About This Guide

The guide contains information about the Cisco Broadband Operating System (CBOS) and is intended for system and network administrators. It is intended for use as a reference guide providing commands that manage any Cisco-based network that implements CBOS as its operating system software.

Audience

This guide is intended for system managers, and network administrators. This guide assumes you have a working understanding of networking concepts.

Document Organization

The Cisco Broadband Operating System User's guide is organized into the following chapters and appendixes:

- Chapter 1. Introduction to the Cisco Broadband Operating System (CBOS) introduces the CBOS system and provides a detailed list of all its features. Also included are descriptions on how to use the help system and the CBOS user interface.
- Chapter 2. Using the Command Line Interface consists of all the commands available in the CBOS system. Each command is described on separate pages and formatted similarly to the industry-standard UNIX man page structure.
- Chapter 3. Using the Web Interface describes how to setup and configure the Cisco 675 Router, through a web browser, using the Web Management Interface.
- Appendix A. ADSL Technology Glossary provides a complete listing of all ADSL-related nomenclature.

Document Conventions

This publication uses the document conventions listed in Table 1, Table 2, and Table 3.

Table 1 Font Conventions

Convention	Definition	Sample
Times bold	Text body font used any argument, command, keyword, or punctuation that is part of a command that the user enters in text and command environments.	This is similar to the UNIX **route** command.
Times italic	Text body font used for publication names and for emphasis.	See the *Cisco 6100 Series User Guide* for further details.
`Courier`	Font used for screen displays, prompts, and scripts.	`Are you ready to continue? [Y]`
`Courier bold`	Font used to indicate what the user enters in examples of command environments.	Login: **`root`** Password: <**`password`**>

Table 2 Command Syntax Conventions

Convention	Definition	Sample
Vertical bar (|)	Separates alternative, mutually exclusive elements	**offset-list** {**in** | **out**} *offset*
Square brackets ([ ])	Indicate optional elements	[**no**] **offset-list** {**in** | **out**} *offset*
Braces ({ })	Indicate a required choice	**offset-list** {**in** | **out**} *offset*
Braces within square brackets ([{ }])	Indicate a required choice within an optional element.	[{*letter*|*number*}**Enter**]

Table 2 Command Syntax Conventions (continued)

Convention	Definition	Sample
Boldface	Indicates commands and keywords that are entered literally as shown	[**no**] **offset-list** {**in** | **out**} *offset*
Italics	Indicate arguments for which you supply values **Note** In contexts that do not allow italics, arguments are enclosed in angle brackets (< >).	**offset-list** {**in** | **out**} *offset*

Table 3 Note, Timesaver, Tip, Caution, and Warning Conventions

Convention	Description
Note	Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the guide.
Timesaver	Means *the described action saves time*. You can save time by performing the action described in the paragraph.
Tip	Means *the following is a useful tip*.
Caution	Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.
Warning	Means *danger.* You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. To see translated versions of the warning, refer to the Regulatory Compliance and Safety document that accompanied the device.

Companion Publications

The following are the companion publications to the *Cisco Broadband Operating System User Guide.*

- *Release Notes for the Cisco Broadband Operating System Release 2.1.0.*

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

Note To view or print any CBOS legacy documentation (material released prior to Release 2.1.0), access the World Wide Web at http://www.netspeed.com/. Click **Technical Support**.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

CHAPTER 1

Introduction to the Cisco Broadband Operating System

This chapter provides an overview of the Cisco Broadband Operating System (CBOS) and its features. CBOS is the common operating system for all Cisco Customer Premise Equipment (CPE), including the Cisco 675, the Cisco 675e, the Cisco 676, and the Cisco 677.

Note These products are referred to as the Cisco 67x product line. When you see 67x in this documentation, substitute the hardware product you are using.

The CBOS is modeled after the Cisco Internetworking Operating System (IOS) and features a similar command syntax and format.

This chapter includes the following sections:

- CBOS Features
- CBOS User Interfaces
- CBOS Help System

For more information on using the CBOS, refer to Chapter 2, “Using the Command Line Interface.”

The list below defines the terminology used in this chapter.

- **Dynamic Host Configuration Protocol (DHCP)—**Assigns IP addresses and other configuration parameters to hosts dynamically. The DHCP protocol is described in RFC 2131, which obsoletes RFC 1541.
- **Network Address Translation (NAT)—**Converts IP addresses on a private network (designated as “inside” or “LAN”) to global IP addresses that are valid on another registered network (designated as “outside” or “WAN”). NAT operates on a router that connects two or more networks together. Port-level multiplexed NAT is used to translate all internal private addresses to ports within one or more outside registered IP addresses.
- **PPP/Internet Protocol Control Protocol (IPCP)—**Dynamically configures IP addresses over Point-to-Point Protocol (PPP). The Cisco CPE family uses PPP/IPCP to dynamically negotiate its own registered WAN interface IP address from a central access server. PPP/IPCP and DHCP are different methods of assigning addresses. The 67x can also be provisioned to obtain its LAN-side (ETH0) address via IPCP.
- **DHCP Client—**An Internet host using DHCP to obtain configuration parameters such as a network address.
- **DHCP Server—**An Internet host that returns configuration parameters to DHCP clients.
- **Inside—**The set of network addresses that are subject to conversion by NAT. These addresses exist on the LAN side of the router.
- **Outside—**Commonly referred to as legal or global addresses. These addresses exist on the WAN side of the router.
- **Outbound Traffic—**Traffic from an inside host to an outside host
- **Inbound Traffic—**Traffic from an outside host to an inside host.
- **Lease Time—**The amount of time that an address given to a DHCP client by a DHCP server remains valid. The lease time can be either:
  - A finite lease-time in which the client must renew the lease before it expires in order to continue using the address.
  - An infinite lease-time in which the client maintains the same IP address as long as it stays connected to the network

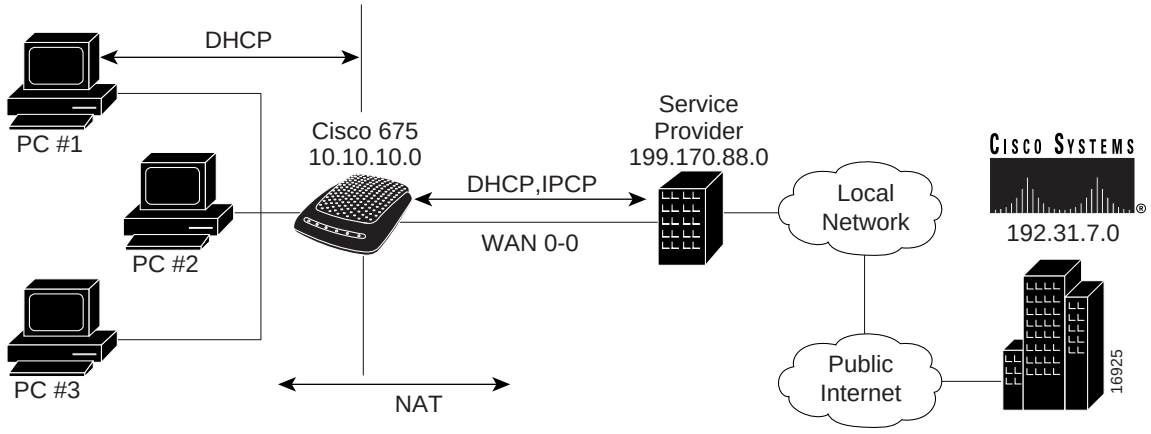
1.1 CBOS Features

This section describes the CBOS-supported features that are common to the Cisco Customer Premise Equipment (CPE) product line.

- Reduces or eliminates the need for you to manually configure CPE devices
- Minimizes the need for configuration of the PCs in a Small Office/Home Office (SOHO) network
- Incorporates the DHCP server and NAT functionality.

  DHCP automatically configures the IP addresses of both the Cisco CPE 67x series products and PC clients within the SOHO network. NAT uses one or more public IP address to translate the SOHO network's private IP address space into real, Internet-valid network IP addresses (Figure 1-1).

Figure 1-1 Configurationless Provisioning with DHCP and NAT



Benefits of Configurationless Provisioning

Configurationless provisioning provides:

- Reduced Internet access costs through the use of dynamically allocated IP addresses
- Simplified router configuration and IP address management
- Conserved registered IP addresses
- Dynamic IP address allocation for remote workstations
- Remote LAN IP address privacy

Note The Cisco 67x CPE products and the CBOS are Y2K compliant.

1.1.1 Configurationless Provisioning Process

The combination of DHCP and NAT in the Cisco PPP/ATM environment supports a configurationless CPE provisioning by automatically configuring both the Cisco 67x and the associated SOHO network at power-on. A minimal configuration is required in the user PC (typically a single check-box to enable DHCP operation) but all PCs within the network have identical settings which simplifies initial provisioning and network support.

Understanding the DHCP Server and DHCP Client

Two components make up the dynamic host configuration protocol on the Cisco 67x:

- DHCP server
- DHCP client

Using the Cisco 67x as a DHCP Server

When the Cisco 67x DHCP server operates in:

- Stand-alone mode—It fully configures the SOHO network with IP addresses, default gateways, and Domain Name Servers (DNSs).
  - The Cisco 67x DHCP then configures the Cisco 67x and provides sufficient information to allow the Cisco 67x-based DHCP server to configure the SOHO network as well.
- Stand-alone server mode—A system administrator manually provisions the Cisco 67x with the appropriate configuration for the clients within the SOHO network.

The configuration information that the Cisco 67x DHCP server is able to assign to SOHO clients includes, but is not limited to, the following:

Note The Cisco 67x does not automatically resolve DNS addresses. Therefore, you must enter the following configuration parameters as IP addresses.

- Gateway
- Primary Domain Name Server
- Netmask
- Internet Address
- SMTP Server
- POP3 Server
- NNTP Server
- WEB Server
- IRC Server

Note Not all DHCP clients accept or understand every configuration parameter option passed to them.

Using the Cisco 67x as a DHCP Client

The Cisco 67x operates as a DHCP client as follows:

1. A PPP session is established over wan0-0.
2. The Cisco 67x (see Figure 1-1) sends a DHCP client request to the service provider's network.
3. The Cisco 67x obtains configuration information from the service provider's DHCP server.
4. The Cisco 67x turns into a DHCP server and can configure SOHO clients (PC#1, PC#2, and PC#3).

Note If you use the DHCP client mode, you must also use the DHCP server mode.

---

5. When the DHCP server is enabled, the Cisco 67x must contain a valid DHCP configuration, which has been either manually provisioned or obtained during a previous client transaction.

   If this is the first time the Cisco 67x has performed a client request, it ignores all network traffic until the Cisco 67x client transaction has completed.

6. The Cisco 67x saves the client configuration information obtained during the client transaction to NVRAM for subsequent use.

   If a client transaction results in configuration information that differs from that which is stored in NVRAM, the Cisco 67x saves the new configuration to NVRAM and uses the new information on the subsequent power-cycle.

Understanding NAT

NAT in the Cisco 67x translates private (or Internet-invalid) IP addresses to public (Internet-valid) IP addresses. By dynamically creating a table of translation information each time data is exchanged with any network outside of the SOHO network, the CPE device allows multiple PCs to oversubscribe a single, public IP address. This powerful feature both conserves IP addresses and minimizes customer reconfiguration of a local SOHO network.

Use NAT if you cannot use a network's internal private addresses outside either for security reasons or because the addresses are invalid outside the network.

- Basic NAT allows a one-to-one mapping between one private address and one public address.
- NAT with Port Address Translation (PAT or NAPT) is an extension to NAT in that PAT uses TCP/UDP ports in addition to network addresses (IP addresses) to map many private network addresses to a single outside address. Cisco CPE products support both NAT and PAT.

Note Cisco CPE products do not support basic NAT for the 2.1.0 Release.

When NAT is enabled, the Cisco 67x obtains a public IP address from the upstream router (in most cases a Cisco 7200) using either PPP's IPCP protocol or a DHCP client transaction. The upstream router, in turn, may obtain the IP addresses from a locally provisioned pool, either a DHCP server or a RADIUS server. This allows the service provider to easily configure the customer premise network and router.

Network Address Translation is predominantly application-independent, with the exception of FTP. However, the Cisco implementation of NAT fully supports full-rate FTP. Applications that include IP addresses within the packet payload will fail without special NAT-wise consideration.

Other benefits of the Cisco implementation of NAT on CPE products include:

- Abstracts the customer premise network from any changes in the service provider network (including changing service providers).
- Enables access (from the public Internet) to a specific private SOHO host by statically mapping a real IP address to a private host's IP address. This static mapping would facilitate the operation of a Web server, for example, within a network served by Cisco CPE products.
- Preserves all of the Cisco 67x's layer three management features. TFTP (for firmware updates), TELNET (for general management), ping, and traceroute all operate in the same manner as when NAT is disabled, provided there is no static mapping from the outside address to an inside address.

- Supports transparent use of the Domain Name Server (DNS) mechanism for outside hosts requests. This means that NAT does not interfere with host name look-ups such as CISCO.COM. However, for hosts inside the SOHO network's private address space, a DNS server (or LMHOSTS file) is required in the SOHO network to resolve host names automatically.
- Does not impose any requirements on service provider configurations. Service providers provide their own NAT IP address (that is, registered to the service provider) for translation of 67xs outside network address.

DHCP and NAT Together

When both NAT and DHCP are enabled, the Cisco 67x becomes virtually configurationless. NAT obtains the public address used for translation in the same manner as described above. However, DHCP does not require any additional provisioning since NAT translates all address information to the outside, public address. You can use a DHCP client transaction to obtain DNS, WINS, and other information for subsequent SOHO DHCP server operation, but this is not required.

When a DHCP client transaction is in progress, the Cisco 67x delays NAT implementation until the client transaction completes. This ensures that the most current information is used for server operation.

The end result for the SOHO users (PC#1, PC#2, and PC#3) (see Figure 1-1) is as follows:

1. SOHO users turn on their un-configured machines with DHCP enabled. Within seconds, they are surfing the Internet using a configuration totally and transparently supplied by their service provider.
2. Clients are not affected by changes at the service provider.

Note When you do not use Network Address Translation, you must maintain a consistent relationship between the information you obtain during the client phase and the configurations passed to the clients on the SOHO network. This occurs because clients retain their DHCP configuration for the configurable lease time.

After a SOHO host's lease time expires, it must request an IP address from the DHCP server. If a Cisco 67x obtains different configuration information during the client phase, the SOHO clients must obtain new address leases. And further, because their default gateway system (the Cisco 67x) has changed addresses, they can no longer access the outside network.

1.1.2 Supported Applications

In addition to DHCP and NAT, CBOS also supports the applications, listed below, for management and control of the system:

- Ping (packet Internet groper)

  Cisco CPE products support the standard version of ping (packet Internet groper), which tests whether a particular network destination is online by sending an Internet control message protocol (ICMP) echo request and waiting for a response.

- RADIUS

  Remote Authentication Dial-In User Service (RADIUS) authenticates users for access to a network. The RADIUS server uses an authentication scheme, such as PAP, to authenticate incoming messages from RADIUS clients. When a password is present, it is hidden using a method based on the RSA Message Digest Algorithm MD5.

  The Cisco 67x has been successfully tested for compatibility with the following RADIUS server providers:

  — Livingston Enterprises RADIUS Version 2.01

  — Sun Solaris Version 2.5

  — Merit RADIUS (Sun binary)

  — RADIUS NT (Microsoft)

Cisco 67x Implementation of the RADIUS Client:

The Cisco 67x supports a RADIUS client. However, for most environments, the RADIUS client is not used. The RADIUS client exists on the service provider's remote access server. The Cisco 67x communicates with the RADIUS client through PAP packets.

- RIP (Routing Information Protocol)

  The CBOS supports the Routing Information Protocol (RIP) and RIP2. RIP is an interior gateway protocol used with TCP/IP to automatically add IP routes to the routing table. It provides routing information such as what networks are accessible and the number of hops required to reach each one. RIP2 includes a larger command set to expand RIP functionality.

- SYSLOG client

  SYSLOG logs significant system information to a remote SYSLOG server for processing without requiring large amounts of local storage or local processing.

  Implementing SYSLOG:

  Using the CBOS, the Cisco 67x allows you to specify a remote server for logging system messages. Cisco supports the following levels of severity:

  — Debug

  — Info

  — Warning

  — Alarm

  — Critical

  — Crash

  These are similar to the standard BSD style severity levels for SYSLOG; however, they do not include None and Mark.

  To configure your **syslog** daemon to receive Cisco SYSLOG messages, modify the `/etc/syslog.conf` configuration file (remember to use tabs, not spaces). Several systems, such as Linux and FreeBSD, have SYSLOG set up properly by default.

- Telnet server

  Use Telnet as a command line interface and as a means of providing remote login connections between machines on several networks, including the Internet.

- TFTP server

  Use the Trivial File Transfer Protocol (TFTP) to transfer files to and from a Cisco 67x using a TFTP client. Cisco 67x runs a TFTP daemon, which allows users from remote machines who have TFTP client software to remotely transfer files to and from the Cisco 67x. The TFTP client can be enabled and disabled from the CBOS or the Web Management Interface.

  For security reasons, Cisco recommends that you disable the TFTP application, except when uploading or downloading a file. Typically, use TFTP to transfer new software from Cisco to your Cisco 67x, where the file name equals `nsrouter.c67x.<version #>ima.hr`. You can also use TFTP to archive an image of your CBOS configuration file. This configuration file can be named anything you wish as long as you can view and edit the file with a standard text editor. Use the `.cfg` extension to make the configuration file easy to locate and to assure that it can be viewed and edited by a standard text editor. Archive an image of your configuration file before making changes to it so you can easily recover the old file if necessary. When uploading a configuration file to the 67x, you must name the configuration file `nscfg.cfg` before uploading.

- Traceroute

  Use traceroute to determine if there is a connection between two systems and to view the intermediate routers between the two systems.

- Web access

  Use the Cisco CPE product's web interface for configuring and changing system settings.

Note These applications are only accessible when the Cisco 67x is in routing mode except for TFTP, ping, and Telnet in managed bridging mode.

1.2 Using CBOS User Interfaces

The CBOS includes two interfaces you can use to configure and operate the Cisco 67x:

- Command Line Interface—This interface is designed for experienced personnel to use in their day-to-day tasks for operating banks of Cisco 67xs. Access this interface using either a Telnet or a terminal emulation program.
- Web Browser Interface—This interface is designed for individuals who prefer a graphical user interface (GUI) program or who are familiar with Web-based navigational principles.

1.3 Using the CBOS Help System

From the CBOS prompt, use the help command to display the online help system for a specified command. Refer to Chapter 2, "Using the Command Line Interface," for more information on the help command. To access the Help Facility, enter the following command from the command line:

help [*command-name*]

or

? [*command-name*]

For example, to display information about the **show version** command, enter:

```
help show version
```

or

```
? show version
```

CHAPTER 2

Using the Command Line Interface

2.1 Commonly Used Commands

This section documents the Cisco Broadband Operating System (CBOS) commands and command arguments that manage the Cisco 67x. CBOS runs in two modes: **exec** and **enable**. The table below lists the commands for each mode.

Table 2-1 Cisco Broadband Operating System Commands

Exec Mode	Enable Mode
help/?	help/?
ping	quit/exit
quit/exit	ping
reboot	reboot
show	set
traceroute	show
enable	traceroute
stats	write
	exec
	stats

2.1.1 help

To get help information on a particular command.

help command-name

You can also do:

? command-name

Syntax Description

command-name Specifies the command.

Command Modes

Exec and Enable

Examples

```
help stats
```

or

```
? stats
```

2.1.2 ping

To send one or more echo ICMP (Internet Control Message Protocol) request message(s) to another host for a reply.

ping *ip-address* [**-t** | **-n** *number*] [**-w** *seconds*] [**-i**]

Syntax Description

ip-address	Specifies the destination IP address to be pinged.
-t	Specifies to ping host IP continuously until the user interrupts. On a PC, press the Enter key to stop the **ping** command.
-n *number*	Specifies the number of pings to send to host.
-w *number*	Specifies the amount of time (in seconds) to wait for response.
-i *number*	Specifies the Time to Live.

Command Modes

Exec and Enable

Example

The following example pings IP address 208.203.234.26 three times.

```
ping 208.203.234.26 -n 3
```

The following example pings IP address 208.203.234.26 indefinitely allowing for a 3 second wait response until the command string times itself out.

```
ping 208.203.234.26 -t -w 3
```

2.1.3 quit/exit

To quit or exit CBOS.

quit | exit

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec and Enable

Example

The following examples quit CBOS.

```
quit
exit
```

2.1.4 reboot

To reboot CBOS.

reboot

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec and Enable

Example

The following example reboots CBOS.

```
reboot
```

2.1.5 set bridging

To enable and disable bridging options.

set bridging {enabled | disabled | users *interface number-of-users* **| rfc1483 | management | ppp}**

Syntax Description

enabled	Enables bridging.
disabled	Disables bridging .
users *interface number-of-users*	Specifies the maximum number of users for a specific port. The port is defined by the variable *interface*. The number of users is defined by the variable *number-of-users*.
rfc1483	Specifies the protocol to be used for bridging is for RFC1483 MAC.
management	Specifies that bridging is for the management VC.
ppp	Specifies that bridging is in PPP-BCP mode.

Command Mode

Enable

Usage Guidelines

The rules that govern the **set bridging** command are:

- Bridging and routing do not operate simultaneously.
- The commands **enabled** and **disabled** are required commands for RFC, management and PPP only.
- The commands listed below do not work in non-managed bridge mode.
  - **ping**
  - **route** (and setting static routes)
  - **rip** related commands (**set** and **show**)
  - **filter** related commands (**set** and **show**)
  - **traceroute** command
  - **Telnet** server
  - **TFTP** server
  - **Web** interface

Note You must reboot to enable bridging options.

Examples

The following examples contain a sequence of commands for setting up bridging.

```
set bridging rfc1483 enabled
set bridging ppp enabled
```

2.1.6 set broadcast forwarding

To set forwarding of broadcast packets.

set broadcast forwarding {**enabled** | **disabled**}

Syntax Description

enabled	Activates broadcast packet forwarding.
disabled	Deactivates broadcast packet forwarding.

Command Mode

Enable

Example

The following example enables broadcast packet forwarding:

```
set broadcast forwarding enabled
```

2.1.7 set dhcp

To activate, deactivate, or configure Dynamic Host Configuration Protocol (DHCP) functionality.

set dhcp

{client {enabled | disabled | interface *interface-name***} |**

{server {enabled | disabled | pool *pool-number* **{dns | sdns | gateway | ip | irc | nntp | pop3 | smtp | web | wins | swims}** *ip-address***}} | {lease** *seconds* **| netmask** *mask* **| size** *pool-size* **| enabled | disabled} |**

{relay {enabled | disabled}}

Syntax Description

enabled	Activates a specific DHCP functionality, either client, server, or relay.
disabled	Deactivates a specifies DHCP functionality, either client, server, or relay.
client	Specifies to configure client settings.
interface *interface-name*	Specifies to configure physical and logical interface settings.
server	Specifies to configure server settings.
pool *pool-number*	Manually modifies a DHCP server pool entry and specifies the number of the pool to modify. *Pool-number* is a number between 0 and 19.
dns *ip-address*	Sets the DNS address for all requests sent out of this pool. If *ip-address* is set to 0.0.0.0, no DNS information is sent out. If you add a pool after setting DNS, you must reset DNS for the new pool.

sdns *ip-address*	Sets the secondary DNS address. If *ip-address* is set to 0.0.0.0, no SDNS information is sent out. If you add a pool after setting SDNS, you must reset SDNS for the new pool.
gateway	Sets the gateway address for all requests sent out of this pool. If *gw-address* is set to 0.0.0.0, no gateway information is sent out. If you add a pool after setting the gateway, you must reset the gateway for the new pool.
ip *ip-address*	Sets the initial IP address for the pool specified.
irc *ip-address*	Sets the IP address of the IRC Server.
nntp *ip-address*	Sets the IP address of the News Server.
pop3 *ip-address*	Sets the IP address of the POP Mail Server.
smtp *ip-address*	Sets the IP address of the Mail Server.
web *ip-address*	Sets the IP address of the Web Server.
wins *ip-address*	Sets the primary wins server address.
swims *ip-address*	Sets the secondary wins server address.
lease *seconds*	Sets the lease time of clients in seconds.
netmask *ip-address*	Sets the subnet mask for all requests sent out of this pool.
size *pool-size*	Sets the size of the allocation pool. Note: Your pool size can never be set to higher then your local subnet mask that you are handing out for the pool.
relay	Sets the DHCP host server up as a relay agent to pass DHCP IP address assignments to the client system.

Command Mode

Enable

Example

The following example enables the DHCP client:

```
set dhcp client enabled
```

The following example sends all DHCP client requests out through the logical wan0-1 port.

```
set dhcp client interface wan0-1
```

You must do the following before you can use a logical wan port:

```
set interface wan0-0 close
set interface maxvcs 4
write
```

Reboot your system after you enter the commands shown above.

The following example enables the DHCP server functionality:

```
set dhcp server enabled
```

The following command adds pool 0 with a specific IP address.

```
set dhcp server pool 0 ip 192.168.0.100 enabled
```

The following example enables the DHCP relay agent:

```
set dhcp relay enabled
```

2.1.8 set download

To download a new router image or new router configuration image.

set download {**code** | **data**}

Syntax Description

code	Begins an XMODEM download of a new router image file.
data	Begins an XMODEM download of a new router configuration image file.

Command Mode

Enable

Example

The following example begins an XMODEM download of a new router configuration image file.

```
set download data
```

2.1.9 set errors

To enable IP packet dumping.

set errors [**client** {**enabled** | **disabled**} | **combo** {**enabled** | **disabled**} | **module** {**rfc1483** | **none**} | **debug** {**enabled** | **disabled**}] | **clear**

Syntax Description

client {enabled | disabled}	Enables IP packet dumping for the client from which the command was invoked. enabled - Enables packet dumping. disabled - Disables packet dumping.
combo {enabled | disabled}	Enables both the **debug** and the **client** modes simultaneously. enabled - Enables packet dumping. disabled - Disables packet dumping.
module {rfc1483 | none}	Enables IP packet dumping only for the RFC1483 module. rfc1483 - Defines the RFC1483 module. none - Disables packet dumping for the RFC1483 module
debug {enabled | disabled}	Sets IP packet dumping utility to display errors to the system display. enabled - Enables debug error display. disabled -Disables debug error display.
clear	Clears any errors from NVRAM.

Command Mode

Enable

Example

The following example enables IP packet dumping for the RFC1483 module.

```
set error module rfc1483
```

The following example clears errors.

```
set errors clear
```

2.1.10 set filter

To specify and modify IP filtering conventions for the Cisco 67x.

set filter {*code* **on | off**} [**deny | allow** {*interface* | **all** *src-ip src-mask dest-ip dest-mask*} **port** *number*]

Syntax Description

code	Enter the numbered filter number to be modified. Valid filter code values are 0 through 9.
**on	off**	Enables or disables the filter.
**deny	allow**	Specifies whether the filter is to allow or deny packets that match the filter's address and mask.
interface	**all**	Displays the Interface on which to apply the filter. This can be a particular interface such as eth0 or wan0-x or all interfaces.
src-ip	Enter the source IP address for packets.
src-mask	Enter the mask to be applied to source IP address. This allows the filter to match a group of incoming IP addresses.
dest-ip	Enter the destination IP address of outgoing packets.
dest-mask	Enter the mask to be applied to destination IP address. This allows the filter to match a group of outgoing IP addresses.

port *number*	Displays the TCP/UDP port number to block.

Command Mode

Enable

Usage Guidelines

The **set filter** command is used to specify IP filtering conventions. The Cisco 67x has 10 filters that can be applied to TCP and UDP packets passing through the router's interfaces. Enabled filters are applied to packets in sequential order according to filter number.

The rules that govern the **filter** command are:

- The minimum parameters required for the **set filter** command are the filter code and the enabled/disable flag.
- Source and destination IP address and masks must both be present on the command line when the **deny | allow** flag is present.
- A *source-address* and *source-mask* of 0.0.0.0 and 0.0.0.0 are used to always match a packet for the filter. Likewise, an address/mask of 255.255.255.255/255.255.255.255 is used to never match a packet.
- Filters are applied to the Ethernet interface (eth0) by default. Include the *interface* variable on the command line to specify another interface, or **all** to specify all interfaces in the router.
- Changes made to the filters will become effective immediately. Packet filtering can be globally suspended and resumed with the **set filter** command.
- All filter related commands (**set** and **show**) are disabled when in bridge mode.

Examples

The following example blocks all web access.

```
set filter 0 on deny all 0.0.0.0. 0.0.0.0  0.0.0.0. port 80
```

The following example blocks all telnet access from the 192.168.0.25 network.

```
set filter 1 on deny all 192.168.0.0 255.255.255.0 0.0.0.0. 0.0.0.0 port 23
```

The following example accepts telnet access from the host 192.168.0.25.

```
set filter 2 on allow all 192.168.0.25 255.255.255.255 0.0.0.0. 0.0.0.0
port 23
```

The following example blocks all FTP access on a wan port.

```
set filter 3 on deny wan0-1 0.0.0.0. 0.0.0.0 0.0.0.0. 0.0.0.0 port 21
```

The following example turns off the first filter.

```
set filter 0 off
```

The following example activates all enabled filters.

```
set filter on
```

Note Press enter only after entering all command parameters. A command may appear on two lines here for readability.

2.1.11 set interface

To configure settings for physical and virtual interfaces.

set interface

{eth0 {address *ip-address* **| mask** *netmask* **| down | up | speed {10 | 100} |**

vip {1 | 2 | 3 | 4} {ip *ip-address* **| mask** *netmask***} |**

wan0 {baud *rate* **| count {1 | 2 | 4 | 8 |} | doh {enabled | disabled} | maxvcs {1 | 2 | 3 | 4} | rate {up | down | down:baud}** *rate-number* **| auto} | [remote] | retrain | scramble {enabled | disabled} | stay} |**

wan0-*x* **{close | destination** *ip-address* **| disabled | enabled | mask** *netmask* **| open | rate** *rate-value* **| VCI** *vci-number* **| VPI** *vpi-number***}**

Syntax Description

enabled	Enables a command or functionality.
disabled	Disables a command or functionality.
eth0	Specifies to set or check values for the Ethernet interface.
address *ip-address*	Specifies the destination IP address for the Ethernet interface.
mask *netmask*	Specifies the netmask address for the Ethernet interface.
down	Disables the interface.
up	Enables the interface.
speed	Specifies the link speed given as [**10	100	auto**].
vip*x*	Specifies to set or check values for a virtual Ethernet interface.
ip *ip address*	Specifies the destination IP address for the virtual interface.

mask *netmask*	Specifies the netmask address for the virtual interface.
wan0	Specifies to set or check values for the wan0 interface.
baud *rate*	Sets the ADSL baud rate.
count	Sets the VPI count.
doh	Specifies to turn the Digital Off-Hook functionality off or on.
maxvcs	Sets the maximum number of virtual connections (VCs).
rate	Sets line rates.
up *rate-number*	Sets upstream ADSL line rate.
down *rate-number*	Sets downstream ADSL line rate.
down:baud *rate-number*	Sets downstream line rate and baud rate.
auto	Sets auto-negotiation mode for this device.
retrain	Retrains the ADSL line.
scramble	Enables or disables ATM cell scrambling.
stay	Sets stay-trained mode; ADSL line will not retrain.
wan0-*x*	Specifies to set or check values for the wan0-*x* interface.
close	Closes the virtual connection.
destination *ip-address*	Sets the IP address.
mask *netmask*	Sets the netmask.
open	Opens the virtual connection.

rate *rate-value*	Sets the scalarate - the transmitted data rate in 64Kbps increments up to a maximum of the current line rate.
VCI *vci-number*	Sets the number of the virtual channel identifier.
VPI *vpi-number*	Sets the number of the virtual path identifier.

Command Mode

Enable

Usage Guidelines

Since the Cisco 67x only has one physical port for the Ethernet port, the default value is always 0 as in *eth0.*

Use this command only when you have a serial connection with Cisco 67x. If you use this command when you are communicating over an Ethernet LAN, you will lose the connection to Cisco 67x. If you forget and issue this command over the LAN, you can reset Cisco 67x by switching the Cisco 67x OFF and then turning the power back ON.

Example

The following example assigns the Ethernet interface an IP address.

```
set interface eth0 address 198.162.55.5
```

The following example sets the maximum number of VCs to two.

```
set interface wan0 maxvcs 2
```

The following examples open or close the wan0-0 port.

```
set interface wan0-0 open
set interface wan0-0 close
```

The following example sets the ScalaRate of the wan0-0 port.

```
set interface wan0-0 rate 1088
```

The following example sets a VPI address for the wan0-0 port to equal 1, which is in the valid range for VPI addresses.

```
set interface wan0-0 vpi 1
```

The following example sets the VCI address for the wan0-0 port to equal 1, which is in the valid range for VCI addresses.

```
set interface wan0-0 vci 1
```

Note The ScalaRate only affects the transmitted data rate. On the Cisco 67x only the upstream rate is affected.

Usage Guidelines

The Cisco 67x has a total number of four VCs (wan0-1 through wan 0-3). Configure only the total number of actual VCs terminated to optimize the performance of the Cisco 67x. Close the wan*x-x* port before making any changes to the port.

The Cisco 67x supports user configuration of VPI/VCI address mapping. The Cisco 67x ships with one VC enabled. Its VPI/VCI address is 1/1. When changing the VPI/VCI address space mapping, it is important to understand that adding VPI space decreases VCI space. For example, if the VPI count is one, 255 possible VCI values are available for the single VPI. If the VPI count is eight, the number of possible VCI values is reduced to 31 VCIs for each of the eight VPIs.

When changing the VPI count values, you must ensure that VPI and VCI port assignments are consistent with the VPI count mode selected. For instance, when changing the VPI count from four to one, you must change the VPI port assignment to zero (0) on all wan0-*x* ports previously assigned to values other than 0, since 0 is the only valid VPI when the VPI count is 1.

The valid ranges for VPI and VCI addresses are shown in the following table:

Table 2-2 Valid VPI and VCI Address Ranges

VPI <*count*>	**VPI Range**	**VCI Range**
1	0	0..255
2	0..1	0..127
4	0..3	0..63
8	0..7	0..31

2.1.12 set multicast

To enable multicast proxy support.

set multicast {**forwarding enabled** | **disabled**}

Syntax Description

enabled	Enables multicast proxy support.
disabled	Disables multicast proxy support.

Command Mode

Enable

Example

The following example enables multicast proxy support.

```
set multicast forwarding enabled
```

2.1.13 set nat

To enable or disable Network Address Translation (NAT) functionality.

set nat {enabled | disabled | timeout {icmp | upd | tcp idle | tcp negotiation | other} *value* **| outside ip** *ip-address* **|**

entry add {*inside-ip inside-port outside-ip outside-port protocol***} |**

entry delete { all | [*inside-ip***] [***outside-ip***] [***protocol***]}}**

Syntax Description

enabled	Activates NAT functionality.
disabled	Deactivates NAT functionality. The default setting for this command is **disabled**.
timeout	Sets the timeout value for the protocols listed below.
icmp	Specifies the ICMP protocol. Default = 60 seconds
udp	Specifies the UDP protocol. Default = 120 seconds
tcp	Specifies the TCP protocol.
idle	Specifies the timeout value to set for the data transfer portion after connection setup. Used for the TCP protocol only. Default = 24 hours
negotiation	Specifies the timeout value to set during TCP setup and tear down. Used for the TCP protocol only. Default = 60 seconds
fragmentation	Specifies how long to maintain ‘out-of-order’ fragments before the **set nat timeout** command terminates. Default = 60 seconds
value	Specifies the timeout value. Expressed in seconds less than or equal to 65000.

outside ip *ip-address*	To set the global outside network address to be used for translation.
entry add	To add a static entry to a NAT table. • Follow the sequence exactly as shown in the example below when entering your command string.
inside *inside-ip*	Specifies the IP address of the inside, private or SOHO network.
inside *inside-port*	Specifies the port number of the inside network port.
outside *outside-ip*	Specifies the IP address of the outside, public or Service Provider's network.
outside *outside-port*	Specifies the port number of the inside network port.
protocol	Specifies the protocols to use. Select between: **udp**, **tcp**, **icmp**.
entry delete	To delete NAT table entries.
all	Deletes all entries from the NAT table.
inside *ip-inside*	Deletes all matching entries with the specified inside IP address (shown as *ip*) from the NAT table.
outside *outside-ip*	Deletes all matching entries with the specified outside IP address (shown as *ip*) from the NAT table.
port	Defines the port associated with the IP address to delete from NAT.
protocol	Specifies the protocols to use. Select between: **udp**, **tcp**, **icmp**.

Command Mode

Enable

Usage Guidelines

To ensure that **PPP** assigns an address for translation, you must issue the following commands:

```
set ppp wan0-0 ipcp 0.0.0.0
write NVRAM
```

Examples

The following example disables NAT.

```
set nat disabled
```

The following examples show various timeout values that you can set:

```
set nat timeout icmp 60
set nat timeout tcp idle 84
set nat timeout tcp negotiation 60
set nat timeout udp 60
set nat timeout fragmentation 60
```

The following example adds an entry to the NAT table that routes external requests destined for IP address 192.168.0.100 on port 322 to the internal station at IP address 10.10.10.100 on port 211.

```
set nat entry add 10.10.10.100 211 192.168.0.100 322 tcp
```

Note You must use the precise sequence, as defined in the Syntax Description listing below, when you enter your command string.

The following command deletes all of the NAT table entries.

```
set nat entry delete all
```

The following command deletes a specific NAT entry. You must enter the port number when deleting a specific NAT entry. Refer to the syntax example at the top of this page.

```
set nat entry delete 10.10.10.100 111 outside 192.168.0.100 10000 udp
```

The following command deletes all entries that match a specific inside address.

```
set nat entry delete inside 1.1.1.1
```

The following command deletes all entries that match a specific outside address.

```
set nat entry delete outside 2.2.2.2
```

Note Do not use the following command for normal setup. In normal setup, either DHCP or IPCP acquires the global outside network address for the 67x.

The following example sets the outside IP address to `192.168.0.100`.

```
set nat outside ip 192.168.0.100
```

2.1.14 set nvram

To configure NVRAM settings.

set nvram {**erase** | **add** *parameter* | **del** *parameter*}

Syntax Description

erase	Erases current configuration.
add *parameter*	Adds parameter manually to NVRAM.
del *parameter*	Removes parameter manually from NVRAM.

Command Mode

Enable

Example

The following example erases NVRAM.

```
set nvram erase
```

2.1.15 set ppp

To configure PPP parameters and statistics.

set ppp {restart {on|enabled|off|disabled}} | wan0-*x* {llc {enabled | disabled} | radius {enabled | disabled} | pap {enabled | disabled} | mru *units* | retry *number* | magicnum *hexnumber* | ipcp {*ip-adr* | clear} | dms *ip-address* | login *pap-login* | password *pap-password* | debug {enabled | disabled | syslog} | subnet *ip-address* | wins *ip-address*}

Syntax Description

restart	Reinitiates the PPP session
**on	enabled**	Allows auto restart of ADSL link after idle
**off	disabled**	Disallows auto restart of ADSL link after idle
wan0-*x*	Specifies the wan0-x port. Wan ports are numbered consecutively 0-3.
pap {**enabled**	**disabled**}	Enables or disables PPP PAP passwords.
llc {**enabled**	**disabled**}	Enables or disables LLC encapsulation.
mru *mru-units*	Enter the Maximum Receive Units.
radius	Sets RADIUS for authentication.
**enabled	disabled**	Enables or disables RADIUS.
retry *retry-number*	Enter a maximum retry count on authentication.
magicnum *hex-magic*	Enter a valid hexadecimal number.
ipcp *ip-address*	Enter the IP address of the destination router.
dns *ip-address*	Enables automatic negotiation of the primary or secondary DNS IP address
login *pap-login*	Enter PAP authentication login name.

password *pap-pass*	Enter PAP authentication password.
debug	Sets PPP trace output debug facility.
on | **off** | **syslog**	Enables or disables the PPP debug facility or enables the **syslog** daemon.

Command Mode

Enable

Examples

The following example sets the Maximum Receive Units.:

```
set ppp wan0-0 mru 10
```

The following example sets the Maximum Retry Counts on PPP authentication.

```
set ppp wan0-0 retry 5
```

The following example sets the PPP Magic Number.

```
set ppp wan0-0 magicnum 16
```

The following example sets the PAP authentication name.

```
set ppp wan0-0 login bjones
```

The following example sets the PAP authentication password.

```
set ppp wan0-0 password 78A55Q
```

2.1.16 set prompt

To set a different prompt for the CBOS command line.

set prompt *new-prompt-name*

Syntax Description

new-prompt-name	Specifies the new name of the CBOS prompt.

Command Mode

Enable

Example

The following example resets the CBOS prompt.

```
set prompt cisco67x
```

2.1.17 set radius

To configure RADIUS security and accounting settings.

set radius {enabled | disabled | remote *ip-address* **| port** *port-number* **| acctport** *udp-port-number* **| secret** *password* **| test [acct]** *login password***}**

Syntax Description

enabled | disabled	Activates or deactivates the application.
remote *ip-address*	Enter IP address for the remote RADIUS server.
port *port-number*	View the Cisco default port setting as defined by the variable *port-number.*
acctport *udp-port-number*	View the Cisco accounting port setting as defined by the variable *udp port number.*
secret *password*	Enter Shared Secret password as defined by the variable *password*.
test	Enables you to send a test the RADIUS serve security and account settings. See **Examples.**
login	Specifies the login name to use when logging into the RADIUS server.
password	Specifies the password to use when logging into the RADIUS server.
acct	Tests RADIUS accounting.

Command Mode

Enable

Examples

The following example enables RADIUS.:

```
set radius enabled
```

The following example sets the IP address of the remote RADIUS server.

```
set radius remote ip-address
```

The following example tests for login user id on the RADIUS server; where `username` is the name of the user who has login permissions and `password` is the user's password to the RADIUS server.

```
set radius test acct username password
```

The following example tests security on the RADIUS server; where `username` is the name of the user who has login permissions and `password` is the user's password to the RADIUS server.

```
set radius test username password
```

2.1.18 set rip

The **set rip** command automatically adds routes to your stream. It can also provide MD5 authentication when the **v2** argument is selected. The **v1** argument provides non-authenticated transmissions.

The usage example below has been separated into three parts for ease of readability. The keywords **eth0** and **wan***x-x* use identical keywords and argument variables.

To configure RIP settings.

set rip {enabled | disabled | aging *aging-value* **| deltimedout {enabled | disabled} | garbage** *garbage-value* **| update** *update-value***} | {eth0 | wanx-x} {announce {default | host | self | static} | delexpired | holdown | splithorizon | poisonreverse | summarize | learn {default | host | sender} {enabled | disabled}} | {authentication {disabled | text | md5} | keyid** *keyid-name* **| receive {disabled | v1compatible | v1 | v2} | rollover** *value* **| send {requests {disabled | v1 | both | v2} | responses {enabled | disabled}}}**

Syntax Description

enabled	Enables the **set rip** command.
disabled	Disables the **set rip** command.
deltimedout *timeout-value*	Delete RIP2 time-outed entries. Expressed in seconds.
enabled	Enables the **deltimedout** keyword.
disabled	Disables the **deltimedout** keyword.
aging	Route aging timeout value (default is 180 seconds).
garbage	Route garbage collection timeout value (default is 120 seconds).
update	Update time interval (default is 30 seconds).

eth0 *ip-address*	Enter IP address for a LAN interface. The address is defined by the variable *eth-address.*
wan*x-x ip-address*	Enter IP address for a WAN interface. The address is defined by the variable *wan-address.*

The Remainder of This List Consists of Keywords and Keyword Arguments in Common to Both eth0 and wan*x-x* Commands

announce	Announces routes.
default {enabled | disabled}	Announces default route.
host {enabled | disabled}	Announces host routes.
self {enabled | disabled}	Announces self as default router.
static {enabled | disabled}	Announces static routes.
authentication	Sets RIP authentication.
disabled | test | md5	**disabled** - Disables the **set rip** command. **text** - Tests the authentication mode. **md5** - Enables encrypted authentication.
delexpired {enabled | disabled}	Auto deletes expired key.
keyid *keyname*	Authentication active key id.
holddown {enabled | disabled}	Sets Route holddown.
splithorizon	Sets split horizon.
{enabled | disabled}	Turns the split horizon mode on or off.
learn	Learns routes.
default {enabled | disabled}	Sets default route.
host {enabled | disabled}	Sets host routes.
password *password*	Sets a plain text password. The maximum number is 16 characters.

poisonreverse	Reverse RIP poison.
enabled | disabled	Turns **poisonreverse** command on or off.
receive	Sets the **receive** command.
disabled | v1compatible | v1 | v2	**disabled** - Disables the **receive** keyword. **v1 compatibl**e - Specifies v1 compatibility (non-authentication mode) with other systems. **v1** - Specifies non-authentication mode. **v2** - Specifies encrypted authentication mode.
rollover *time-period*	Period in advance to start rollover.
send	Sets the **send** command.
requests	Sets RIP requests.
disabled | v1 | both | v2	**disabled** - Disables the **receive** keyword. **v1** - Specifies non-authentication mode. **both** - Specifies both **v1**and **v2** modes. **v2** - Specifies authentication mode.
responses	Sets RIP responses.
enabled | disabled	Turns RIP responses on or off.
summarize	Sets RIP summary.
enabled | disabled	Enables or disables the **summary** keyword.

Command Mode

Enable

Example

The following example disables all requests.

```
set rip eth0 send requests disabled
```

The following example disables all responses from **rip**.

```
set rip eth0 send responses disabled
```

The following examples sets **rip** to receive only V1-compatible messages.

```
set rip eth0 receive v1compatible
```

The following example enables **rip** to learn the default IP address path.

```
set rip eth0 learn default enabled
```

2.1.19 set route

To build a routing table by manually adding or deleting entries in a routing table.

set route {default *target* **| add {ip** *address* **gw** *address* **[mask** *netmask***] [metric** *hops***]} | delete** *address***}**

Syntax Description

default *target*	Sets a default route to an IP address or a WAN interface.
delete *ip-address*	Deletes an existing route.
add	Adds a new route.
ip *address*	Specifies the IP address of the host you are trying to reach. The IP host address is specified by the keyword argument variable, *address.*
gw *address*	Specifies the IP address of an external gateway. Data is sent through the external gateway to the destination address. Therefore, this address must be the address of a gateway physically linked to your network. The gateway address is specified by the keyword argument variable, *address.*
mask *netmask*	Specifies the netmask of the host you are trying to reach.
metric *hops*	Specifies the distance in hops between the destination address and the gateway. The default value is 1.This value is required when you add a route.

Command Mode

Enable

Examples

The following example shows how to add a route without specifying a netmask or metric.

```
set route add ip 192.9.9.1 gateway 192.168.10.250
```

The following example shows how to delete a route.

```
set route delete 192.168.10.1
```

The following example shows how to add a route specifying a netmask and a gateway.

```
set route add ip 192.10.10.0 mask 255.255.255.0
gateway 208.203.245.228
```

The following example shows how to add a default route.

```
set route default 208.203.245.228
```

The following example shows how to add a route add a route specifying a netmask, gateway and a metric.

```
set route add ip 192.10.10.0 mask 255.255.255.0
gateway 208.203.245.228 metric 1
```

Note Press **Enter** only after entering all command parameters. Command examples appear on two lines for readability.

2.1.20 set serial

To configure serial port settings.

set serial timeout {*timeout-value* **more** *lines-number***}**

Syntax Description

timeout *timeout-value*	Sets the value in seconds to disconnect the serial connection. The value must be less than or equal to 65334.
more *lines-number*	Sets the number of lines for the **more** output. Enter a numeric value of '**0**' to disable this command.

Command Mode

Enable

Example

The following example set the timeout value for the serial port.

```
set serial timeout 50000
```

2.1.21 set snmp

To configure SNMP settings.

set snmp enabled | disabled | remote *remote-address* **| traps** *host-address*

Syntax Description

disabled	Disabled SNMP settings
enabled	Enables SNMP settings.
remote *remote-address*	Specifies the IP address for the remote location running SNMP.
traps *host-address*	Sets the IP address of the host on which to trap SNMP messages.

Command Mode

Enable

Example

The following command uses hypothetical IP addresses to demonstrate the use of **set snmp**.

```
set snmp remote 198.162.2.57
set snmp traps 198.162.2.50
```

2.1.22 set syslog

To invoke the Syslog application and its options.

set syslog {disabled | enabled | port *port-number* **| remote** *remote-address* **| test** *test-string***}**

Syntax Description

disabled	Disables the Syslog application.
enabled	Enables the Syslog application.
port *port-number*	Specifies the Syslog port number.
remote *remote-address*	Specifies the remote IP address of the Syslog server.
test *test-string*	Sends a test message to the Syslog server

Syntax Description

This command has no arguments or keywords.

Command Mode

Enable

Example

The following command disables the Syslog application.

```
set syslog disabled
```

The following example sets the IP address for the remote Syslog server.

```
set syslog port 232
```

The following example sets the IP address for the remote Syslog server.

```
set syslog remote 198.162.5.3
```

The following example sends the message “Testing syslog” to the Syslog server.

```
set syslog test Testing syslog
```

2.1.23 set telnet

To configure the **telnet** daemon settings.

set telnet {enabled | disabled | remote *ip-address* **| timeout** *# |* **port** *udp-port-number***}**

Syntax Description

enabled	Enables Telnet functionality.
disabled	Disables Telnet functionality.
remote *ip-address*	Specifies the IP address for the remote location running the Telnet server.
timeout *#*	Specifies the timeout value, in seconds, for a Telnet connection.
port *udp-port-number*	Specifies the Telnet port number.

Command Mode

Enable

Example

The following example sets the remote address for the Telnet application.

```
set telnet remote 1.1.1.1
```

The following example sets the number of seconds for the Telnet connection to timeout.

```
set telnet timeout 300
```

2.1.24 set tftp

To configure the TFTP settings.

set tftp {enabled | disabled | remote *ip-address* **| port** *udp-port-number***}**

Syntax Description

enabled	Enables TFTP functionality
disabled	Disables TFTP functionality.
remote *ip-address*	Specifies the IP address for the remote location running the TFTP server.
port *udp-port-number*	Specifies the TFTP port number.

Command Mode

Enable

Example

The following example sets the remote address for the TFTP application.

```
set tftp remote 198.162.58.23
```

2.1.25 set timeout

To configure timeout settings.

set timeout {idle *seconds* **| session** *seconds* **| reset** *seconds***}**

Syntax Description

idle *seconds*	Enter number of seconds to disconnect after idle.
session *seconds*	Enter number of seconds to disconnect after session uptime.
reset *seconds*	Enter number of seconds to wait to reopen connection.

Command Mode

Enable

Example

The following example sets the timeout values for the idle timeout.

```
set timeout idle 60
```

2.1.26 set web

To configure web server settings.

set web remote *ip-address* **port** *tcp-port-number* **enabled | disabled**

Syntax Description

remote *ip-address*	Specifies the IP address of the web server.
port *tcp-port-number*	Specifies the web server port number.
enabled	Turns on the web server.
disabled	Turns off the web server.

Command Mode

Enable

Example

The following example sets the web server IP address to 192.168.0.100.

```
set web 192.168.0.100
```

2.1.27 show

To display statistics on a particular application or interface.

show {arp | broadcast | dhcp {client | relay | server {pool {*number* | **all}** | **leased}** | **errors** | **filter** | **interface [***interface-name***]** | **multicast** | **nat [timeout [all** | **icmp** | **ipd** | **tcp** | **fragmentation]]** | **nvram** | **nvram#** | **ppp** | **radius** | **rarp** | **rates** | **rfc1483** | **rip {status** | **eth0** | **wan0-***x***}** | **rout** | **running** | **running#** | **serial** | **snmp** | **syslog** | **telnet** | **tftp** | **timeout** | **uptime** | **version** | **web}**

Syntax Description

arp	Displays ARP Table.
dhcp {**client** | **server** [**pool 0** | **allocated**] }	Displays whether the dhcp client, server, or server pool 0 is enabled. The **allocated** argument shows which addresses are currently leased.
errors	Displays list of errors that have occurred.
filter	Displays IP Filters.
interface **wan0**	Displays transmit power and remote transmit power statistics.
nat	Displays whether NAT is enabled and NAT entries (if any).
nat timeout {**all** | **icmp** | **udp** | **tcp** | **fragmentation**}	Displays timeout values for specified protocols or all protocols in NAT. The keyword **fragmentation** specifies the duration of time to maintain ‘out-of-order’ fragments.
nvram	Displays the configuration file located in NVRAM.

nvram#	Displays written configuration file in NVRAM without any comments you may have entered in the configuration file.
ppp	Displays PPP Parameters and Statistics.
radius	Displays RADIUS security and accounting settings.
rarp	Displays RARP Table.
rates	Displays list of possible scalar ATM line rate settings.
rfc1483	Displays RFC1483 Bridging Parameters and Statistics.
rip {**status** | **eth0** | **wan0-***x*}	Displays RIP settings and status on specified interfaces.
running	Displays configuration settings that are currently running, but not saved to NVRAM through the **write** command.
running#	Displays configuration settings that are currently running without comments, but not saved to NVRAM through the **write** command.
serial	Displays serial port setting.
snmp	Displays SNMP configuration settings.
syslog	Displays syslog settings.
telnet	Displays telnet daemon settings.
tftp	Displays tftp settings.

timeout	Displays Idle and Session timeout settings.
uptime	Displays uptime.
web	Displays Web Server settings.

Command Mode

Exec and Enable

Examples

The following example displays an application's configuration settings.

```
show tftp
show syslog
show radius
```

The following example displays the status of IP filters.

```
show filter
```

The following example displays web browser status.

```
show web
```

The following example displays possible ATM line rates at prescribed baud rates.

```
show rates
```

The following example displays error reports.

```
show errors
```

2.1.28 stats

To show operating statistics.

stats {bridging {eth0 | wan0-*x*} | dhcp | eth0 | ip {eth0 | general | rip | vip*x* | wan0-*x*} | nat | ppp | radius | serial | snmp | syslog | telnet | tftp | wan0 | wan0-*x* | web}

Syntax Description

ip	Displays IP statistics.
general	Displays general statistics on the WAN interface.
rip	Displays RIP statistics on the WAN interface.
eth0	Displays eth0 statistics on the WAN interface.
wan0-*x*	Displays wan0-x statistics on a VC.
vip *x*	Displays virtual interface statistics.
bridging	Displays statistics on bridging.
eth0	Displays statistics on the Ethernet interface.
wan0	Displays statistics on the Wan interface.
wan0-*x*	Displays statistics on a VC.
telnet	Displays statistics on telnet.
syslog	Displays statistics on syslog.
tftp	Displays statistics on tftp.
web	Displays statistics on web.
ppp	Displays ppp statistics.
serial	Displays statistics on the serial port.
radius	Displays statistics on RADIUS.

snmp	Displays statistics on SNMP.
nat	Displays NAT statistics.
dhcp	Displays DHCP statistics.
wan0	Displays wan0 statistics.
wan0-*x*	Displays wan0-*x* statistics.

Command Mode

Exec and Enable

Example

The following command displays the statistics for the Ethernet interface:

```
stats ip eth0
```

The following command enables MAC address dumping in bridging mode:

```
stats bridging eth0
```

The following command enables MAC address dumping on the wan0-o port:

```
stats bridging wan0-0
```

2.1.29 traceroute

To trace the routes that a data packet takes until it reaches its destination IP address. The **traceroute** command traces routes along the network, listing all hops and gateways, until it reaches the specified IP address.

traceroute *ip-address* [**-m** *number-of-hops*] [**-w** *wait-time* [**-p** *udp-port-number*]

Syntax Description

ip-address	Specifies the final destination IP address.
-m *number-of-hops*	Sets the Max Time to Live by specifying the number of hops to the trace.Most systems use a default of 64 TTL. Please refer to the appropriate system documentation for your system's default.
-w *wait-time*	Specifies the amount of time, in seconds, to wait for response.
-p *udp-port-number*	Specifies the UDP port number on which to use the trace facility.

Command Mode

Exec and Enable

Example

The following command traces the route for IP address 208.192.56.1. The example uses all arguments and assigns a server from which to originate the command string.

```
traceroute 208.192.56.1 -m 64 -w 5 -p 198.162.2.1
```

2.1.30 write

To write configuration changes to NVRAM.

write

Syntax Description

This command has no arguments or keywords.

Command Mode

Enable

Example

The following command writes all configuration changes you make to NVRAM.

```
write
```

CHAPTER 3

Using the Web Interface

3.1 Purpose

The **Web Management Interface** chapter describes how to use your web browser to manage the a Cisco router.

The Web Management Interface is designed for individuals who prefer a GUI program, or who are familiar with web-based navigational principles. The Web Browser Interface enables you to set some configuration parameters in the browser, and to view other settings. The view-only functionalities are marked as “Display Only.”

Internet Explorer 2.0 from Microsoft is incompatible with the Cisco 67x router. You must use Netscape 3.01 or higher or Internet Explorer 3.01 or higher for the Cisco Web Management Interface.

Note The Web Management Interface may not be available for certain Cisco 67x configurations. Contact your service provider if you have questions concerning this feature.

3.2 Before Using the Web Management Interface

You must receive an IP address to access the Cisco 67x web management page and a user password from a support representative before you can use the Web Management Interface. The IP address for the web management home page is the same as the Eth0 IP address assigned by your Service Provider (SP).

The user password comes in two modes: Exec, or read-only, and Enable. You must have Enable privileges to save changes made via the Web interface to NVRAM.

You must click on the Submit Changes button and issue a **write** command (at the command line interface) to apply any changes though the Web Management Interface.

Do the following to write to NVRAM.

Step 1 Close the web interface.

Step 2 Logon to the CBOS using either the serial or Telnet interfaces.

Step 3 Write changes to NVRAM:
```
cbos>write
```

Step 4 Reboot the system.
```
cbos>reboot
```

The system disregards all changes when rebooted if you have not written the changes to NVRAM.

3.3 Activating the Web Management Interface

Do the procedure below to activate the Web Management Interface.

Step 1 Logon to CBOS using either a serial or telnet interface.

Step 2 Enter the user name `exec` or `enable` and press `Enter` to bypass the initial password if you have not yet created a password. If you have already created a password, proceed to Step 6.

Step 3 To set a new password for the exec login, enter:
`cbos>set password exec` *`new-password`*

Set a new password for user logins by substituting `enable` for `exec` in the above example.

Step 4 To save the new password, enter:
`cbos>write`

Step 5 Enable the Web Management Interface
`cbos>set web enabled`

Step 6 Launch your preferred web browser.

Step 7 Enter the IP address for the Cisco 67x Web Management page in the browser locator field. For example, instead of `http//www.cisco.com/` insert the dotted decimal format (`http://10.0.0.1/`) of the Cisco 67x IP address. The following screen appears:

Figure 3-1 Password Verification

Step 8 Enter the user name and the password.

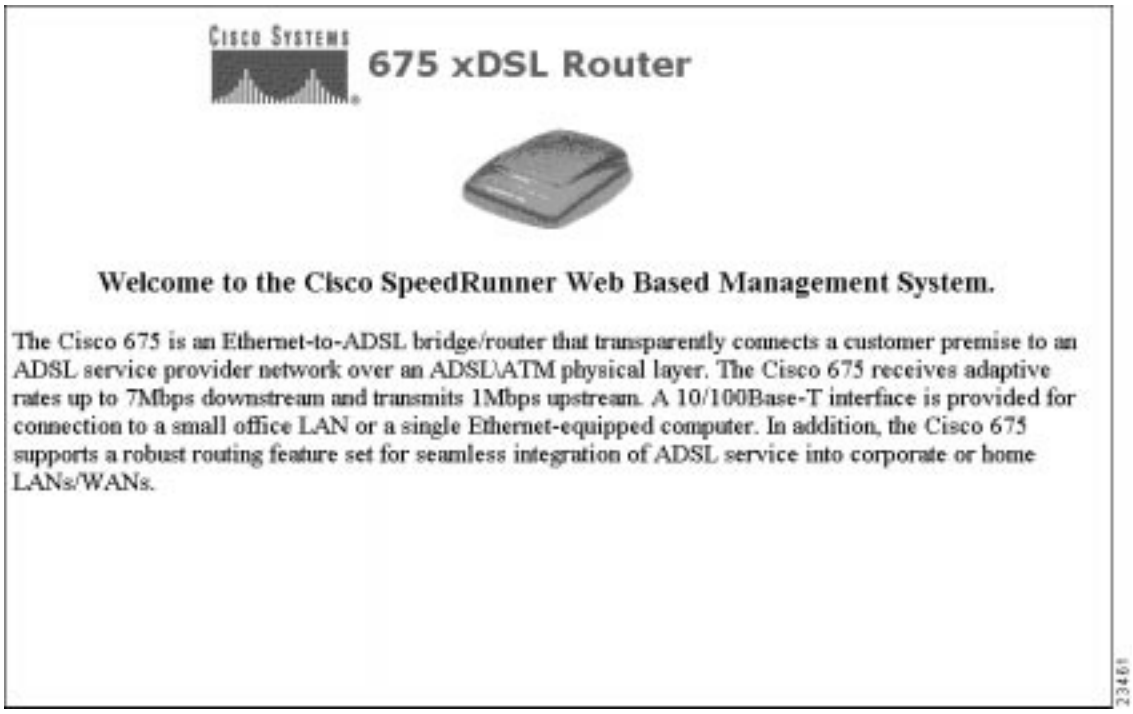
Step 9 Once the Web Management Interface home page appears, you should add a bookmark in your browser for the new Cisco 67x location. Once the bookmark has been added, simply activate the bookmark to access the Web Management Interface. Figure 6-2, on page 6-4 shows the interface home page.

Note If you have a exec-only password, all screens are greyed out so that you cannot make changes.

3.4 Navigating the Web Management Interface

The screen below is the Cisco Web Management Interface home page.

Figure 3-2 Web Management Interface Home Page



3.5 Web Management Pages

The Web Management Interface home page has four buttons that link to other Web pages. To navigate to the various pages, click on the icon or on the appropriate word in the navigation line at the bottom of each page. The purpose of each of the pages is as follows:

- Home Page—Displays the Web Management Interface home page.
- Configure—Displays buttons that correspond to Cisco 67x configuration tasks.
- Statistics—Displays application, port, and error statistics.
- Information—Displays the latest readme file, technical support information, and a feedback form.

3.6 Configure

Click on the **Configure** button and five sub buttons appear.

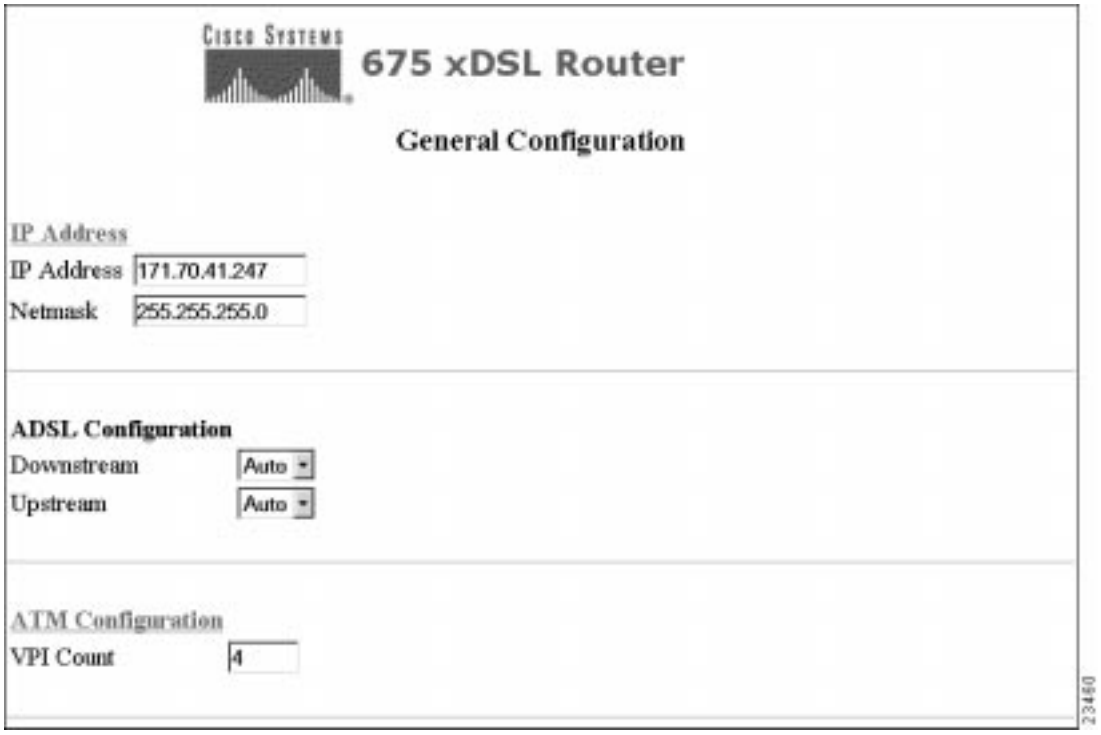
Figure 3-3 Configure Buttons, Statistics Button, and Information Button

The functions for each button are explained below.

3.6.1 General

The **`General`** button allows you to set general configuration parameters, such as the IP address of the Cisco 67x, the ADSL values given to you by your service provider, and the VC base and count metrics. The three sections of the General Configuration screen and instructions on how to use these options are described below.

Figure 3-4 General Configuration Screen



IP Address

This option allows you to set the address and netmask for the Ethernet port of your Cisco equipment.

To use this option:

Step 1 Enter the address and netmask (usually provided by LAN administrator or ISP).

Step 2 To apply these addresses, click on the **Submit Changes** button.

Step 3 To reject these addresses, click on the **Reset Values** button.

Step 4 The new addresses are displayed.

ADSL Configuration

This option allows you to set the up and downstream rates for your ADSL connection.

Note You should not need to change these values. To alter the values, consult your service provider.

ATM Configuration

This option allows you to set up the total number of VPI addresses that you can configure. The VC Base drop down menu allows you to choose a base address, normally one greater than zero. The VC Count drop down menu allows you to specify the number of Virtual Paths to be supported by the Cisco equipment you are using.

To use this option:

Step 1 Select the Base and Count number from their respective drop down menus.

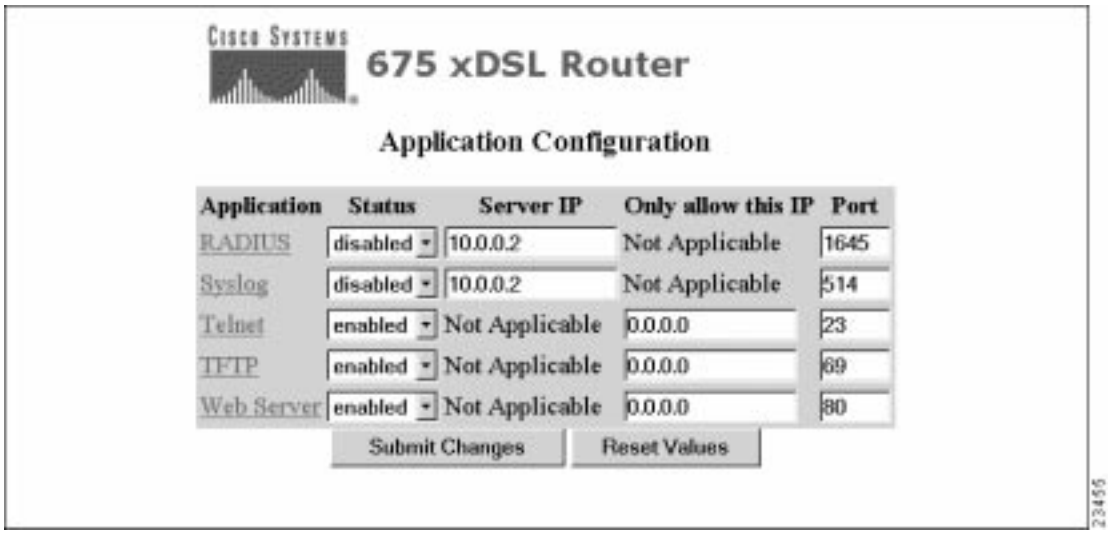
Step 2 To apply these numbers, click on the **Submit Changes** button.

Step 3 To reject these numbers, click on the **Reset Values** button.

3.6.2 Applications

Click on the **Apps** button and the Application Configuration screen appears. The **Apps** button allows you to enable and disable applications associated with the Cisco 67x.

Figure 3-5 Application Configuration Screen



Each of the applications is described in the following sections.

RADIUS

Remote Authentication Dial-In User Service (RADIUS), authenticates users for access to a network. The RADIUS server uses an authentication scheme, such as PAP, to authenticate incoming messages from RADIUS clients. When a password is present, it is hidden using a method based on the RSA Message Digest Algorithm MD5.

Enabling or disabling RADIUS

Select whether you want to enable or disable RADIUS via the first drop down menu.

Step 1 Specify the IP address of the server.

Step 2 Enter a port number.

Step 3 Click on the **Submit Changes** button to apply changes or the **Reset Values** button to discard changes.

Syslog

Syslog logs system information to a specified Syslog server for processing without requiring large amounts of local storage or local processing.

Enabling or disabling Syslog

Step 1 Select whether you want to enable or disable Syslog via the first drop down menu.

Step 2 Specify the IP address of the Syslog server.

Step 3 Enter a port number.

Step 4 Click on the **Submit Changes** button to apply changes or the **Reset Values** button to discard changes.

Telnet

Telnet provides access to the CBOS command line interface via a network.

Enabling or disabling Telnet

Step 1 Select whether you want to enable or disable Telnet via the first drop down menu.

Step 2 Specify the IP address of the machine allowed to use Telnet to connect to the Cisco 67x. To allow any machine to connect, specify 0.0.0.0.

Step 3 Enter a port number.

Step 4 Click on the **Submit Changes** button to apply changes or the **Reset Values** button to discard changes.

TFTP

The Trivial File Transfer Protocol (TFTP) server allows you to transfer a new configuration file or new software to and from Cisco equipment.

Enabling or disabling TFTP

Step 1 Select whether you want to enable or disable TFTP via the first drop down menu.

Step 2 Specify the IP address of the machine allowed to use TFTP to connect to the Cisco 67x. To allow any machine to connect, specify 0.0.0.0.

Step 3 Enter a port number.

Step 4 Click on the **Submit Changes** button to apply changes or the **Reset Values** button to discard changes.

Web Server

The Web Server allows you to use the web interface to access Cisco equipment.

Enabling or disabling the Web Server

Step 1 Select whether you want to enable or disable the web interface via the first drop down menu.

Step 2 Specify the IP address of the machine allowed to use the web interface to connect to the Cisco 67x. To allow any machine to connect, specify 0.0.0.0.

Step 3 Enter a port number.

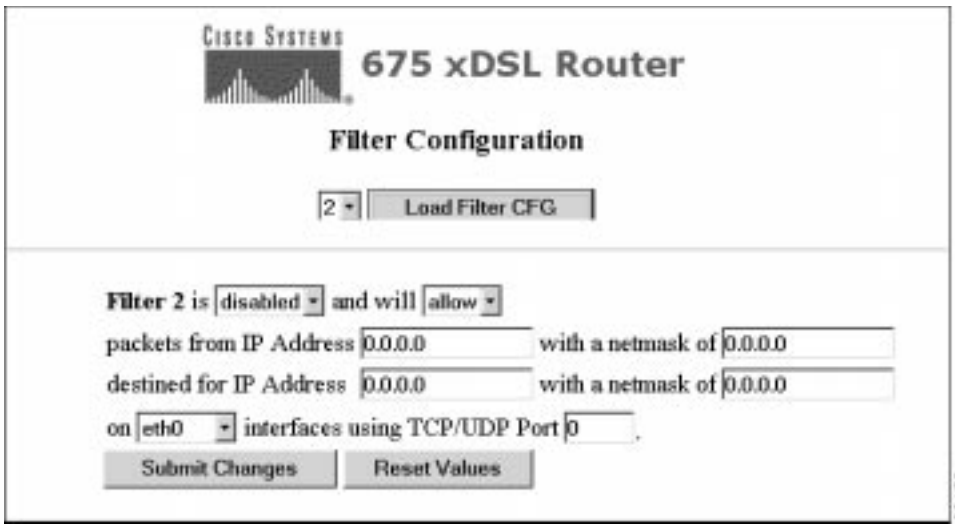
Step 4 Click on the **Submit Changes** button to apply changes or the **Reset Values** button to discard changes.

Note You must write changes using the command line interface (via a serial or telnet connection) before rebooting to apply changes. These changes take effect the next time you log in. For information on the **write** command, see Chapter 2 , “Using the Command Line Interface”.

3.6.3 Filter Configuration Screen

Click on the **Filtering** button and the Filter Configuration screen appears. This option allows you to set up filters to prevent or allow the flow of IP packets into Cisco Equipment.

Figure 3-6 Filter Configuration Screen



Setting filters

Step 1 Select the filter name and number from the first drop down menu at the top of the screen. Click on the **Load Filter CFG** button to load existing filter information.

Step 2 Set filters by completing the sentence.

Step 3 Select either the *enabled* or *disabled* option from drop down menu to activate a filter.

Step 4 Select either the *allow* or *deny* option from the drop down menu. The *allow* option allows the specified filter to accept packets from a particular IP address. The *deny* option does not permit these packets to flow to a particular IP address.

Step 5 Enter the source address and netmask of where the packet is originating. The source address is the IP address of the source computer from which you will allow or deny traffic. The source netmask is the source network from which you will allow or deny traffic. By entering a source netmask, you can filter a group of incoming IP addresses.

Step 6 Enter the destination address and netmask. The destination address is the IP address of the computer that, if allowed, will receive packets originating from the source IP address. The destination netmask is the destination network that, if allowed, will receive packets originating from the source netmask. By entering a destination netmask, you can filter a group of outgoing IP addresses.

Step 7 Select the interface that this filter affects from the drop down menu. Select the *all* option for all interfaces.

Step 8 Select the TCP/UDP Port this affects from the drop down menu. Select 0 for all ports.

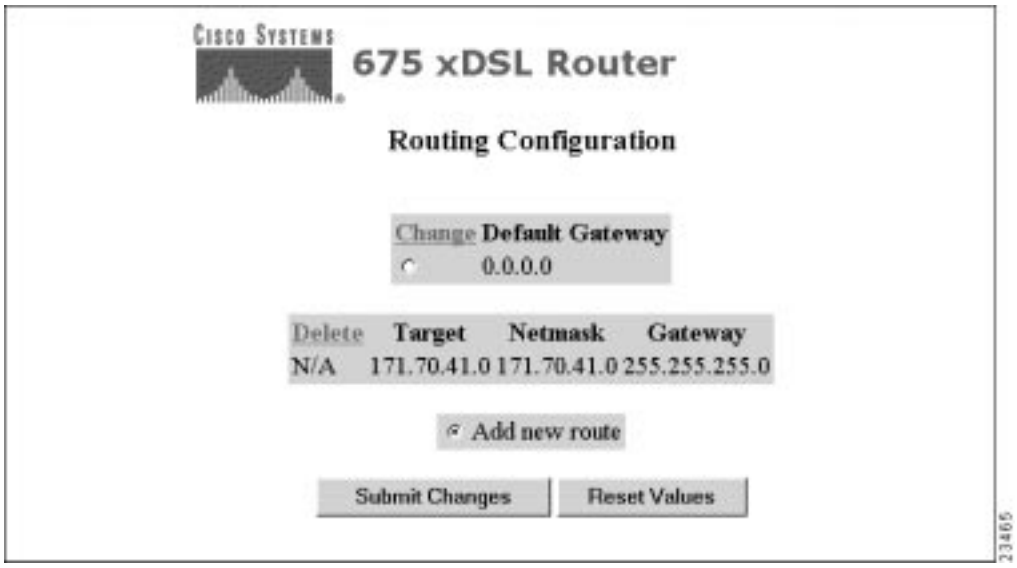
Note You must click the **Submit Changes** button to save the routing changes to NVRAM. Also, once you change an IP address, you should reboot the Cisco 67x to bind the new IP addresses to the ports.

3.6.4 Routing

Click on the **Routing** button and the Routing Configuration screen appears. This option allows you to build a new routing table or change an existing routing table. Routes consist of the IP addresses of all machines you want to communicate with plus the netmask, gateway, and metric of those machines.

Figure 3-7 Routing Configuration Screen

n



Routing Operations

The Routing Configuration screen allows you to change your routing table. See the sections below for instructions on individual tasks.

To change the default gateway

Step 1 Left click in the Default Gateway box to select it.

Step 2 Click on the **Enter** key. A new screen appears that allows you to change the IP address of the default gateway.

Step 3 Enter the IP address.

Step 4 To apply changes, click on the **Submit Changes** button. To clear the changes, click on the **Reset Values** button.

To change an existing route

Step 1 Left click on the route you want to change.

Step 2 Click on the **Enter** button. A new screen appears that allows you to change the route.

Step 3 Enter the target address, the netmask, and the gateway.

Step 4 The *target address* is the IP address of the machine with which you are trying to communicate. You can modify or delete existing IP addresses by simply typing in the new address.

Step 5 The *netmask* is the address of the network with which you want to communicate. You can modify or delete existing netmask addresses by typing in the new address.

Step 6 The *gateway* is the address of the gateway machine through which the information you are sending is routed. Data is sent through the external gateway to the destination address. Therefore, this address must be the address of a gateway that is physically linked to your network. You can modify or delete existing gateway addresses by simply typing in the new address.

Step 7 To apply changes, click on the **Submit Changes** button. To clear the changes, click on the **Reset Values** button.

Step 8 The new routing information is displayed.

To add a new route

Step 1 Click on the Add new route option.

Step 2 Click on the **Submit Changes** button. A new screen appears.

Step 3 Enter the new route including the target IP address, the netmask, and the gateway. See the section above for further descriptions on these addresses.

Step 4 To apply changes, click on the **Submit Changes** button. To clear the changes, click on the **Reset Values** button.

3.6.5 User CFG

Click on the **User CFG** button and the User Configuration screen appears. This option allows you to set up a user profile for each logical WAN connection. The user profile can be saved and reloaded each time you want to reuse it.

Figure 3-8 User Configuration Screen

Configuring users

Step 1 Select the Virtual Circuit (VC) from the drop down menu.

Step 2 Click on the **Load VC Profile** button.

Step 3 Enter or change existing user information. The field definitions are:

- **User Name**—Allows you to specify the name of user associated with this WAN connection.
- **Password**—Allows you to specify user's password.
- **Authentication**—Allows you to specify type of authentication required. Choices are None, Radius, and Pap.
- **VPI**—Allows you to specify the Virtual Path Identifier of this VC.
- **VCI**—Allows you to specify the Virtual Circuit Identifier of this VC.
- **ScalaRate**—Allows you to specify the amount of scaled bandwidth you want to set for this user.
- **Dest IP**—Allows you to specify the IP address of the subscriber-side Cisco equipment.
- **Dest Mask**—Allows you to specify the destination mask of the subscriber-side Cisco equipment.

Step 4 To submit changes, click on the **Submit Changes** button. To undo all changes, click on the **Reset Values** button.

After you apply changes, the new user configuration information is displayed.

3.7 Statistics

The **Statistics** button allows you to display statistics about applications, errors, and ports. The **Statistics** button has three sub-buttons shown below.

Figure 3-9 Statistics Button

3.7.1 Applications

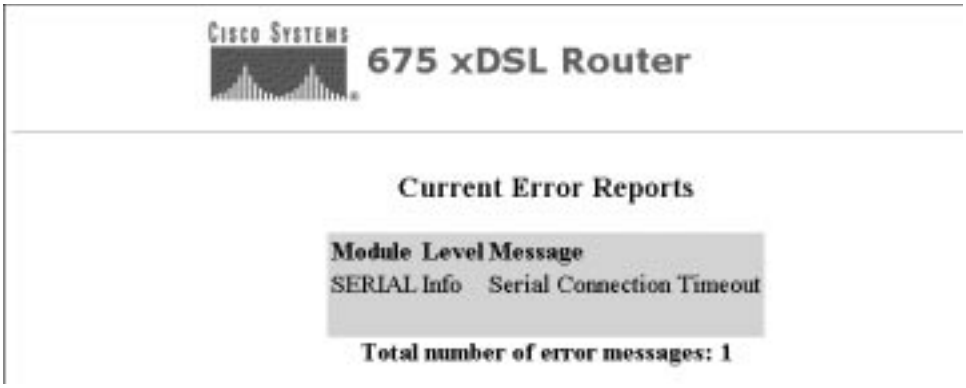
Click on the **Apps** button and the Application Statistics screen appears. This screen displays the applications that you can configure for the Cisco 67x.

Figure 3-10 Application Statistics Drop Down

3.7.2 Errors

Click on the **Errors** button and the screen below appears. This screen displays the current errors reported by the CBOS.

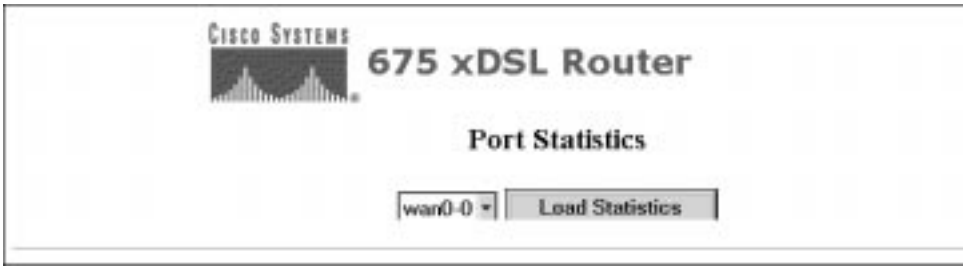
Figure 3-11 Error Report for All Modules and All Levels



3.7.3 Ports

Click on the **Ports** button and Port Statistics screen appears. This screen allows you to display statistics on the Ethernet and WAN ports.

Figure 3-12 Port Statistics Drop Down



Displaying Port Statistics

Step 1 Select a port from the drop down menu.

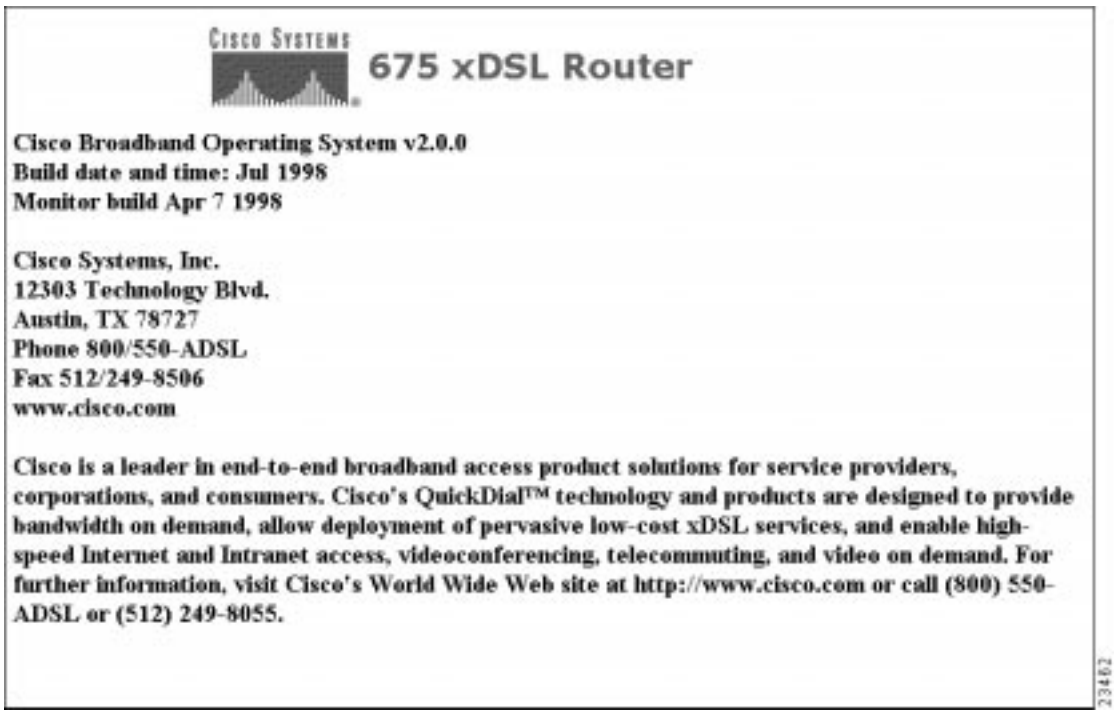
Step 2 Click on the **Load Statistics** button. The statistics for the port are displayed as shown below.

Step 3 Repeat for all ports for which you want to display statistics.

3.8 Information

Click on the **Information** button to get information about the Cisco equipment you are working on and about Cisco, Inc. The **Information** button has four sub-buttons shown below.

Figure 3-13 Copyright and Build Information



3.9 Cisco Home Page

For more information about Cisco and its products, go to the Cisco home page on the World Wide Web at **http://www.cisco.com**.

3.10 Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Note For more information about Cisco and its products, go to the Cisco home page on the World Wide Web at **http://www.cisco.com**.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com

- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

For the latest information on caveats and known problems, follow these steps to consult CCO:

Step 1 Connect to CCO as directed in the section above.

Step 2 On the CCO home page, click LOGIN, which appears in green in the menu bar at the top of the page, and log into CCO. (If you are not a registered CCO user, follow the instructions to register so that you can log in.)

Step 3 After you log in, click Software & Support on the CCO home page.

Step 4 On the Software & Support page, click Technical Tools.

Step 5 On the Technical Tools page, click Bug Toolkit II. (Bug Toolkit II is not visible on the Technical Tools page unless you log in to CCO as directed in Step 2.)

Step 6 Use one of the tools to get up-to-date bug information. For example, click Search for Bug by ID Number, then enter a bug ID, such as CSCdk09616, when prompted. For instructions on using the bug tools, go to the bottom of the Bug Toolkit II page and click Help—How to Use the Bug Toolkit.

APPENDIX A

ADSL Technology Glossary

address mask
A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called subnet mask.

AAL5
ATM Adaption Layer. This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

ADSL
Asymmetric Digital Subscriber Line. A digital subscriber line (DSL) technology in which the transmission of data from server to client is much faster than the transmission from the client to the server.

ADSLAM
Advanced Digital Subscriber Line Access Multiplexer. Concentrates and multiplexes signals at the telephone service provider location to the broader wide area network.

ATM
Asynchronous Transfer Mode. A cell-based data transfer technique in which channel demand determines packet allocation. ATM offers fast packet technology, real time, demand led switching for efficient use of network resources.

authentication
A security feature that allows access to information to be granted on an individual basis.

auto-negotiation
Procedure for adjusting line speeds and other communication parameters automatically between two computers during data transfer.

AWG
American Wire Gauge. The measurement of thickness of a wire.

bandwidth
The range of frequencies a transmission line or channel can carry: the greater the bandwidth, the greater the information-carrying capacity of a channel. For a digital channel this is defined in bits. For an analog channel it is dependent on the type and method of modulation used to encode the data.

bandwidth on demand
The ability of a user to dynamically set upstream and downstream line speeds to a particular rate of speed.

bps
Bits per second. A standard measurement of digital transmission speeds.

bridge
A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are: repeaters which simply forward electrical signals from one cable to the other, and full-fledged routers which make routing decisions based on several criteria. See repeater and router.

broadband
Characteristic of any network that multiplexes independent network carriers onto a single cable. This is usually done using frequency division multiplexing (FDM). Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another since the “conversations” happen on different frequencies in the “ether” rather like the commercial radio system.

Broadband Remote Access Server
Device that terminates remote users at the corporate network or Internet users at the Internet Service Provider (ISP) network, such as the Cisco FireRunner product that provides firewall, authentication, and routing services for remote users.

broadcast
A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

CAP encoding
Carrierless Amplitude Modulation and Phase. A modulation technology for ADSL.

central office
Refers to equipment located at a Telco or service provider’s office.

customer premise
Refers to equipment located in a user's premises.

downstream rate
The line rate for return messages or data transfers from the network machine to the user’s customer’s premise machine.

DRAM
Dynamic Random Access Memory. A type of semiconductor memory in which the information is stored in capacitors on a metal oxide semiconductor integrated circuit.

DSLAM
Digital Subscriber Line Access Multiplexer.

encapsulation
The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data.

Ethernet
One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps; a newer standard called Fast Ethernet will carry 100 Mbps.

FCC
Federal Communications Commission. A U.S. government agency that regulates interstate and foreign communications. The FCC sets rates for communication services,

FTP
File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.

hop count
A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.

HTML
Hypertext Markup Language. The page-coding language for the World Wide Web.

HTML browser
A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

http
Hypertext Transfer Protocol. The protocol used to carry world-wide web (www) traffic between a www browser computer and the www server being accessed.

ICMP
Internet Control Message Protocol. The protocol used to handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

Internet address
An IP address assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where *x* is an eight- bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

Internet
A collection of networks interconnected by a set of routers which allow them to function as a single, large virtual network. When written in upper case, Internet refers specifically to the DARPA (Defense Advanced Research Projects Agency) Internet and the TCP/IP protocols it uses.

Internet Protocol (IP)
The network layer protocol for the Internet protocol suite.

IP
See Internet Protocol.

IP address
The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

IP datagram
The fundamental unit of information passed across the Internet. It contains source and destination addresses along with data and a number of fields that define such things as the length of the datagram, the header checksum, and flags to say whether the datagram can be or has been fragmented.

ISO
International Standards Organization. A voluntary, non-treaty organization founded in 1946, responsible for creating international standards in many areas, including computers and communications.

ISP
Internet Service Provider. A company that allows home and corporate users to connect to the Internet.

ITU-T
International Telecommunications Union, Standardization Sector. ITU-T is the telecommunication standardization sector of ITU and is responsible for making technical recommendations about telephone and data (including fax) communications systems for service providers and suppliers.

LAN
Local Area Network. A limited distance (typically under a few kilometers or a couple of miles) high-speed network (typically 4 to 100 Mbps) that supports many computers (typical two to thousands).

LED
Light Emitting Diode. The lights indicating status or activity on electronic equipment.

line rate
The speed by which data is transferred over a particular line type, express in bits per second (bps).

logical port
A logical entry to a server machine. These ports are mostly invisible to the user, though you may occasionally see a URL with a port number included in it. These ports do not refer to physical locations; they are set up by server administrators for network trafficking.

loopback
A diagnostic test that returns the transmitted signal back to the sending device after it has passed through a network or across a particular link. The returned signal can then be compared to the transmitted one. The discrepancy between the two help to trace the fault. When trying to locate a faulty piece of equipment, loopbacks will be repeated, eliminating satisfactory machines until the problem is found.

MAC
Media Access Control Layer. A sub-layer of the Data Link Layer (Level Two) of the ISO OSI Model responsible for media control.

MIB
Management Information Base. A collection of objects that can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

modem pooling
The ability of a service provider to dynamically switch users' messages between modems, rather than requiring a modem to be dedicated to a particular user on a network.

multiplexer
A device that can send several signals over a single line. They are then separated by a similar device at the other end of the link. This can be done in a variety of ways: time division multiplexing, frequency division multiplexing and statistical multiplexing. Multiplexers are also becoming increasingly efficient in terms of data compression, error correction, transmission speed and multi-drop capabilities.

NAT
Network Address Translation.

network layer
The OSI layer that is responsible for routing, switching, and subnetwork access across the entire OSI environment.

node
A general term used to refer to a computer or related device; often used to refer to a networked computer or device.

NVT
Network Virtual Terminal.

octet
A networking term that identifies 8 bits. In TCP/IP, it is used instead of *byte*, because some systems have bytes that are not 8 bits.

OSI
Open Systems Interconnection. An international standardization program to facilitate communications among computers from different manufacturers. See ISO.

packet
The unit of data sent across a packet switching network.

PAP
Password Authentication Protocol.

PCI
Peripheral Component Interconnect. An industry local bus standard. Supports up to 16 physical slots but is electrically limited to typically three or four plug-in PCI cards in a PC. Has a typical sustained burst transfer rate of 80 Mbs, which is enough to handle 24-bit color at 30 frames per second (full-color, full-motion video).

Permanent Virtual Connection (PVC)
A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed.

physical layer
Handles transmission of raw bits over a communication channel. The physical layer deals with mechanical, electrical, and procedural interfaces.

physical port
A physical connection to a computer through which data flows. An “Ethernet port”, for example, is where Ethernet network cabling plugs into a computer.

port
The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host. See selector.

POTS
Plain Old Telephone Service.

PPP
Point-To-Point-Protocol. The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. See SLIP.

protocol
A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

PVC
See Permanent Virtual Connection.

RADIUS
Remote Authentication Dial-In User Service (RADIUS). A client/server security protocol created by Livingston Enterprises. Security information is stored in a central location, known as the RADIUS server.

RADIUS Accounting Client
Permits system administrators to track dial-in use.

RADIUS Security Client
Controls access to specific services on the network.

RADSL
Rate Adaptive Digital Subscriber Line (RADSL). A technique for keeping the quality of transmissions within specified parameters.

remote address
The IP address of a remote server.

remote server
A network computer that allows a user to log onto the network from a distant location.

RFC
Request for Comment. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs.

route
The path that network traffic takes from its source to its destination. The route a datagram may follow can include many gateways and many physical networks. In the Internet, each datagram is routed separately.

router
A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as “routing metrics.” See bridge and repeater.

routing table
Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

RS-232
An EIA standard which is the most common way of linking data devices together.

secret
It is the encryption key used by RADIUS to send authentication information over a network.

serial line
A serial line is used to refer to data transmission over a telephone line via a modem or when data goes from a computer to a printer or other device.

shared secret
RADIUS uses the shared secret to encrypt the passwords in the authentication packets, so outside parties do not have access to the passwords on your network.

SNMP
Simple Network Management Protocol. The network management protocol of choice for TCP/IP-based internets.

socket
(1) The Berkeley Unix mechanism for creating a virtual connection between processes. (2) IBM term for software interfaces that allow two Unix application programs to talk via TCP/IP protocols.

Spanning-Tree Bridge Protocol (STP)
Spanning-Tree Bridge Protocol (STP). Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment. When three or more LAN segments are connected by bridges, a loop can occur. Because a bridge forwards all packets which are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

spoofing
A method of fooling network end stations into believing that keep-alive signals have come from and return to the host. Polls are received and returned locally at either end of the network and are transmitted only over the open network if there is a condition change.

STP
See Spanning-Tree Bridge Protocol.

subnet
For routing purposes, IP networks can be divided into logical sub nets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

subnet mask
See address mask.

synchronous connection
During synchronous communications, data is not sent in individual bytes, but as frames of large data blocks.

SYSLOG
SYSLOG allows you to log significant system information to a remote server.

TCP
Transmission Control Protocol. The major transport protocol in the Internet suite of protocols providing reliable, connection-oriented full-duplex streams.

TFTP
Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often used to boot diskless workstations and other network devices such as routers over a network (typically a LAN). Has no password security.

Telnet
The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and act as normal terminal users of that host.

training mode
Characteristic of a router that allows it to use RADSL technology to adjust its line speed according to noise conditions on the transmission line.

transparent bridging
So named because the intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

Trivial File Transfer Protocol (TFTP)
See TFTP.

twisted pair
Two insulated copper wires twisted together with the twists or lays varied in length to reduce potential signal interference between the pairs.

UDP
User Datagram Protocol. A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first setting up a connection would take more time than sending the data.

UL
Underwriters Laboratories. A private organization that tests and certifies electrical components and devices against rigorous safety standards. A UL Listing Mark on a product means that representative samples of the product have been tested and evaluated to nationally recognized safety standards with regard to fire, electric shock, and other related safety hazards.

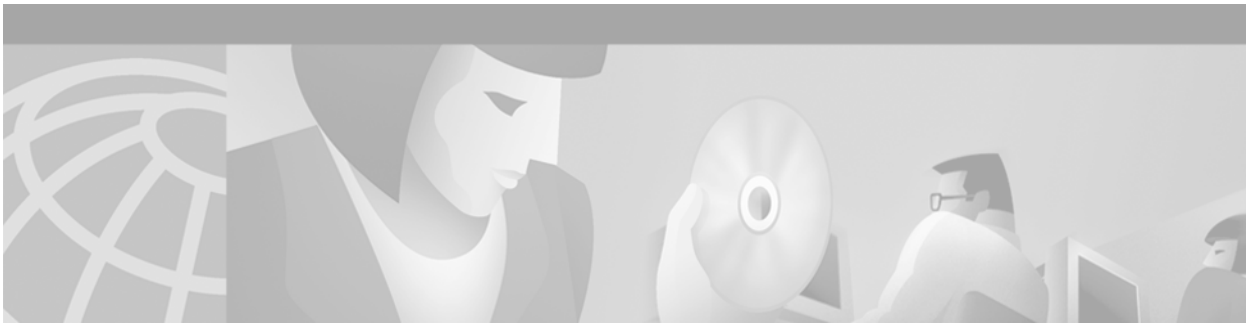
UNI signaling
User Network Interface signaling for ATM communications.

upstream rate
The line rate for message or data transfer from the source machine to a destination machine on the network. Also see downstream rate.

VC
See Virtual Connection.

Virtual Connection (VC)
A link that seems and behaves like a dedicated point to point line or a system that delivers packets in sequence, as happens on an actual point to point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

WAN
Wide Area Network. A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider).



Release Notes for the Cisco 600 Series Products

September 27, 2000

These release notes describe documentation updates for the following Cisco 600 series products:

- Cisco 627 ADSL DMT modem
- Cisco 633 SDSL modem
- Cisco 673 SDSL router
- Cisco 675 ADSL router
- Cisco 675e ADSL router
- Cisco 676 ADSL router
- Cisco 677 ADSL DMT router
- Cisco 677i and Cisco 677i-DIR ADSL over ISDN routers
- Cisco 678 ADSL router

For more detailed information about the features of the Cisco 600 series products, refer to the "Related Documentation" section on page 6. You can find information about electronic documentation in the "Obtaining Documentation" section on page 6.

Contents

These release notes provide the following information:

CISCO SYSTEMS

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

OL-0787-01

Documentation Updates

The following section replaces the "Frequently Asked Questions about the WAN LNK LED" section in the *Cisco 600 Series Installation and Operation Guide.*

Frequently Asked Questions about the WAN LNK LED

The WAN LNK LED blink patterns indicate the connection state of the customer premises equipment (CPE). Table 6-1 describes the meaning of the blink patterns that apply to all the Cisco 600 series CPEs.

Table 6-1 WAN Link LED Blink Patterns

Blink Pattern/Rate	Description
Steady ON	A link is established to the WAN port. All parameters for physical and logical connections are correctly set. The CPE successfully transmits and receives data.
Continuous rapid blinking, about 3 blinks per second	The CPE is trying to establish a connection. The pattern continues until a connection is established.
Intermittent blinking. For the Cisco 675: 6 rapid blinks followed by a 2-second pause before repeating. For the Cisco 676 or 677: 5 rapid blinks followed by a 2-second pause before repeating.	The CPE is trying to establish a physical connection. At this time, the training session is not yet completed; there are no logical connections and negotiated line conditions with other equipment (such as DSLAMs) are not yet established.
OFF	Check all connections. Ensure the WAN0 interface is not disabled.

Cisco 675 WAN LNK LED Blink Patterns

Table 6-2 describes the WAN LNK LED blink patterns that apply to the different versions of the Cisco Broadband Operating System (CBOS) on the Cisco 675 and the problems each blink pattern indicates.

Table 6-2 Cisco 675 WAN LNK Blink Patterns

CBOS Version	Authentication Failure	PVC Failure	Not Trained
2.1.*x* or 2.2.*x*	Continuous blinking for 12 seconds; then, on for 5 seconds; then it turns off. See "Authentication Problem."	On for approximately 100 seconds; then, it turns off. See "PPP Requests Are Not Being Answered."	Continuous blinking or off. See "The CPE Doesn't Train."
2.3.*x*	On. See "Authentication Problem."	On. See "PPP Requests Are Not Being Answered."	5 rapid blinks followed by a 2-second pause before repeating. See "The CPE Doesn't Train."

Cisco 677 WAN LNK LED Blink Patterns

Table 6-3 describes the WAN LNK LED blink patterns that apply to the different versions of CBOS on the Cisco 677 and the problems each blink pattern indicates.

Table 6-3 Cisco 677 WAN LNK Blink Patterns

CBOS Version	Authentication Failure	PVC Failure	Not Trained
2.1.*x* or 2.2.*x*	Continuous blinking for 12 seconds; then, on for 5 seconds; then, it turns off. See “Authentication Problem.”	On for approximately 100 seconds; then, it turns off. See “PPP Requests Are Not Being Answered.”	Continuous blinking. See “The CPE Doesn’t Train.”
2.3.*x*	On. See “Authentication Problem.”	On. See “PPP Requests Are Not Being Answered.”	5 rapid blinks followed by a 2-second pause before repeating. See “The CPE Doesn’t Train.”

Cisco 678 WAN LNK LED Blink Patterns

Table 6-4 describes the WAN LNK LED blink patterns that apply to the Cisco 678 and the problems each blink pattern indicates.

Table 6-4 Cisco 678 WAN LNK Blink Patterns

RADIUS Failure	PVC Failure	Not Trained
On. See “Authentication Problem.”	On. See “PPP Requests Are Not Being Answered.”	Off. See “The CPE Doesn’t Train.”

See the following sections for descriptions of the possible causes and corrective actions to be taken for the problems described in Table 6-2, Table 6-3, and Table 6-4.

The CPE Doesn’t Train

The Cisco 600 series never trains to a system such as the Cisco 6*xxx* series:

- ADSL/SDSL line is not connected to the Cisco 600 series.
- Subscriber is locked on the Cisco 6*xxx* series.
- Subscriber's LIM port is locked on the Cisco 6*xxx* series
- Subscriber's LIM port is not associated to an ATU-C pool
- ADSL/SDSL circuit is physically too long.
- There is excessive noise on the ADSL/SDSL circuit.

PPP Requests Are Not Being Answered

The CPE PPP requests are not being answered by the equipment on the service provider's network, such as a Cisco 7200 series or Cisco 6400. There are a number of possibilities why this would happen:

- VPI/VCI provisioning is not correct in the ATM cloud. This could signify that the service provider's equipment or the ATM switch along the path does not have the correct provisioning.
- VPI/VCI mapping in the service provider's equipment or the CPE is not configured properly.
- ATM Cell scrambling is enabled on one end of the link but not the other. The **show running** command displays an entry with "*ATM WAN Cell Scrambling = disabled*" if cell scrambling is disabled. No entry implies the default behavior of ATM cell scrambling is enabled.
- Service provider's equipment is turned off.
- CPE is configured for routing mode, but the equipment at the service provider's network that is terminating CPE traffic is configured for bridging.

Use the **show errors** command to check the contents of the error log.

Use the **show ppp** command to see a summary of each virtual circuit for PPP mode. Check that the state of each virtual circuit is opened.

```
cbos#show ppp
VC       VPI/VCI  STATE       MRU    USERNAME  RADIUS   TX       RX
wan0-0   01/01   Starting     2048   ppp1      disabled 0        60742
wan0-1   01/02   Starting     2048   ppp2      disabled 0        59950
wan0-2   01/03   Starting     2048   ppp3      disabled 1476     738
wan0-3   01/00   Starting     2048   ppp4      disabled 0        59822
```

No ATM Cell Delineation

If the CPE trains up and the WAN LNK LED turns off, this is a sign of no ATM cell delineation.Verify that you have the ATM link terminated at the central office end. Without ATM cell delineation, the router will attempt to retrain the line in 1 to 10 seconds.

DMT Firmware Incompatibility

If the CPE trains up and then immediately drops the connection, the near-end DMT firmware may not be compatible with the far-end DMT firmware. For example, an ITU G.Lite router may not train to an ANSI Issue 1 Central Office. To see the DMT firmware version installed on your router, use the **show version** command.

Timeout Set

If the WAN LNK LED turns off after the CPE has successfully been transferring data end-to-end for some time, this means that the CPE or the service provider's equipment may have a timeout set. Use the **show errors** command to see if the error log shows that timeouts caused the drop. There are two timeouts that could affect the WAN LNK LED:

- IDLE timeout—You can set this timeout on the CPE or the service provider's equipment. If you set the IDLE timeout to some value, then the CPE WAN LNK LED turns off if the CPE is idle for that specified period of time. Use the **`show timeout`** command to see the current timeout status and settings.

- SESSION timeout—This timeout can be set on the CPE or the service provider's equipment. If you set the SESSION timeout to some value, then the CPE WAN LNK LED turns off after the set time. Use the **show timeout** command to see the current timeout status and settings.

Authentication Problem

After the CPE trains, and the service provider's equipment that is being used to authenticate its PPP session is using RADIUS, then the symptoms described in Table 6-2, Table 6-3, and Table 6-4 could point to a failed RADIUS authentication. Possible reasons for a failed RADIUS authentication include:

- Service provider's equipment has the wrong IP address for the RADIUS server.
- Username and password on the CPE do not match the username and password running on the RADIUS server's user list.
- RADIUS server is not running.

Disabling RADIUS on the service provider's equipment would be a simple test to see if it is a RADIUS problem.

Useful Diagnostic Commands

Entering the **show interface wan0** command provides feedback on the wan0 configuration as well as the actual configuration negotiated with the central office equipment as shown here:

```
cbos#show interface wan0
wan0   ADSL Physical Port
       Line Trained
Actual Configuration:
  Overhead Framing:          3
  Trellis Coding:            Disabled
  Standard Compliance:       T1.413
  Downstream Data Rate:      8032 Kbps
  Upstream Data Rate:        864 Kbps
  Interleave S Downstream:   1
  Interleave D Downstream:   64
  Interleave R Downstream:   2
  Interleave S Upstream:     4
  Interleave D Upstream:     8
  Interleave R Upstream:     16
  Modem Microcode:           G96
  DSP version:               0
  Operating State:           Showtime/Data Mode
Configured:
  Echo Cancellation:         Disabled
  Overhead Framing:          3
  Coding Gain:               Auto
  TX Power Attenuation:      0dB
  Trellis Coding:            Enabled
  Bit Swapping:              Disabled
  Standard Compliance:       Multimode
  Remote Standard Compliance:T1.413
  Tx Start Bin:              0x6
  Tx End Bin:                0x1f
  Data Interface:            Utopia L1
Status:
  Local SNR Margin:          3.5dB
  Local Coding Gain:         0.0dB
  Local Transmit Power:      12.5dB
  Local Attenuation:         28.5dB
  Remote Attenuation:        18.5dB
```

```
Local Counters:
  Interleaved RS Corrected Bytes:        0
  Interleaved Symbols with CRC Errors:   2
  No Cell Delineation Interleaved:       0
  Out of Cell Delineation Interleaved:   0
  Header Error Check Counter Interleaved:0
  Count of Severely Errored Frames:      0
  Count of Loss of Signal Frames:        0
Remote Counters:
  Interleaved RS Corrected Bytes:        0
  Interleaved Symbols with CRC Errors:   0
  No Cell Delineation Interleaved:       0
  Header Error Check Counter Interleaved:0
  Count of Severely Errored Frames:      0
  Count of Loss of Signal Frames:        0
```

You can also use the **show interface wan0-0** command to see the status of the virtual circuit:

```
cbos#show int wan0-0
WAN0-0  ATM Logical Port
        PVC (VPI 1, VCI 1) is open.
        ScalaRate set to Auto
        AAL 5         UBR Traffic
        PPP LCP State: Starting
        PPP NCP State (IP Routing): Starting
        PPP MRU: 2048    HDLC Framing: enabled    MPOA Mode: VC Mux
        PPP Login: ppp1
        Authentication Type: Autodetecting/PAP
        RADIUS: disabled
        PPP Tx: 0                Rx: 60742
        Dest IP: 205.142.210.1
        Dest Mask: 255.255.255.255
        IP Port Enabled
```

Related Documentation

Use these release notes in conjunction with the Cisco 600 series product documentation found at http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c600s/index.htm.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.