the 192.168.1.0/24 subnet), and then connect to the router using a web browser on the computer to configure the router accordingly (typically, the router internal interface IP address is 192.168.1.1).

Another feature of newer Linksys routers that can be enabled but is typically disabled by default is Universal Plug-and-Play (UPnP). UPnP allows hosts on the internal network that are using UPnP-capable operating systems to automatically configure the router to allow traffic from the external network to access the corresponding internal network resource. As a general rule, unless this functionality is required, you should disable UPnP on your router.

To facilitate connectivity to various broadband providers, most Linksys routers support multiple Internet connection types. The default setting is just to use DHCP to obtain an external IP address from the service provider, but static assigned IP addresses and PPPoE are supported, as well as solutions specific to certain areas of the world, such as Remote Access Service (RAS), PPTP, and Heart Beat Signal. Because many service providers provide only a dynamic IP address for use on the external interface, most Linksys routers also support dynamic Domain Name System (DNS) through either DynDNS (http://www.dyndns.org) or TZO (http://www.tzo.com). This support allows the router to automatically update the DNS entries for hosts that are protected by the router but need to be Internet accessible (such as websites). In both cases, you need to have a valid account with either DynDNS or TZO for this functionality to work properly.

Linksys Requirements

Most Linksys routers have an extremely small requirements list. Because the assumption is that the router will be connected to a small or home network that lacks any kind of DHCP server, the routers ship with the internal interface configured with the IP address of 192.168.1.1 and are configured to act as a DHCP server to provide IP addresses to any host on the internal network. Therefore, connecting internal hosts to the router for the purpose of configuring the router is very much plug and play. Just plug a host into the internal network of the router (either through the integrated switch on models that feature it, or through a separate hub or switch for models that do not contain a built-in switch), turn the router on, and then turn the computer on. The computer should obtain an IP address, allowing it to communicate with the router.

To provide for the external connectivity, you need to coordinate with the service provider to determine what the requirements are to connect to their network. If the service provider supports DHCP clients, the router will automatically obtain the proper IP address information. If your service provider requires the use of PPPoE or something similar, they will provide you with the appropriate information, and you just configure the router accordingly.

At this point, the router will allow all internal hosts unrestricted access, while allowing no external hosts to initiate access to internal resources.

How the Linksys Router/Firewall Works

Most Linksys routers/firewalls rely on simple NAT routing and basic port filtering to control the flow of traffic through the router. Depending on the direction of the traffic flow, a different filtering methodology is applied.

Filtering Traffic from External Sources

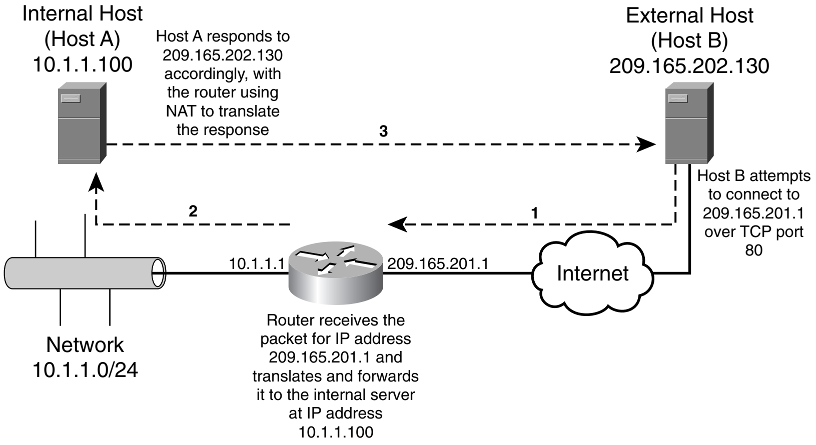
Linksys adheres to the minimalist approach to filtering when it comes to filtering traffic from external sources. By default, all traffic that originates from an external host is blocked by the router/firewall unless it is specifically permitted. This policy ensures that only the traffic you explicitly permit is allowed to access protected resources. Linksys provides three methods of explicitly permitting traffic:

- Port-range forwarding
- Port triggering
- DMZ forwarding

Port-Range Forwarding

Port-range forwarding is the classic port-forwarding configuration that most firewalls and routers implement. With port-range forwarding, you enter the starting and ending port that should be permitted, select the appropriate transport protocol (TCP, UDP, or both), and specify the IP address of the internal host that is providing the specified service. Doing so causes the router to take all traffic received on the external interface that is destined to the specified ports and forward the traffic to the internal host. Unfortunately, there is no way to specify which external hosts should be allowed to access the internal resources, so you are forced to allow all external resources access, or allow none at all. In many cases (for example, a Simple Message Transfer Protocol [SMTP] server), you want all external hosts to be able to access the server, so this is not a problem. If you have an FTP server that you only want certain external hosts to access, however, you really need to implement a firewall other than the Linksys router. Figure 5-2 illustrates how port-range forwarding works with an internal host running a web server.

Figure 5-2 *Port-Range Forwarding*


Internal Host
(Host A)
10.1.1.100
Host A responds to 209.165.202.130 accordingly, with the router using NAT to translate the response
3
External Host
(Host B)
209.165.202.130
Host B attempts to connect to 209.165.201.1 over TCP port 80
2
1
10.1.1.1
209.165.201.1
Internet
Network
10.1.1.0/24
Router receives the packet for IP address 209.165.201.1 and translates and forwards it to the internal server at IP address 10.1.1.100

In Figure 5-2, the router is configured to allow port forwarding for TCP port 80 to the internal web server (HostA) located at IP address 10.1.1.100. The process works like this:

1. The router receives a packet destined to its external IP address using TCP port 80.
2. The router forwards the response to the internal web server (HostA), keeping the source IP address of the original external host (HostB) unchanged.
3. This allows the web server (HostA) to know that it needs to respond to the external host (HostB), the reply to which the router will then translate using NAT, causing the external host (HostB) to think it has been communicating with the router the whole time.

Port Triggering

Port triggering forwards traffic to internal hosts in a similar manner to how port-range forwarding works, with one important difference. Port triggering does not forward any traffic to an internal host until that internal host has initiated some form of traffic for an external destination. When that occurs, the port triggering mechanism automatically allows traffic to be forwarded to the host that initiated the trigger condition.

Port triggering is used primarily to support applications that attempt to communicate with hosts using different ports than what they were contacted on. A common example of this is many gaming applications. For example, Unreal Tournament uses UDP ports 7777 through 7779 to communicate between hosts, but uses port 27900 to communicate with the central game server. Using port forwarding, you would need to potentially permit all of those ports, all the time, to allow a host to run the application. With port triggering, you can configure the router to open ports 7777 through 7779 only after an internal host has attempted to connect to something on the external network using port 27900.

DMZ Forwarding

DMZ forwarding is the most insecure of all filtering methods from external sources because it applies absolutely no filtering. The host still resides behind NAT, but the router will allow all traffic from external sources to access the host in a completely unfiltered and unrestricted manner. For all intents and purposes, you might as well not even have a firewall.

Filtering Traffic from Internal Sources

Filtering of traffic from internal sources breaks with the minimalist approach and applies a terribly flawed filtering philosophy to the router. The router allows all traffic from internal sources, blocking only the traffic that is explicitly defined. The reason for this "backward" implementation speaks to the heart of the debate over security and functionality.

The vast majority of home users do not know what a port is, much less what they should or should not be filtering. By allowing all traffic by default, Linksys ensures that the router/firewall is easy to set up, with little to no configuration required to allow access to external resources. This easy setup dramatically saves technical support costs. Unfortunately, this insecure method of implementation allows all traffic to exit the network (for example, allowing a back door that has been installed on the user's computer to send sensitive information to a host on the Internet or allowing a virus/worm to propagate to external hosts). Because it is so easy to implement, however, ease has won out over security.

Linksys generally supports three levels of filtering of traffic from internal sources:

- By IP address
- By port range
- By MAC address

In all instances, any IP addresses, destination port numbers, or MAC addresses specified will not be allowed to access external hosts.

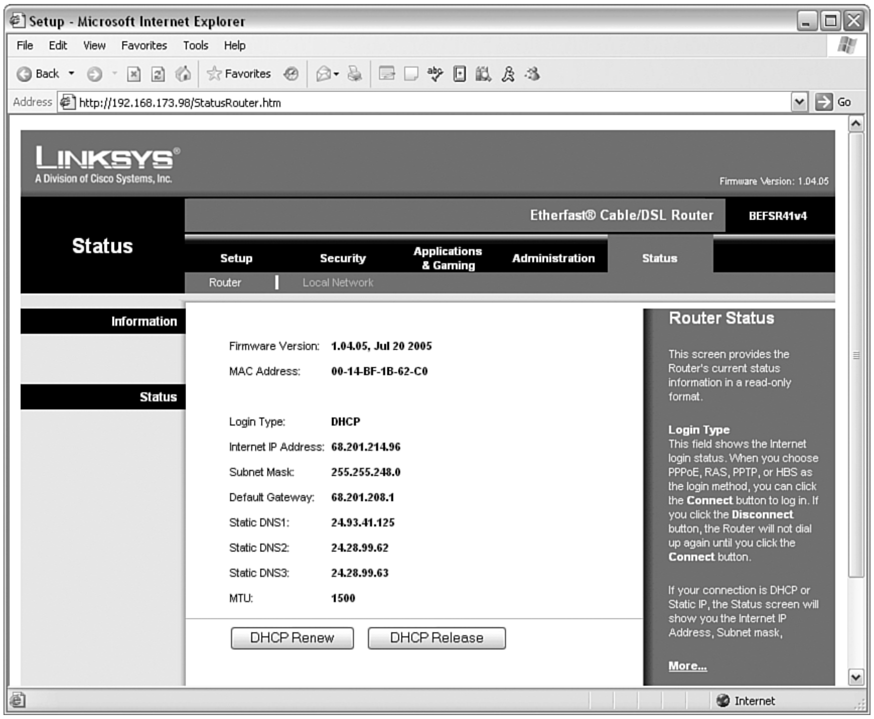
Configuring Linksys

Linksys uses a web-based interface to perform all configuration functions. This interface is accessible by default from any internal host and is accessed using a web browser such as Microsoft Internet Explorer. Upon accessing the web-based interface, you are prompted with a Username/Password dialog box. Refer to the user guide of your appropriate router for the relevant information, but typically the username/password combination of admin/admin is the default user account. You can change the password from the Management screen, which is discussed later in this chapter. In the case of the BEFSR41v4, the interface is separated into five main tabs:

- Setup
- Security
- Applications & Gaming
- Administration
- Status

No configuration settings are accessible from the Status tab. As shown in Figure 5-3, it merely displays the status of the router.

Figure 5-3 *Linksys Status Tab*



http://192.168.173.98/StatusRouter.htm

Firmware Version: 1.04.05, Jul 20 2005
MAC Address: 00-14-BF-1B-62-C0

Login Type: DHCP
Internet IP Address: 68.201.214.96
Subnet Mask: 255.255.248.0
Default Gateway: 68.201.208.1
Static DNS1: 24.93.41.125
Static DNS2: 24.28.99.62
Static DNS3: 24.28.99.63
MTU: 1500

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,

Configuring Basic Setup

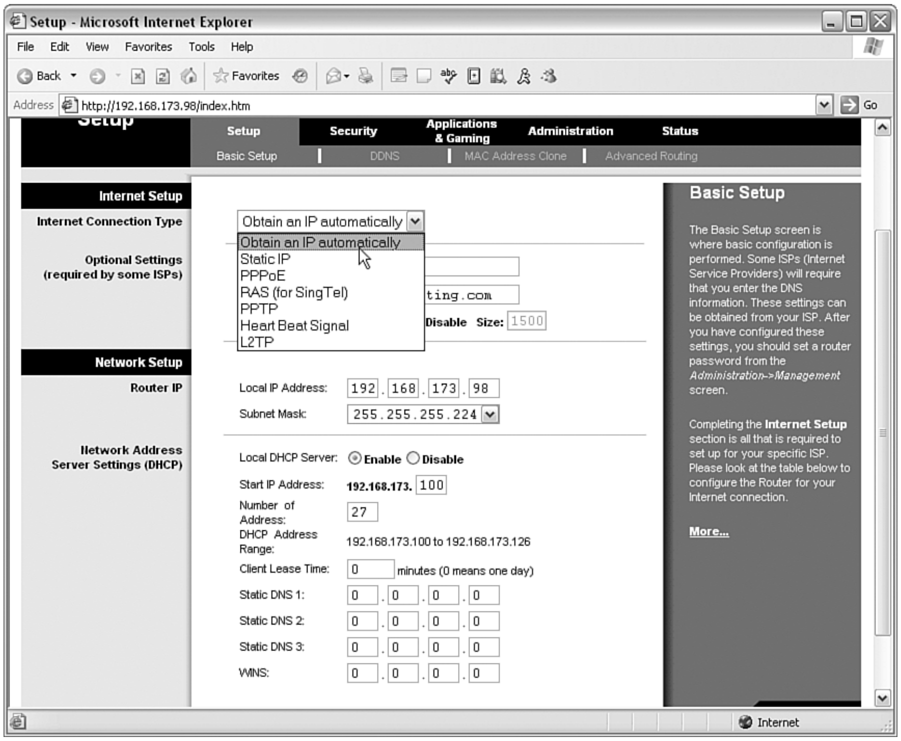
The BEFSR41v4 Setup tab consists of four screens:

- Basic Setup
- DDNS
- MAC Address Clone
- Advanced Routing

On the Basic Setup screen, you can configure how the router connects to the service provider (for example, using DHCP or PPPoE). Depending on which connection type you specify, additional options will be made available on the screen. You can also specify the host and domain name as well as the maximum transmission unit (MTU) for the router, if it is required by your service provider.

The Basic Setup screen is also where you configure the local network settings for the router (such as the internal interface IP address, and the DHCP server settings for the router). In the DHCP settings, you can specify the DNS servers to use; if you leave the values empty, the router automatically uses the values that it obtained from the service provider as the DNS server for the internal clients. Figure 5-4 shows the Basic Setup screen.

Figure 5-4 *Basic Setup Screen*



Address: http://192.168.173.98/index.htm

Internet Setup

Internet Connection Type: Obtain an IP automatically

- Obtain an IP automatically
- Static IP
- PPPoE
- RAS (for SingTel)
- PPTP
- Heart Beat Signal
- L2TP

Optional Settings (required by some ISPs): ting.com; Disable Size: 1500

Network Setup

Router IP
Local IP Address: 192 . 168 . 173 . 98
Subnet Mask: 255.255.255.224

Network Address Server Settings (DHCP)
Local DHCP Server: ● Enable ○ Disable
Start IP Address: 192.168.173. 100
Number of Address: 27
DHCP Address Range: 192.168.173.100 to 192.168.173.126
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

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.

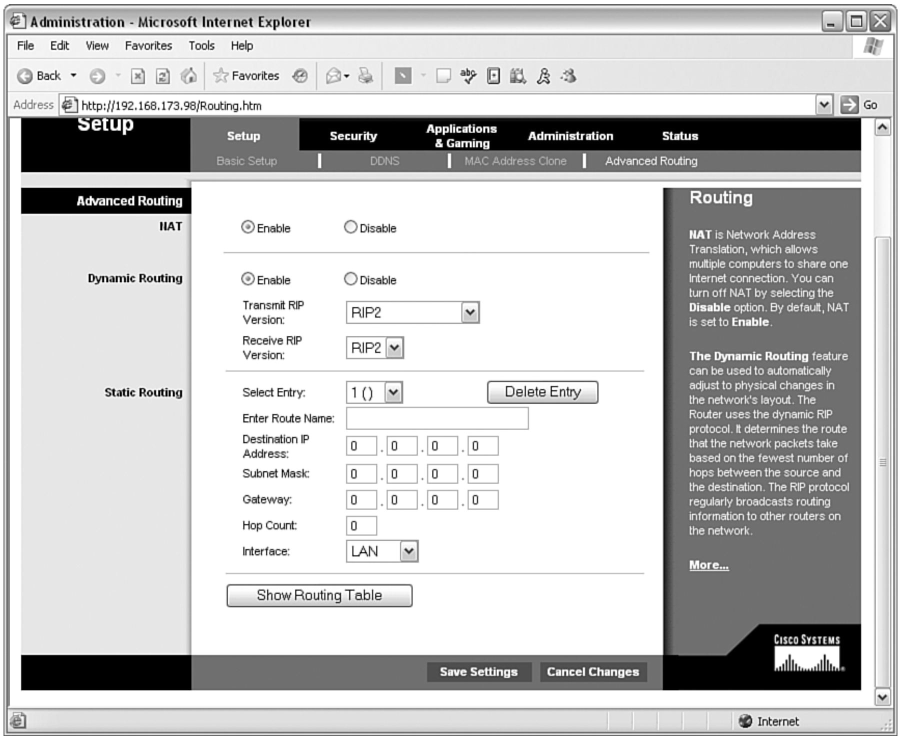
More...

The DDNS screen is where you can configure the router with the appropriate settings to enable it to dynamically update the DNS settings with either DynDNS or TZO when the external IP address of the router changes. Just enter the username (DynDNS) or e-mail address (TZO) that you registered with, along with the appropriate password and domain name, and the router will automatically update DNS anytime the router's external IP address changes.

On the MAC Address Clone screen, you can configure a specific MAC address (for example, if your ISP requires a specific MAC address to be used by your router).

On the Advanced Routing screen, you can configure whether to use NAT as well as configure RIP or static routes, as shown in Figure 5-5.

Figure 5-5 *Advanced Routing Screen*



NAT ● Enable ○ Disable

Dynamic Routing ● Enable ○ Disable

Transmit RIP Version: RIP2

Receive RIP Version: RIP2

Static Routing

Select Entry: 1 () Delete Entry

Enter Route Name:

Destination IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Hop Count: 0

Interface: LAN

Show Routing Table

Routing

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**.

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.

More...

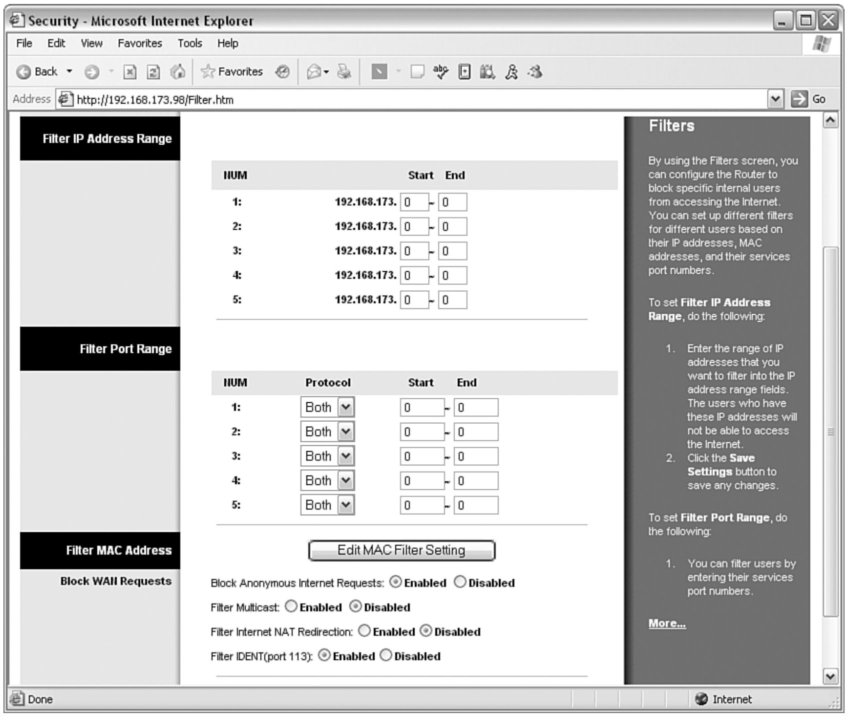
NAT configuration is a simple enable/disable toggle. To enable RIP routing, just select **Enable** and then select the transmit and receive RIP versions from the drop-down boxes. To enter a static route, fill in the appropriate information and specify the interface that the route uses as the exit interface.

Configuring Security

The Security tab consists of two screens, Filter and VPN Passthrough. In both instances, the configuration applies to traffic from the internal network accessing external resources (egress filtering).

The Filter screen is where you can configure IP address, port, and MAC address filtering of internal hosts. For example, if you want to prevent host 192.168.173.115 from accessing the Internet, you can specify that IP address in the Filter IP Address Range fields, and the router will not allow that host to access external resources. Similarly, if you want to prevent certain port numbers from being accessed by internal hosts (for example, instant messenger software or gaming ports), you specify them, too. Keep in mind that the router only supports five entries for either IP address range or port range, so you need to be judicious about what you filter. Figure 5-6 shows the filter screen.

Figure 5-6 *Filter Screen*


Security - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Favorites
Go
Done
Internet

Address http://192.168.173.98/Filter.htm

Filter IP Address Range

NUM		Start		End
1:	192.168.173.	0	~	0
2:	192.168.173.	0	~	0
3:	192.168.173.	0	~	0
4:	192.168.173.	0	~	0
5:	192.168.173.	0	~	0

Filter Port Range

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

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...

If you want to filter by MAC address, just click the **Edit MAC Filter Setting** button and specify the MAC addresses that should be denied access. At the bottom of the screen are four radial selections with the default setting in parenthesis:

- **Block Anonymous Internet Requests** (**Enabled**)—This setting prevents the router from being able to be pinged or otherwise connected to on the external interface, unless you have defined a port-forwarding filter. This should be enabled, but keep in mind that not being able to ping the router can make it more difficult to troubleshoot.
- **Filter Multicast** (**Disabled**)—This setting allows multicast traffic to be forwarded to the appropriate destination. Multicast traffic is traffic destined to multiple hosts. This allows the traffic to be sent one time, while allowing multiple registered hosts to receive it, which it

more efficient than sending the traffic individually to each host (which is a process known as unicast). A host registers to receive this multicast traffic by virtue of the fact that it is running an application that is configured to listen on the corresponding multicast IP address. Multicast is frequently used for the transmission of multimedia and streaming data. Multicast traffic is frequently filtered when it is either unnecessary (for example, because no applications that utilize multicast are running on the network) or to prevent multicast-based attacks from being initiated (for example, to prevent an attack that uses multicast traffic to saturate a network with bogus traffic, thus effecting a DoS on the network). Although somewhat counterintuitive, you want to disable filtering if you want to permit multicast traffic.

- **Filter Internet NAT Redirection** (**Disabled**)—This setting enables you to configure the router to block access to local resources from other local computers that are attempting to access the local resource via the external (NAT) address.
- **Filter IDENT(port 113)** (**Enabled**)—IDENT allows hosts to query the device, and thus discover information about the host. Unless applications specifically require this degree of access, you should always filter IDENT traffic.

On the VPN Passthrough screen, you can configure the router to transparently pass IPSec, PPPoE, and PPTP traffic from internal hosts to external resources. All three settings are enabled by default, and if you are going to use NAT and need to access remote resources using any of the three protocols, you should enable these settings.

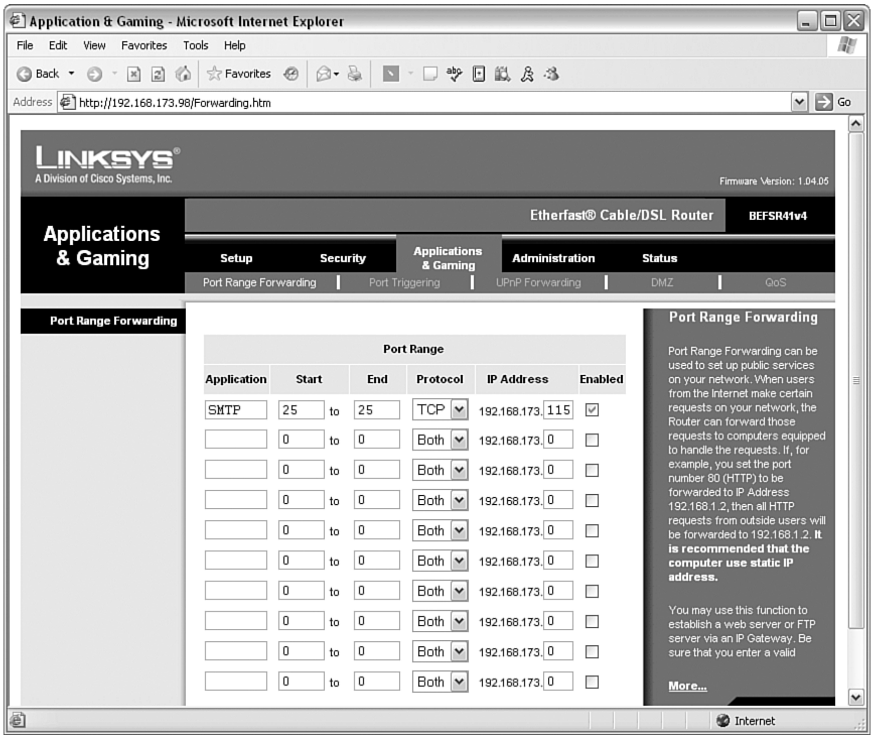
Configuring Applications & Gaming

The name of the Applications & Gaming tab is somewhat misleading because although the settings are typically going to be implemented by home users to support their gaming applications, in function the Applications & Gaming tab is where the configuration of filtering from external sources to internal resources is performed. This tab has five screens:

- Port Range Forwarding
- Port Triggering
- UPnP Forwarding
- DMZ
- QoS

On the Port Range Forwarding screen, you can configure the router to permit certain types of traffic from all external hosts over the specified ports to the specified internal destination. Thus, you can protect servers behind the router/firewall, while still allowing access to the applications and resources on the server from external hosts. For example, if you were running an SMTP server on the internal server located at 192.168.173.115, you would configure the router as shown in Figure 5-7.

Figure 5-7 *Configuring Port-Range Forwarding*


Application & Gaming - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Favorites
Address http://192.168.173.98/Forwarding.htm
Go
LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: 1.04.05
Applications & Gaming
Etherfast® Cable/DSL Router
BEFSR41v4
Setup
Security
Applications & Gaming
Administration
Status
Port Range Forwarding
Port Triggering
UPnP Forwarding
DMZ
QoS
Port Range Forwarding
Internet

Port Range

Application	Start		End	Protocol	IP Address	Enabled
SMTP	25	to	25	TCP	192.168.173. 115	☑
	0	to	0	Both	192.168.173. 0	☐
	0	to	0	Both	192.168.173. 0	☐
	0	to	0	Both	192.168.173. 0	☐
	0	to	0	Both	192.168.173. 0	☐
	0	to	0	Both	192.168.173. 0	☐
	0	to	0	Both	192.168.173. 0	☐
	0	to	0	Both	192.168.173. 0	☐
	0	to	0	Both	192.168.173. 0	☐
	0	to	0	Both	192.168.173. 0	☐

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

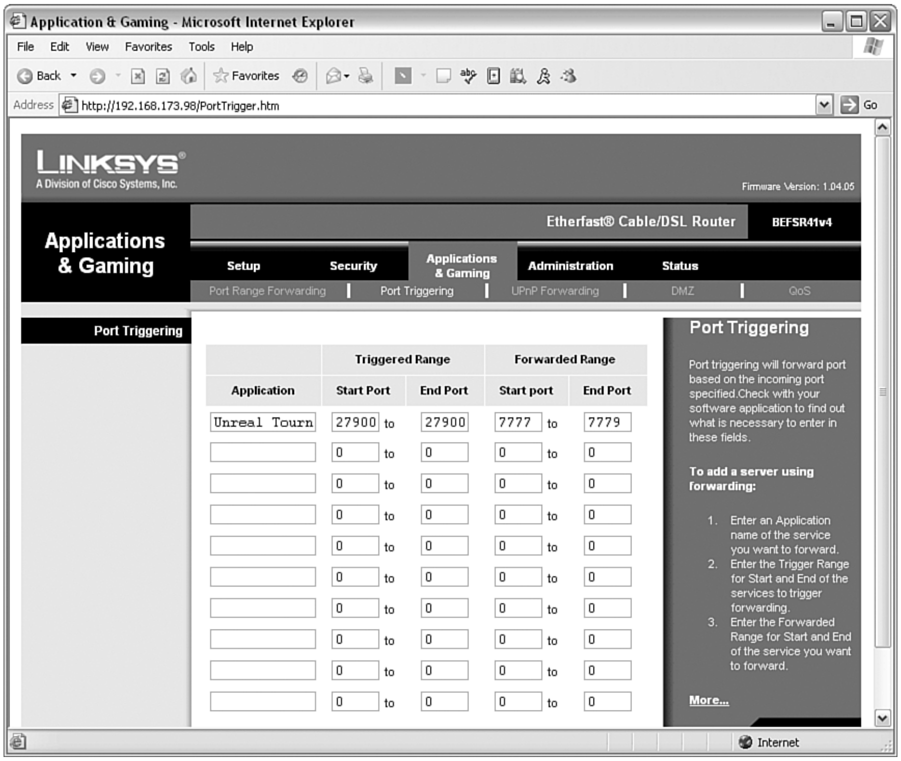
More...

On the Port Triggering screen, you can define a port or range of ports that, when the router detects an internal host attempting to connect to, causes the router to dynamically permit a port or range of ports to be forwarded to the internal host. In this fashion, applications that are running on external servers and that attempt to connect to the internal host over ports other than the one the internal host originally used can be configured to be permitted. This is typically done to support gaming applications, which frequently work by having a computer initiate a connection to a central server on one port and then communicate with any number of other servers using a different set of ports. For example, to support Unreal Tournament, you configure the router as shown in Figure 5-8. In this case, when the router detects an internal host attempting to connect to an external resource using TCP or UDP port 27900, the router automatically configures a forwarding rule to allow all external hosts to connect to the internal host over TCP or UDP ports 7777 through 7779.

On the UPnP Forwarding screen, you can configure port forwarding to UPnP-based devices. Unless you require UPnP, it is recommended to use basic port forwarding, which is more secure because it cannot be manipulated by hosts running the UPnP protocol.

On the DMZ screen, you can identify a single host that will be treated as a completely unfiltered and unprotected host by the router. Although the internal host still uses NAT for communications with external resources, the router/firewall allows all solicited and unsolicited traffic from external sources to the server specified as being in the DMZ.

Figure 5-8 *Configuring Port Triggering*


Application & Gaming - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Favorites
Address http://192.168.173.98/PortTrigger.htm Go
LINKSYS®
A Division of Cisco Systems, Inc.
Firmware Version: 1.04.05
Applications & Gaming
Etherfast® Cable/DSL Router
BEFSR41v4
Setup
Security
Applications & Gaming
Administration
Status
Port Range Forwarding
Port Triggering
UPnP Forwarding
DMZ
QoS
Port Triggering
Internet

	Triggered Range				Forwarded Range			
Application	Start Port		End Port		Start port		End Port	
Unreal Tourn	27900	to	27900		7777	to	7779	
	0	to	0		0	to	0	
	0	to	0		0	to	0	
	0	to	0		0	to	0	
	0	to	0		0	to	0	
	0	to	0		0	to	0	
	0	to	0		0	to	0	
	0	to	0		0	to	0	
	0	to	0		0	to	0	
	0	to	0		0	to	0	

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.

More...

On the QoS screen, you can define specific levels of service and priority for different types of network traffic. Such distinctions are typically done to ensure that latency-sensitive applications such as videoconferencing and Voice over IP (VoIP) are given priority and preferential treatment by the router. On this screen, you can configure the router to essentially place the defined traffic in front of any other traffic, to ensure that the specified traffic is allowed to pass instead of being delayed by other less-important traffic.

You can specify quality of service (QoS) priority by either the device MAC address, the Ethernet switch port that the traffic came from, or the application port in question. For example, if you are running an Internet-based phone, you can specify the MAC address to ensure that all traffic coming from the phone is given preferential treatment by the router. There are two priorities, low and high, allowing you to decide how the traffic should be treated.

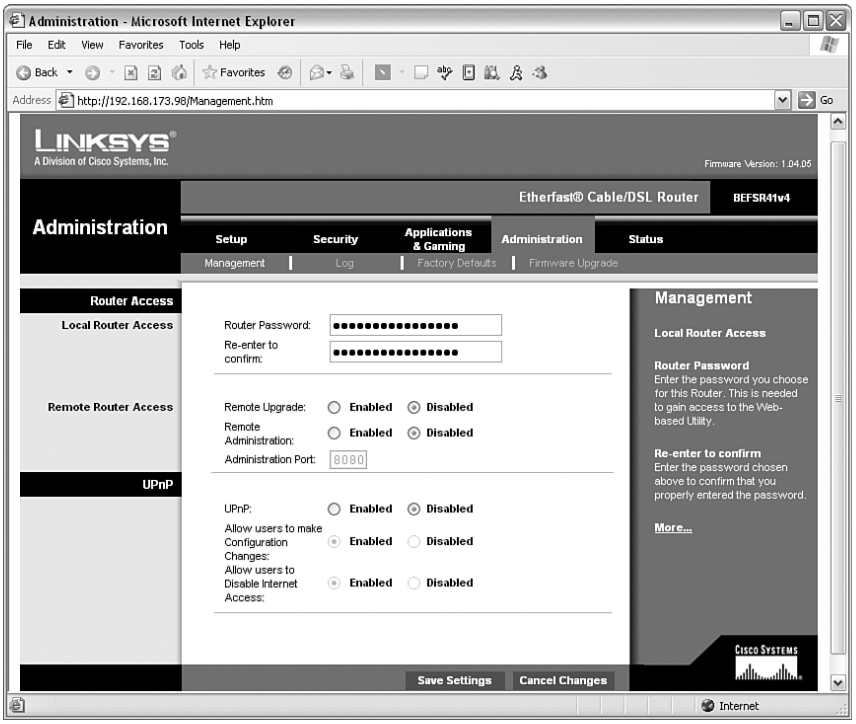
Configuring Administration

On the Administration tab, you can define how the router will be managed and how logging should be configured. You can also perform software upgrades and reset the router to the factory defaults.

The Management screen is used to specify what the router password is. Keep in mind that all users will access the router web-based interface using the same password, so you should consider using a unique password for the router and sharing the password with as few people as possible. In addition, you can configure the router to allow remote management access, which can prove handy if your company has distributed the routers to remote locations, but expects the routers to be managed by a central entity. As a word of caution, however, permitting remote access allows anyone on the remote network who knows the password to potentially be able to access and configure the router; therefore, unless you really need this functionality, you should disable it. Also, keep in mind that because the router uses HTTP as the access protocol, all the data being transmitted—including passwords—is sent in an unencrypted format, which means anyone with a network sniffer can capture and obtain that information. As a general rule, remote management access should not be permitted, and you should ensure that Block Anonymous Internet Requests is enabled on the Security|Filter screen.

The Management screen is also where you can configure the router to use UPnP to automatically configure the router to open ports and permit traffic. This is used in conjunction with the UPnP Forwarding screen of the Applications & Gaming tab that was previously mentioned in this chapter. Because UPnP allows for the automatic configuration of the router from UPnP hosts, unless you require UPnP it should be disabled, which is the default setting. Figure 5-9 shows the Management screen.

Figure 5-9 *Management Screen*



Address: http://192.168.173.98/Management.htm

Router Password: ●●●●●●●●●●●●●●●●

Re-enter to confirm: ●●●●●●●●●●●●●●●●

Remote Upgrade: ○ Enabled ● Disabled

Remote Administration: ○ Enabled ● Disabled

Administration Port: 8080

UPnP: ○ Enabled ● Disabled

Allow users to make Configuration Changes: ● Enabled ○ Disabled

Allow users to Disable Internet Access: ● Enabled ○ Disabled

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.

More...

On the Log screen, you can specify the IP address of a syslog server and enable logging from the router. The Factory Defaults screen contains a simple toggle selection that enables you to reset the router to the factory defaults.

If you need to upgrade the software on the router, you can do so on the Firmware Upgrade screen. You can browse for an upgrade file on the local computer that is managing the router and click the button to upgrade. When the router has been upgraded, it reboots to begin running the new code.

Linksys Checklist

To implement a basic Linksys router, perform the following tasks:

Step 1 Obtain the connection information required by your ISP.

Step 2 Plug the router into the service provider device or network jack using the external/WAN interface of the router.

Step 3 Connect a computer that is configured to be a DHCP client to one of the switch ports on the router.

Step 4 Turn the router on.

Step 5 Turn the computer on. The computer should automatically obtain an IP address from the router, allowing it to connect to the router.

Step 6 Using a web browser, connect to the router's internal network interface IP address, typically http://192.168.1.1. When prompted, enter the default username (admin) and password (admin).

Step 7 At the Setup tab, configure the router using the information from Step 1.

Step 8 At the Management screen of the Administration tab, enter a new password.

Step 9 At this point, the router should allow all traffic to external destinations, while blocking access to all internal resources from external sources.

Step 10 If you require filtering, define the appropriate port-range forwarding (for ingress filtering) or filtering (for egress filtering) rules as needed.

Step 11 Test connectivity to external resources from internal systems, and to internal systems as defined by the port-forwarding rules from external systems.

Summary

Linksys broadband routers provide a simple, NAT-based packet-filtering router solution (some of which include stateful packet inspection) for small office environments as well as for home-based networks and users. Although some broadband router models lack the robustness of stateful packet-inspecting firewalls and lack granularity for configuring port forwarding, you can use them in simple environments where the security risk does not justify a substantial investment. If you require granular filtering rules, or if you require more advanced filtering mechanisms than simple NAT and port forwarding, you should consider implementing a more advanced firewall such as the Cisco Secure PIX Firewall, Microsoft ISA Server, or NetFilter over Linux.