Global Information Assurance Certification Paper

GSEC Security Essentials Practical
Version 1.2f

Getting the Most Security out of the Linksys® Cable/DSL Router

Earl Charnick
echarn2001
Fall 2001 – Original
Online via
Mary Washington College
James Monroe Center

Introduction

The FCC reports that more than 7.1 million lines connected homes and businesses to the Internet in 2000, with DSL enjoying a whopping 435 percent rise in subscriptions over the previous year.[1] With statistics like this, it is no wonder security is such a hot topic. A common form of security implemented in small business and home networking environments is the use of cable/DSL routers. Providing extra security at a minimal cost with little expertise to setup and maintain makes these low-end routers very attractive to the general public.

One such model is the Linksys® EtherFast Cable/DSL Router with the following security features:

- NAT (Network Address Translation) – Maintains internal-external connection mapping data to public IP address to hide internal hosts from the Internet.
- Address and Port Filtering – Prevents internal hosts from connecting to restricted external sites and/or services.
- SPI (Stateful Packet Inspection) – Verifies destination address of traffic matches the original source address of the original request.
- Port Forwarding – Provides ability to host services without completely exposing the server.
- Switch Behavior – Internal interfaces are segregated to improve bandwidth by reducing network traffic.

Configuration

Configuring the Linksys® router is made simple with the built-in HTML user interface. The router comes out of the box with 192.168.1.1 defined as the local area network IP address. So to start the configuration process, use a web browser and make a request for http://192.168.1.1 from any of the router's local interfaces.

A username and password dialog should then appear. Leaving the user name field blank, fill in the password field with 'admin' and press 'Enter'. The LAN device IP address and password factory defaults can be modified as will be described in later steps. If the setup web screen does not appear or errors are encountered, refer to the troubleshooting steps below.

The following configuration sections are based on firmware version 1.40.2. As the firmware changes, so do the configuration options and pages. Upgrading the router's firmware is relatively easy and should be applied as newer versions become available. Extra features, bug fixes, and security changes are just a few reasons to do so. Check http://www.linksys.com/download/firmware.asp for current firmware versions. If a firmware upgrade is required, refer to the section on upgrading firmware.

SETUP

The setup screen contains the basic information required to get the router working. Your specific settings will be based on your Internet service provider, ISP, and what they required for you to connect to their service.

[1] Gill, Lisa. "Broadband Use Skyrocketing – FCC"

If the ISP has assigned a host and/or domain name to use, fill these into the host name and domain name fields. Typically, these will be used to query the ISP's DHCP server to determine the IP configuration assigned for your service account.

Depending on the network the router is placed; the default router LAN IP address and/or subnet mask may require changing. For example, if the router is placed within an already established network with a different address mapping scheme than the default, an update to the subnet mask and network segment would be required.

Some ISPs assign static IP addresses that will never change, others use DHCP to assign IP addresses based on host names and/or network card MAC addresses. If your ISP uses DHCP to assign your public address configuration, then the 'WAN IP Address' field should be set to 'Obtain an IP Address Automatically'. Otherwise, choose 'Specify an IP Address' and fill in the ISP provided values for your IP address, subnet mask, default gateway address, and up to three DNS servers.

If your ISP requires logging in to their services, then fill in the user name and password fields. In most cases, this is required for DSL types of service. Select your service type 'PPPoE' or 'RAS'.

> PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices.[2]

RAS, remote access service, is similar service that is supported.

If a cost is associated with maintaining the Internet connection, the optional 'Connect on Demand' and 'Keep Alive' parameters can be configured to manage when to connect and disconnect in order to save money.

PASSWORD

The default 'admin' password of the router is a **MUST** to change. With the ability to connect on any local interface to the router, keeping the obvious default password is a major security hole waiting to be exploited, not to mention one of SANS top ten most critical Internet security threats:

> Some systems come with "demo" or "guest" accounts with no passwords or with widely-known default passwords. Service workers often leave maintenance accounts with no passwords, and some database management systems install administration accounts with default passwords. In addition, busy system administrators often select system passwords that are easily guessable ("love," "money," "wizard" are common) or just use a blank password. Default passwords provide effortless access for attackers. Many attackers try default passwords and then try to guess passwords before resorting to more sophisticated methods. Compromised user accounts get the attackers inside the firewall and inside the target machine. Once inside, most attackers can use widely-accessible exploits to gain root or administrator access.[3]

[2] "PPPoE – a searchNetworking definition."
[3] "How to Eliminate the Ten Most Critical Internet Security Threats."

In the event the password is lost or forgotten, a hardware reset is required to recover the factory defaults. This screen also has the ability to perform a soft reset to put the router configuration back to factory defaults. However, if access can't be gained to the router, a pen button exists on the front of the router and is used as the hardware reset.

*****WARNING*** ***WARNING*** ***WARNING*****

The largest security issue identified with the Linksys® router is changing the administrator password. Changing the password is submitted to the router through a CGI web interface call in plaintext form. Using windump on the administrator's interface during a password change showed the following output:

```
21:58:54.872755 DUKE'S.2794 > 192.168.1.1.80: P 0:467(467) ack 1
win 8760 (DF)
0x0000   4500 01fb 71ee 4000 8006 034e c0a8 016f  E...q.@....N...o
0x0010   c0a8 0101 0aea 0050 0ae3 2be5 0000 de09  .......P..+.....
0x0020   5018 2238 288a 0000 4745 5420 2f47 6f7a  P."8(...GET./Goz
0x0030   696c 612e 6367 693f 7379 7350 6173 7377  ila.cgi?sysPassw
0x0040   643d 6164 6d69 6e26 7379 7350 6173 7377  d=admin&sysPassw
0x0050   6443                                     dC
```

Therefore, make every attempt to verify the administrator's workstation is on a trusted segment and protected against network traffic sniffing while updating the password!!!

*****WARNING*** ***WARNING*** ***WARNING*****

STATUS

At any time, this screen shows how the router is currently configured. It has a similar layout to the setup screen with a few more options. If DHCP is used on the WAN interface, DHCP releases and refreshes are accessible via two buttons on this screen. If the router is acting as a DHCP host on the local network, the ability to view its client table is also available.

DHCP

By default, the Linksys® router is configured to be a DHCP server for the local interfaces. To turn this feature off, click 'Disable'. Keep in mind, only one DHCP server can exist on your subnet. If desired, the ability to specify the starting IP address and the number of DHCP users exists.

LOG

Logging should always be enabled; unfortunately, the router can only store up to the last seventy outgoing and the last seventy incoming requests. If a scripted probe were to occur, the logs would quickly wrap. With the aid of the Windows logviewer tool, or any other logging application that handles SNMP-TRAP (UDP port 162) messages, this limitation can be overcome. In the 'Send Log to' field, fill in the IP address of the server running the logging application. Network connection traces are invaluable to intrusion analysts to discover hackers, their attacks, and what they compromise.

SECURITY

With 1.40.2 firmware, a firewall and a virus software interface has been created. The security of the router has improved with the aid of ZoneAlarm Pro firewall and PC-Cillin virus software packages. With the purchase and use of these products on the internal hosts, two more layers of protection are added to our ideal defense-in-depth architecture.

In order to activate the extra firewall protection, the ZoneAlarm Pro license key has to be entered and the option to 'Enforce ZoneAlarm Pro Security' selected. For maximum protection, use the 'More secure' option; however, if bandwidth consumption becomes an issue, use the alternative 'Conserve Bandwidth' option.

With the PC-Cillin virus software installed locally on the hosts, select 'Enforce PC-Cillin Anti-Virus' option to enable extra virus protection.

For those hosts that are not using the extra security features, a range of IP addresses can be given to exempt extra traffic those hosts. Fill this in the 'Exempt Computers' fields and 'Enable' the option if exempt hosts exist.

FILTERS

For those internal hosts that should not have Internet access, a filtering capability exists. Up to five ranges of addresses can be specified. Enter in line by line the range of hosts to restrict access.

A filtering capability also exists for Internet service requests that are prohibited from the internal network. Up to five protocols and port ranges can be specified. For each restricted service, fill in line by line the protocol and port range pair.

For those internal hosts identified by their MAC addresses, up to fifty hosts can be given for the router to filter from having Internet access. Select 'Edit MAC Filter Setting' and fill in restricted address values.

By selecting 'Enable' for the 'SPI' option, the router changes the internal firewall from the NAT firewall to the stateful. From this point on, for every originating request, the source address is saved. As return traffic comes back, if the destination address is not in the list of originating source addresses, the router drops the traffic. Since NAT is turn off, the hosts have to have valid routable address. Also, all port forwarding is turned off. Since the servers will not originate traffic, their addresses would not be in the state table as awaiting return traffic. Therefore, this option has to be disabled if running any type of server or the use of NAT is desired.

Due to reconnaissance probes using ICMP traffic, disabling the router's ICMP echo-reply is highly recommended. 'Enable' the 'Block WAN Request' to prevent the router responding to Internet ICMP echo-request traffic.

UDP multicast traffic can be blocked from entering the internal network via selecting 'Enable' for 'Multicast Pass Through'. If there is no need to allow multicast data into the network, then it should be enabled to deny this traffic.

Enabling the 'IPSec Pass Through' allows internal client to negotiate security parameters.

Enabling the 'PPTP Pass Through' allows internal clients to establish VPN connections. Disable this feature if VPN is not part of your network.

Disabling 'Remote Management' is strongly suggested. With this feature enabled, anyone establishing a connection from the WAN interface has the potential to access the router configuration.

Disabling 'Remote Upgrade' is also strongly suggested. With this feature enabled, the router is listening on the WAN interface for TFTP traffic. Exposed to an attack from the Internet, the router's firmware could potentially be compromised.

MTU feature is more for performance issues. This allows you to specify the maximum transmission unit allowed through the router before fragmentation is required. Recommend using 1492 for DSL connections; otherwise, the default value of 1500 is used when disabled.

FORWARDING

The Linksys® router has the ability to forward external service requests to internal servers based on port and protocol. Preferred method to using the DMZ method, which completely opens the machine to everyone and everything. For each public service, fill in line by line the port range, the desired the protocol, and the IP address of the server for that service. For single port services, specific a start and end range of the same port number.

DYNAMIC ROUTING

Dynamic routing allows the router to adjust as the network layout changes (i.e. network path changes). When there are no other routers present on the network, this feature is not needed and 'Gateway' should be the 'Working Model'. When this router is used in conjunction with other routers, select 'Router' as the 'Working Model'. With 'Router' selected, receive and transmit routing protocols have to be chosen. For receiving, RIP1 or RIP2 is available; as transmitting also has RIP1-Compatible available. RIP, Routing Internet Protocol, is a distance-vector protocol; meaning the route a packet takes is based on the fewest number of hops to the destination. A protocol used between routers to update and maintain routing table information.

STATIC ROUTING

If the router is used between more than one network, static routes may be required to send establish network to network traffic. Up to twenty static routes can be specified.

DMZ HOST

Specifying a host IP address on this screen places that host on the demilitarized zone. Any connection attempt made on the WAN interface of the router is directed to the given host. This host in essence is directly connected to the Internet and becomes wide open to attacks. I strongly recommend port forwarding over this option. However, for cases where a large number of dynamic ports are required, this may be the only option. If this option is desired, it is strongly recommended a firewall product be installed on the host. Enter the host IP address to expose in the 'DMZ Host IP Address' field.

MAC ADDRESS CLONE

Some ISPs require the customer to register a network interface card's MAC address with their service. Once registered, only the computer with that card would have access. This feature mimics a given MAC address, thus allowing the router to configure to the ISP service without removing the originally registered network interface card. If required to do so, fill in the hexadecimal MAC address to use on the WAN interface of the router.

Confirm Configuration

After hardening the Linksys® router, its time to verify it is working as desired.

1. Verify the administrator password has been changed. From an internal site, request http://<IP>, where IP is the router's internal address. When the dialog appears, enter 'admin' in the password field. If authentication fails, the administrator password is no longer 'admin.'
2. Verify 'Block WAN Request' is working. From an external Internet host, type 'ping <IP>', where IP is your public IP address. As long as an echo-reply is not received back, the router is correctly dropping ICMP requests.
3. Verify 'Remote Management' is disabled. From an external Internet host, try to connect to http://<IP>:8080, where IP is your public IP address. If this request fails, remote management of the router is disabled.
4. Verify 'Remote Upgrade' is disabled. From an external Internet host, try to upgrade the router's firmware following the upgrade procedure using your public IP address. After a few seconds, a message indicating the server is not responding should appear indicating remote upgrade is disabled.
5. Verify filtering IP addresses is working. For all filtered private IP addresses, attempt to make a connection to a non-filtered public service on the Internet. If a dump trace on the external interface of the router shows no traffic for the attempt, filtering of the private addresses is working.
6. Verify filtering private service ports is working. For all filtered private ports, attempt to make a connection to a restricted Internet service from an internal host,

which has Internet privileges. If a dump trace on the external interface of the router shows no traffic for the attempt, filtering of the private ports is working.
7. Verify filtering MAC addresses is working. From all filtered MAC addresses, attempt to make a connection to a non-filtered public service on the Internet. If a dump trace on the external interface of the router shows no traffic for the attempt, filtering by MAC addresses is working.
8. Establish connectivity to the services from an external Internet site to check their availability. Using a dump trace on the local interface of the servers would also indicate the traffic is forwarded to the proper host.
9. Run a port scanner, such as nmap, against the public Internet IP address to determine if unwanted ports are open or forwarded.
10. Verify logging is working before, during, and after all tests and they don't contradict the test results.

Firmware Upgrade Procedure

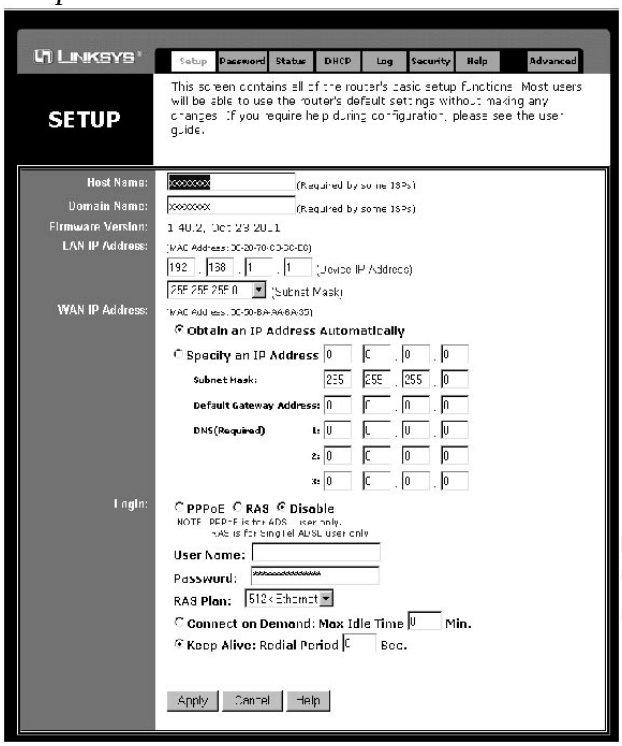
1. Backup current configuration.
2. Download the latest firmware version from: http://www.linksys.com/download/firmware.asp
3. Uncompress the zip file.
4. Run the Tftp.exe command.
5. Fill in the IP address of the internal router interface.
6. Fill in the password for administrator access.
7. Fill in the path to the extracted 'code.bin' file.

Troubleshooting

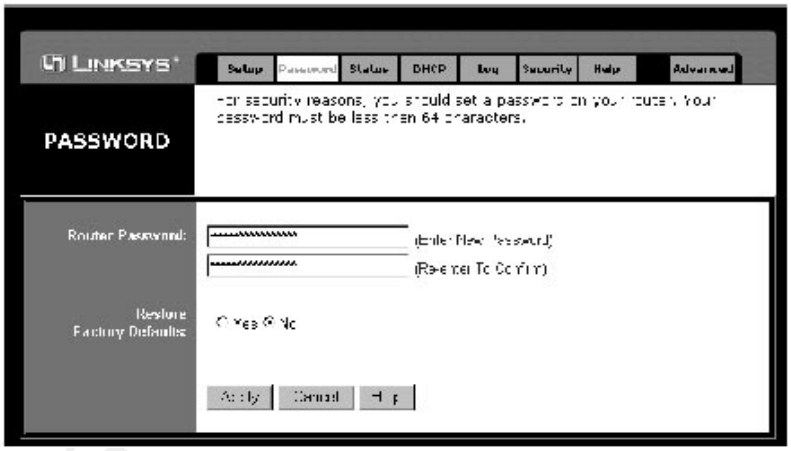
1. Verify Internet connected to WAN interface and all internal network segments are connected to the LAN interfaces of the router.
2. Verify power and LED lights are showing 'green' status.
3. Verify status page showing correct configuration, if not; try releasing then renewing the DHCP configuration for the WAN interface.
4. Verify DHCP client information in router tables.
5. Press the reset button on the router to restore factory settings and reconfigure.

Screen Shots

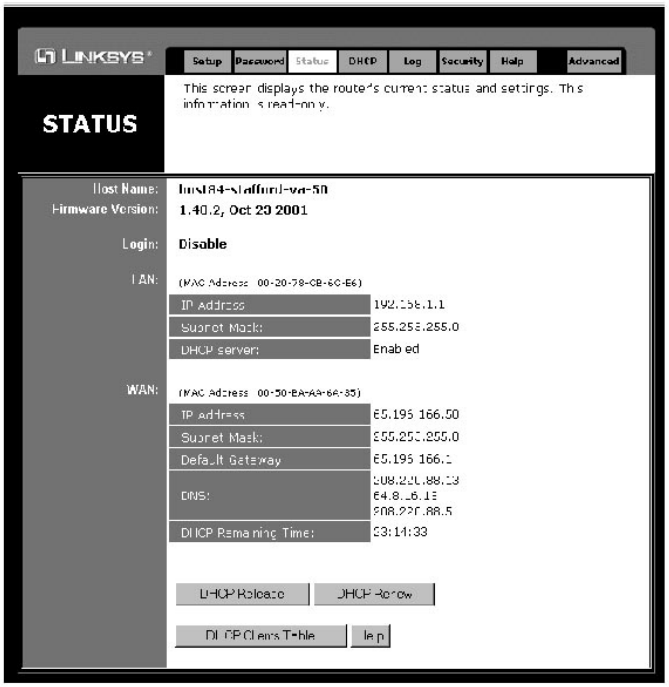
Setup



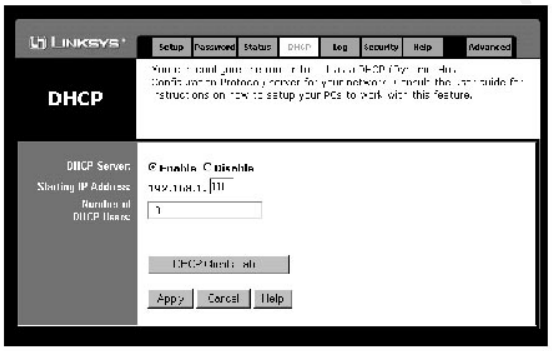
Password



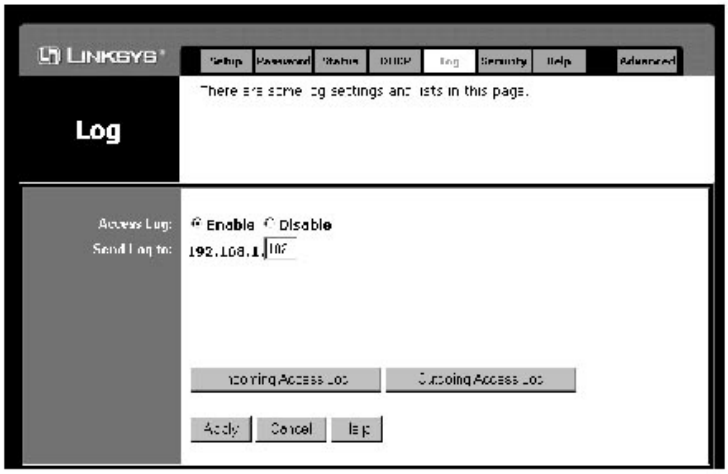
Status



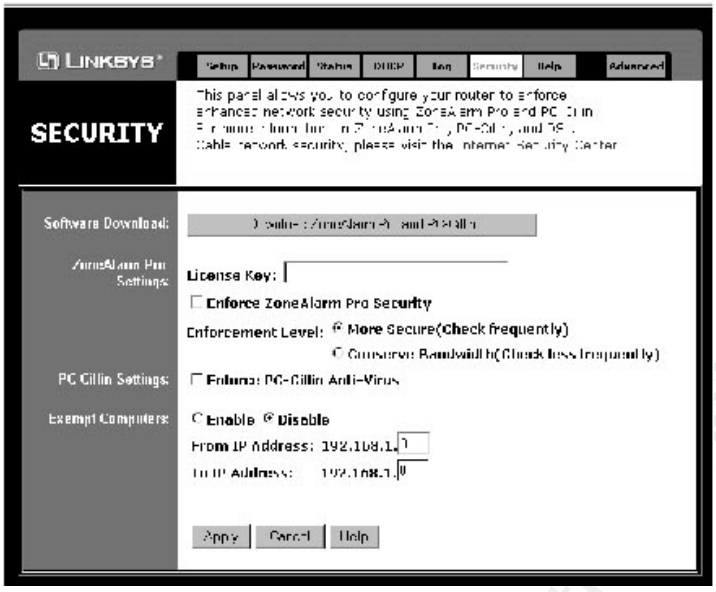
DHCP



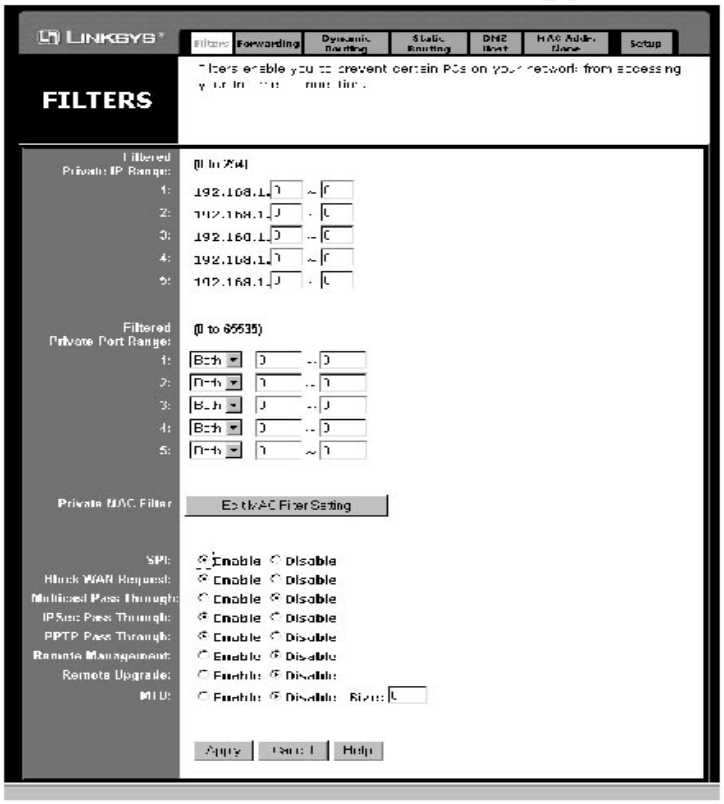
Log



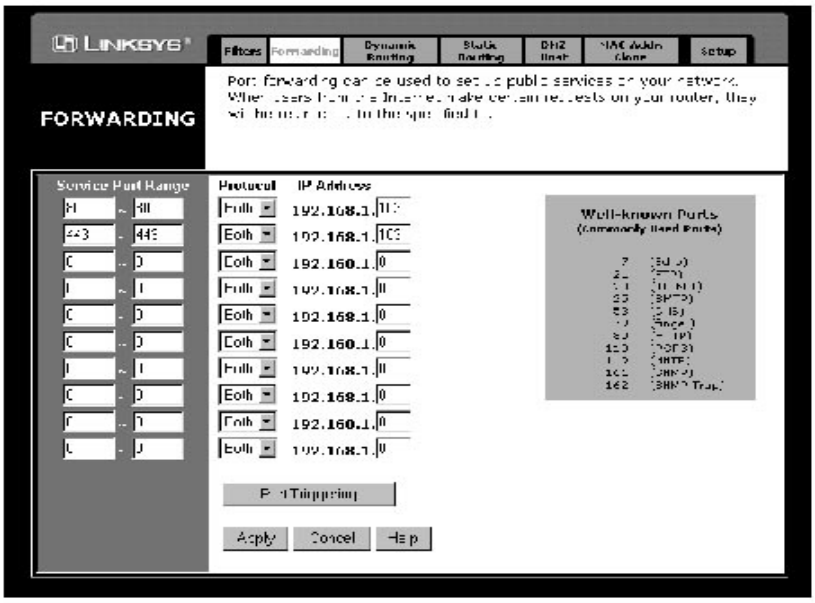
Security



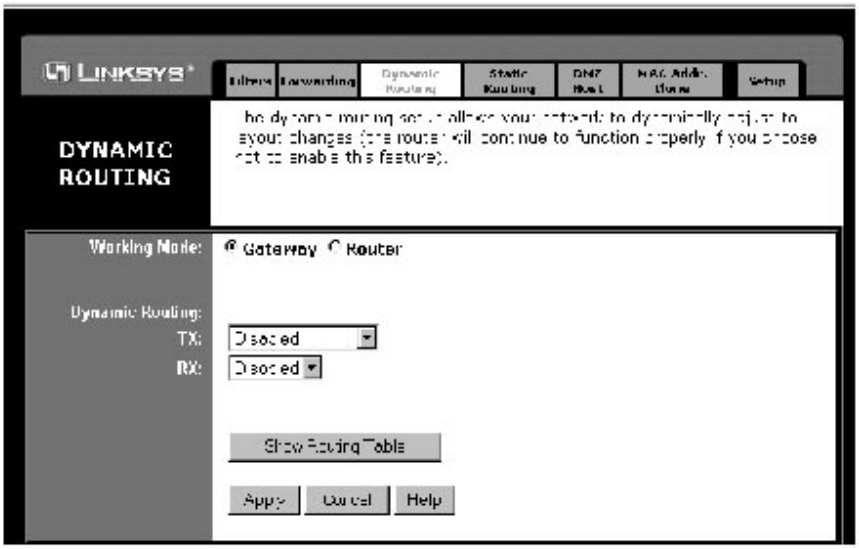
Filters



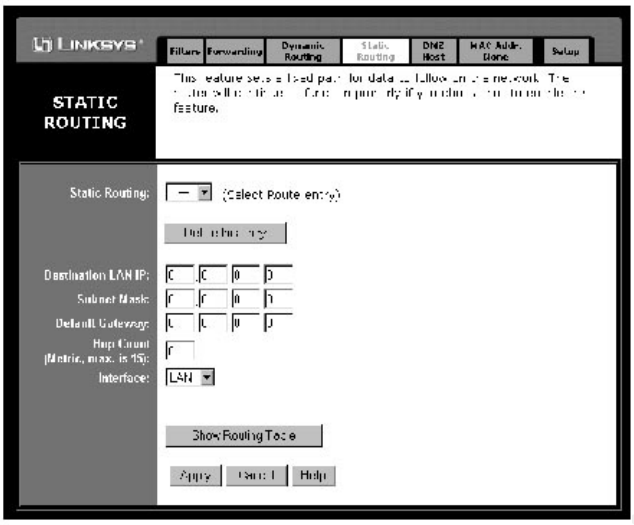
Forwarding



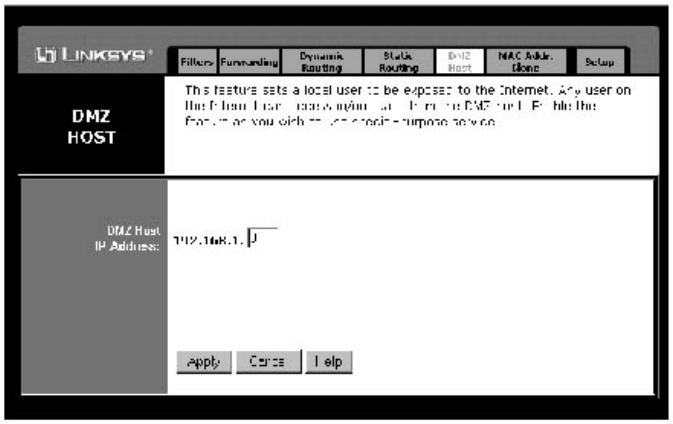
Dynamic Routing



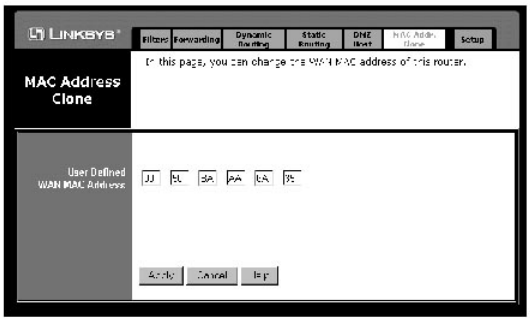
Static Routing



DMZ Host



MAC Address Clone



References

McCabe, Mike. "Cable/DSL Router and Personal Firewall: Belt and Suspenders?" URL: http://www.sans.org/infosecFAQ/homeoffice/cable.htm (30 Nov. 2001)

"How to Eliminate the Ten Most Critical Internet Security Threats." Version 1.33 25 Jun. 2001. Copyright 2000 – 2001, The SANS Institute. URL: http://www.sans.org/topten.htm (30 Nov. 2001)

"PPPoE – a searchNetworking definition." Jul 27, 2001. URL: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214430,00.html (30 Nov. 2001)

"Etherfast Cable/DSL Routers User's Guide." UG-BEFSR11/41/U31-010521A-AC. URL: ftp://ftp.linksys.com/pdf/befsr11&befsr41ug.pdf (30 Nov. 2001)

"Linksys cable/DSL Router Help-Port Forwarding." URL: http://www.practicallynetworked.com/support/linksys_router_help_pg4.htm (30 Nov. 2001)

Gill, Lisa. "Broadband Use Skyrocketing – FCC." 10 Aug. 2001. NewsFactor Network. URL: http://www.newsfactor.com/perl/story/12705.html. (30 Nov. 2001)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS