Technical Reference Guide

SpeedStream™ 5700, 5800, 7400, 7800 & FlowPoint™ Routers

Part Number: 956-00-976-01

Contents

Key Router Features

This guide provides essential information for router installation and troubleshooting. It covers:

SpeedStream Models 5711, 5781, 5861, 7451, 7851

FlowPoint Models 144, 2200

The principal software features embedded in each router are described below:

DHCP (Dynamic Host Configuration Protocol) allows dynamic IP addressing from the WAN. Router software provides DHCP Server, Client, & Relay functions.

NAT (Network Address Translation) allows multiple devices on your network to share a single WAN IP address. It also allows mapping of existing LAN IP addresses to a range of WAN IP addresses

WAN Protocols -- IP/IPX routing, Bridging, and MAC Encapsulated Routing (MER) -- support a wide range of network applications.

Firewall (IP filtering) software prevents unwanted visitors from accessing the LAN.

Secure VPN (Virtual Private Network) is optional, key-activated software that protects data while it is being transferred across the Internet.

Windows-Based Management Tools are provided on an Installation CD:

Quick Start GUI simplifies initial router configuration.

Configuration Manager GUI provides access to Advanced Configuration.

Terminal Window lets you access the Command Line Interface directly using a customized terminal emulator.

SNMP tool is useful when you have made access to your router more secure by changing its SNMP community name and/or the UDP port that SNMP uses.

TFTP and BootP tools allow you to reboot a router using the companion BootP and TFTP servers.

WAN Port Monitor graphically displays and logs ongoing router activity.

Router Ports

Ethernet LAN Connection

A LAN cable connection is made through an 8-pin RJ-45 10Base-T (10 Mbps Ethernet/IEEE-802.3) port on the rear of the router.

DSL WAN Connection

Connectivity to a DSL network is made through an 8-pin RJ-45 port on the rear of the router.

Note: *Since only the center two pins (4 and 5) are active, a RJ-11 can be connected to this RJ-45 port by centering the RJ-11 connector inside the RJ-45 port.*

Console Port Connection

An 8-pin RJ-45 Console port provides asynchronous RS232 connectivity with the serial port of a workstation. The Console port is primarily used for troubleshooting and diagnostics. A Console cable kit that contains a DB-9 to RJ-45 adapter and a cable is provided with each router.

Voice Port Connection

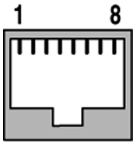
SpeedStream 7400 VoDSL routers include voice (POTS) 6-pin RJ-11 ports for telephone and fax machines.

Port Wiring

Pin	Ethernet	DSL	Console	Voice
1	Transmit +	Not connected	Receive data	Not connected
2	Transmit -	Not connected	Request to send	Not connected
3	Receive +	Not connected*	Not used	Tip or Line A
4	Ground	Tip	Transmit data	Ring or Line B
5	Ground	Ring	Ground	Not connected
6	Receive -	Not connected*	Clear to send	Not connected
7	Ground	Not connected	Not used	N/A
8	Ground	Not connected	Ring indicator	N/A

** Router Model 120-5861-001 uses these pins*

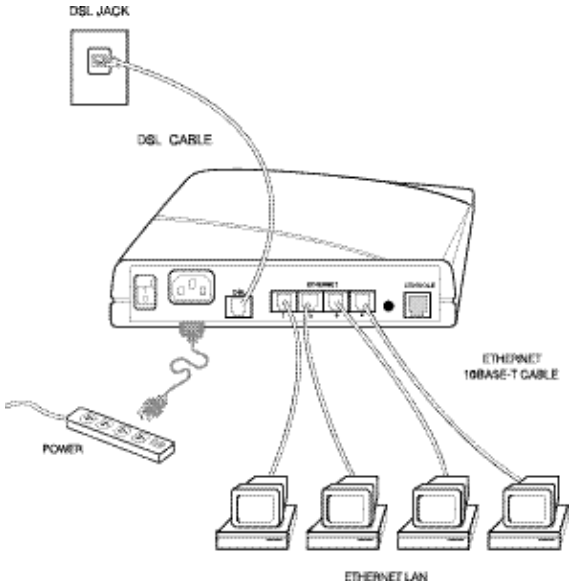
Pin Orientation



Router Cables

Connecting a LAN Workstation to the Router

The example below shows 4 workstations connected to a FlowPoint 2200 SDSL router. In this situation, workstation network adapter cards are connected to the 4 Ethernet ports of the router via straight-through cables. Other single Ethernet port routers require crossover cables.



Connecting a 10Base-T Hub to a Router

Hubs that do not have an internal crossover function require a crossover cable to coordinate the hubs' transmit and receive lines (see Port Wiring table on previous page). Some hubs have an "uplink" port that is wired as a crossover connection, allowing you to connect it to a router with a straight-through cable.

Some hubs auto-sense a hub-to-hub configuration and compensate internally. Other hubs have a manual switch, which can be used to indicate a hub-to-hub connection. Port labels vary from manufacturer to manufacturer, so check your hub's documentation for details. Both auto-sensing and hardwired hubs typically have one or more ports labeled "Crossover", "Uplink", or similar indicators. Likewise, a switch may be labeled "Crossover" or "X" on one end and "Straight" or "=" on the other end.

Device Cables for Routers with 4 10Base-T Ethernet ports (built-in uplink hub)

To connect the router hub to a workstation, use the straight-through cable (provided).
To connect the router hub to an uplink hub port, use the straight-through cable (provided).
To connect the router hub to a standard hub port, use the crossover cable (provided).

Device Cables for Routers with a single 10Base-T Ethernet port

To connect the router Ethernet port to a workstation, use the crossover cable (provided).
To connect the router Ethernet port to an uplink hub port, use the crossover cable (provided).
To connect the router Ethernet port to a standard hub port, use a straight-through cable (not provided).

Connecting a 100Base-T Hub to a Router

You can connect to a 100Base-T hub if the hub has a 10/100 switch, however, the switch must be set for a 10Base-T port connection to the router.

Switching capabilities vary from hub to hub. Some hubs have auto-sensing, some require a manual switch to be set, and some do not handle a 10-to-100 conversion at all. Check you hub's documentation for details.

Ethernet 10Base-T Crossover Cable Wiring

The two ends of a crossover cable must be crossed as shown below:

Pin	End 1	End 2
1	Transmit +	Receive +
2	Transmit -	Receive -
3	Receive +	Transmit +
4	Ground	Ground
5	Ground	Ground
6	Receive -	Transmit -
7	Ground	Ground
8	Ground	Ground

Console Cable RJ-45 to DB9 Adapter Cable Wiring

RJ-45 Pin	Color	DB-9 Pin	Description
1	Blue	**2**	Receive
4	Red	**3**	Transmit
5	Green	**5**	Ground
2	Orange	**7**	Request to send
6	Yellow	**8**	Clear to send

Router Lights

FlowPoint 144 IDSL Router

The lights on the front panel are labeled:

PWR LAN LINE CH1 CH2 NT1

Interpretation:

CH1 / CH2 flashing = WAN traffic
LAN flashing = LAN traffic
PWR green and NT1 flashing = Bad cabling on WAN
PWR / LINE / NT1 green and CH1 / CH2 off = Good cabling, but bad PVC/DLCI
PWR / LINE / CH1 / CH2 / NT1 all green = Ready

Dual Ethernet Router

The lights on the front panel are labeled:

PWR LAN TX0 RX0 TX1 RX1

Interpretation:

PWR green = Power applied
TEST amber = POST in progress
TEST green = POST successful
TX0 flashing = Transmitting on ETH/0 interface
RX0 flashing = Receiving on ETH/0 interface
TX1 flashing = Transmitting on ETH/1 interface
RX1 flashing = Receiving on ETH/1 interface

All Other SpeedStream and FlowPoint Routers

The lights on the front panel are labeled:

PWR TEST LINK WAN LANT LANR

Interpretation:

PWR green = Power applied
TEST amber = POST in progress
TEST green = POST successful
TEST red = In password override mode
TEST flashing = Stuck in boot menu or no kernel
LINK amber = Establishing DSL link
LINK green = DSL link established
LINK red = WAN speed locked down (SDSL)
WAN flashing = WAN transmit and receive
LANT flashing = LAN Transmit data
LANR flashing = LAN Receive data
PWR/TEST/LINK all green = Ready

DIP Switches and Manual Boot Options

When a router with DIP switches is shipped, it is set for automatic boot from FLASH memory. If you wish to allow for network booting, change the order of boot procedures, or perform a manual boot, you must enter manual boot mode. The Options menu will be displayed if the router's kernel is missing.

To access manual boot mode, first set switch 6 in the down position, then reboot the router by issuing the reboot command or powering up the router.

The router then displays the Options menu:

1. Retry start-up
2. Boot from FLASH memory
3. Boot from network
4. Boot from specific file
5. Configure boot system
6. Set date and time
7. Set console baud rate
8. Start extended diagnostics

To return to automatic boot mode, set switch 6 up, then reboot by selecting options 1, 2, 3, or 4. The router will boot router software automatically in the order and manner that you have specified.

Option 1: Retry Start-Up

You can reboot the router in the boot procedure order, which is either the one you have specified or the default order. The default order is to boot from FLASH memory and then from the network (if defined).

Option 2: Boot from FLASH Memory

The router will attempt to boot from FLASH memory. If the boot is unsuccessful, the router will return to manual boot mode.

Option 3: Boot from Network

First, you need to define permanent network boot parameters using Option 5. Then, Option 3 will allow you to perform a manual boot from the network.

If you have not defined network boot parameters, the router attempts to locate a BootP or RARP server on the network. BootP can be used to supply an IP address, a TFTP Server IP address, and a filename. RARP is used to obtain an IP address when the MAC address is known. The router assumes that the RARP server is also capable of performing the duties of a TFTP server

and it will request the filename KERNEL.F2K or the filename assigned when permanent network boot parameters are set. If a BootP or RARP server exists and is properly configured with the router's MAC address, the router will boot from the network. If unsuccessful, the router will return to manual boot mode.

Option 4: Boot from Specific File

You can temporarily override permanent network boot parameters when you perform a network boot. After you set the parameters, hit the return key and the router will boot from the network using the temporary boot parameters. If the boot is unsuccessful, the router will return to manual boot mode. Once you have installed router software on a network TFTP server, you can have the router boot across the LAN. Network booting requires three parameters: the boot IP address, the TFTP boot server address, and the file name.

Identifying Fatal Boot Failures

Fatal boot failures can be identified by the light patterns displayed on the front panel of the router. **TEST, LNK, WAN, and LANT** display these fatal errors according to the following light patterns.

0 = *light off*
G = *light blinking green*
Y = *light blinking yellow*
* = *light could be on, off, or blinking*
FG = *light blinking fast*

0-0-0-G	CPM fail
0-0-G-0	Timer fail
0-0-G-G	Bad FCS
0-G-0-0	DRAM fail
0-G-0-G	Interrupt fail
0-G-G-0	SCC fail
Y-0-0-0	CPU step fail
Y-0-0-G	Ethernet loop fail
FG-0-0-*	Wait stuck in the boot menu; kernel file could be missing.
G-0-0-*	The router is issuing BootP requests.

Any other combinations of the four lights flashing in a regular pattern will indicate an internal error. Should this occur, return the router to the factory for repair or replacement.

Note: Non-fatal errors are not displayed by the lights, but they do prompt the system to print explanatory messages on the console.

Quick Start Windows GUI

What Can Be Configured with the Windows-based Quick Start GUI

- WAN protocol and port address
- Data rate (IDSL)
- PVC or DLCI (data and voice)
- IP routing or bridging
- Domain name, primary and secondary DNS
- DHCP enable/disable
- LAN IP address and mask
- Address Translation
- SNMP community name and port
- Microsoft networking enable/disable

System Defaults BEFORE Quick Start is Run

Ethernet IP address: 192.168.254.254

Ethernet IP Mask: 255.255.255.0

Voice PVC = 0*39 or DLCI = 22

IP routing and bridging OFF, RIP ON.

DHCP server ON with auto-detect of other servers enabled
Command: `dhcp add 192.168.254.0 255.255.255.0` (Subnet to serve)

Default DHCP address pool is from 192.168.254.2 through 192.168.254.20
Command: `dhcp set addr 192.168.254.2 192.168.254.20` (Address pool)

Router's address is the gateway for the network
Command: `dhcp set value 192.168.254.0 3 192.168.254.254` (Gateway)

System Defaults AFTER Quick Start is Run

Ethernet IP address: 192.168.254.254

Ethernet IP Mask: 255.255.255.0

DHCP server is ON with auto-detect of other servers enabled

Default DHCP address pool is from 192.168.254.2 through 192.168.254.20

Remote entry called `internet` is created

For the Internet WAN link:

IP routing is ON (source IP set by user)
Default IP route
Address Translation is ON
WAN protocol ATM PVC = 0*39 (most SDSL) or 0*35 (DMT) and Frame Relay DLCI =16

Resetting the Quick Start program to Factory Defaults

Delete the file C:\xDSL\ROUTER.INI on the management workstation. This causes the Quick Start program to think that it is being run for the first time.

Easy Setup Web GUI

Easy Setup is a software program in the router's kernel that allows you to configure a router on any platform – Windows, Macintosh™, or Unix – via a web browser. After opening a browser, you should enter the router's default address `192.168.254.254` in the URL bar. You must next enter the default User Name `login` and Password `admin` in the Network Password window. A series of router configuration windows will appear that allow you to configure the following:

- WAN protocol and port address
- Data rate (FlowPoint 144 router only)
- PVC or DLCI
- IP routing or Bridging
- Domain name, primary and secondary DNS
- DHCP enable/disable
- LAN IP address and mask
- Address Translation
- SNMP community name and port
- Block HTTP, SNMP, Telnet access
- Microsoft networking enable/disable
- Activate software keys
- IPSec (if option enabled)

Scripting Options

Examples of basic configuration scripts are provided in subsequent sections of this guide. However, more advanced users may wish to consult the **Command Line Interface Reference Manual** that is available on the Installation CD. It provides a comprehensive list of router commands that allow you to:

- Set names, passwords, PVC numbers, and link and network parameters
- Configure specific details within a protocol, such as IP or IPX addresses, and IP protocol controls
- Activate bridging and routing protocols
- Manage the router's file system
- Set bridging filters
- Configure DHCP
- Configure NAT
- Configure Telnet/SNMP security
- Configure host mapping
- Configure IP multicast
- Configure IP filtering (firewall)
- Configure encryption and tunneling (VPN)
- Configure a Dual-Ethernet router
- Issue online status commands
- Monitor error messages
- Set RIP options
- Enable software options keys

Login

When a Terminal Window is opened via a Telnet or Console connection, you are prompted for a password. The default password is `admin`. See the Password Bypass section if you forget the password.

Command Input

The router Command Line Interface follows these conventions:

- Command line length may be up to 120 characters long.
- The Command Line Interface is not case sensitive except for passwords and router names.
- Parameters between characters < and > must be entered.
- Parameters between characters [and] are optional.
- All commands are positional; i.e. each keyword/parameter must be entered in the order displayed.
- The router has a 10 line command buffer.
- Control P will recall the last typed command; Control N will scroll in the opposite direction.
- When Telneting to the router, entering SYS LOG START will display event messages.

Command Output

After execution of most commands, the system will return a `#` to indicate the end of command execution. If you have not entered the correct parameters, the syntax of the command is displayed.

System-level Commands

```
system
```

Router Configuration Commands

```
eth
remote
adsl
atm
eth (specific to the Dual Ethernet router)
hdsl
isdn/idsl
sdsl
dhcp
l2tp
filters
save
erase
```

File System Commands

```
copy
save
erase
dir
msfs
format
execute
rename
```

? or HELP

This lists the commands at the current level as well as subcommands. At the lowest level of the subcommand, entering a **?** may return the syntax of the command. Note that **?** will be taken as a character string in some commands.

Top-Level Commands

?	help	version
filter	logout	exit
reboot	mem	ps
copy	dir	delete
rename	execute	format
sync	msfs	ifs
ipifs	iproutes	arp
ipxroutes	ipxsaps	bi
system	eth	save
erase	key	remote
call	ping	tcp
dhcp	l2tp	ipsec
ike	atom	dsp
sdsl	voice	

Working with Scripts

If you elected to install the documentation and samples when installing the Quick Start GUI, a set of sample configuration files should have been copied to the Samples subdirectory (C:\DSL\samples). These files contain CLI configuration commands that can be copied to the router and run with the `execute` command. Be sure to select the correct sample file for your configuration. Each file will probably need some edits to make it fit your network settings. The following sample scripts are provided:

ADSL with MAC Encapsulated Routing	- adsl_mer.txt
Dual Ethernet	- eth_ip.txt
Dual Ethernet with filters	- eth_fil.txt
Dual Ethernet with L2TP, router A	- eth_tuna.txt
Dual Ethernet with L2TP, router B	- eth_tunb.txt

IDSL IP routing	- idsl_ip.txt
IDSL Bridging	- idsl_brg.txt
ISDN HQ example	- is_hq.txt
ISDN SOHO example	- is_soho.txt
IP Filters for internet remote	- filters.txt
IPSec Main mode example, Home	- ipsec1cp.txt
IPSec Main mode example, Office	- ipsec1co.txt
IPSec Aggressive example, Home	- ipsec2cp.txt
IPSec Aggressive example, Office	- ipsec2co.txt
L2TP CLI example, Client router	- L2_LAC.txt
L2TP CLI example, Internet router	- L2_inter.txt
L2TP CLI example, ISP router	- L2_isp.txt
L2TP CLI example, LNS router	- L2_LNS.txt
SDSL Central office end IP	- sd_co_ip.txt
SDSL Central office end bridge	- sd_co_bg.txt
SDSL Customer premises end IP	- sd_cp_ip.txt
SDSL Customer premises end bridge	- sd_cp_bg.txt
SDSL Frame Relay IP	- fr_ip.txt
SDSL Frame Relay bridging	- fr_brg.txt
VPN CPE example from html on CD	- vpn_cpe.txt
VPN CO example from html on CD	- vpn_co.txt

The first example below shows how to run a script on a FlowPoint 144 IDSL router when it has no existing configuration.

Status at the beginning of Test 1:
Only the KERNEL.FP1 file exists in the router file system.
Type the **`dir`** command to confirm Quick Start application
Select **SCRIPT_1** (default) as the script in Quick Start
Copy the script from the PC to the router and named **AUTOEXEC.BAT** on the router.
The router is rebooted.
As soon as the router is booted, it looks for AUTOEXEC.BAT file on the router.
If it exists (and it does in this case), it is executed and renamed to AUTOEXEC.OLD.

Result of Test 1:
The router is rebooted to its **factory default configuration** *plus* the SCRIPT_1. commands in the AUTOEXEC.BAT file.

The second example shows what happens when you run a script on a router that already has a configuration.

Status at the beginning of Test 2:
No AUTOEXEC.BAT or AUTOEXEC.OLD files exist in the router file system.

Type the **`dir`** command to confirm Quick Start application

The file **SCRIPT_1** (default) is selected as the script in Quick Start
The script is copied from the PC to the router and named **AUTOEXEC.BAT** on the router.
The router is rebooted.
As soon as the router is booted, it looks for AUTOEXEC.BAT file on the router.
If it exists (and it does in this case), it is executed and renamed asAUTOEXEC.OLD.

Result of Test 2:
The router is rebooted to its **existing configuration** *plus* the commands in the AUTOEXEC.BAT file, however, the router is **NOT configured properly for SCRIPT_1.**

Interesting Note:

After **Test 2** is run, the results from **Test 1** can be obtained by:
Starting **Quick Start.**
Selecting the **Tools** menu.
Selecting **Upgrade/Backup** and then **Reset Defaults**.

This will cause the router to:
Reboot to factory default settings.
Rename AUTOEXEC.OLD as AUTOEXEC.BAT.
Execute AUTOEXEC.BAT.
Rename AUTOEXEC.BAT as AUTOEXEC.OLD.

How to Duplicate Quick Start on Non-Windows Platforms

If your computer is not running Windows, or you simply wish to configure the router for Internet access via a script, simply copy the commands shown below. You will then need to modify the PVC, protocol, and DHCP commands (in bold) as appropriate for the router model.

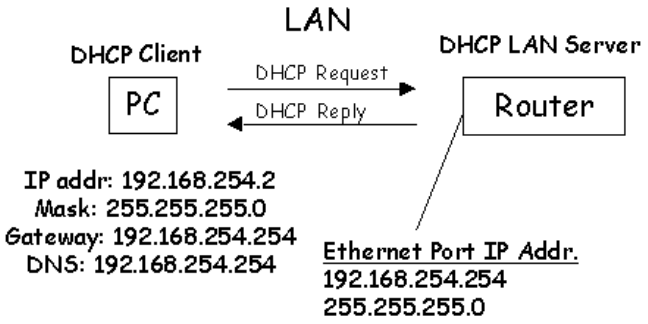
For a FlowPoint 144 IDSL router with a WAN address of 190.225.63.2 and NAT enabled, the script might appear as follows:

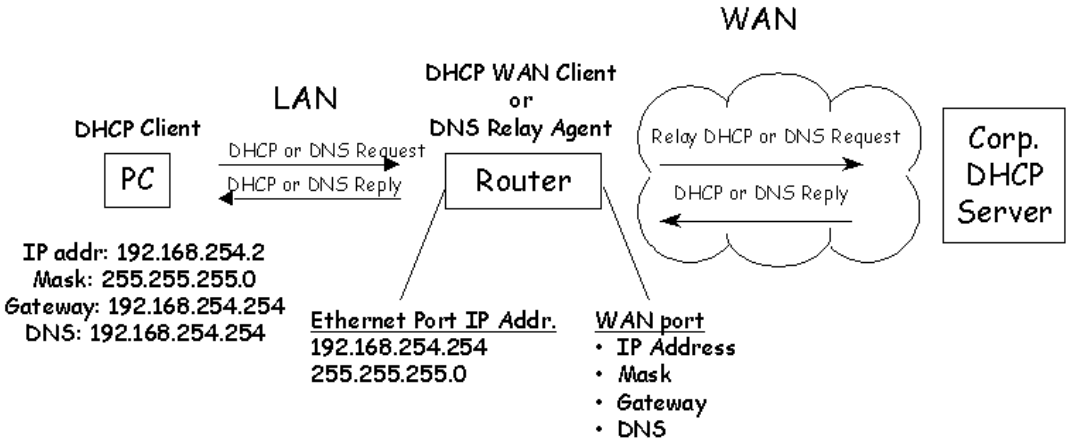
```
eth ip enable
remote add internet
remote setdlci 16 internet
remote setproto fr internet
remote setsrcipaddr 190.225.63.2 255.255.255.248 internet
remote addIProute 0.0.0.0 255.255.255.255 1 internet
remote setiptranslate on internet
dhcp add 192.168.254.0 255.255.255.0
dhcp set addr 192.168.254.2 192.168.254.20
dhcp set value 192.168.254.0 15 192.168.254.254
dhcp set value 192.168.254.0 0 myisp.com
save
reboot
```

DHCP

DHCP is a service that allocates IP addresses automatically to any DHCP client (any device, such as your PC) attached to the network that is requesting an IP address. DHCP is also used to acquire IP addresses and options (such as the subnet mask, DNS, gateway, etc.) automatically from the WAN.

The router functions described above fall into the categories of DHCP Server, Client, and Relay Agent. On the practical level, acquiring router initialization parameters with DHCP translates into avoiding the more tedious initialization process of manually reconfiguring router and/or PC addresses so that they are in the same network.





DHCP Server Defaults

Server is ON with Auto-detect enabled.
If another DHCP server is detected, the router DHCP server disables itself.
It auto-generates a DHCP address pool.
When the Ethernet port address is changed, the DHCP address pool is automatically rebuilt for the new IP subnet.
When no DNS information is configured in the DHCP server, the router's IP address is placed in the configuration.

DHCP Client becomes active on the WAN when the WAN interface has not been configured completely. The router will attempt to "fill in the blanks" in the WAN port configuration.

IP address pool = .2 through .20 in the same subnet as the Ethernet interface
Mask = Same as Ethernet interface mask
Gateway = Ethernet interface address
DNS = Ethernet interface address

Configuring DHCP

To configure DHCP for a network, the network administrator defines a range of valid IP addresses as well as other parameters to be used in the subnetwork. Once DHCP is configured for the network, each DHCP client (your PC for example) can easily request an IP address from the pool of valid IP addresses. The DHCP client will learn part or all of the network parameters automatically. IP addresses and options assigned to a client are collectively called the **lease**. The lease is only valid for a certain period and is automatically renewed by the client.

NOTE 1: The TCP/IP protocol has to be active on all networked PCs for DHCP to work.

NOTE 2: In Windows, DHCP is enabled by selecting it on your PC (under Settings, Control Panel, Network, and TCP/IP in Configuration).

Configuring DHCP can be a complex process, therefore, this section is intended for network managers. DHCP administration and configuration is divided into the following parts:

1. Manipulating subnetworks and explicit client leases
2. Setting option values
3. BootP
4. Defining option types
5. Other information

To save the DHCP configuration or changes to FLASH memory in the router, be sure to use the command `dhcp save.`

1. Manipulating subnetworks and explicit client leases

The manipulation of subnetworks and client leases is divided into the following parts:

- Enabling/disabling a subnetwork or a client lease
- Adding subnetworks and client leases
- Setting the lease time
- Manually changing client leases

To enable/disable a subnetwork or a client lease, use the commands:

```
dhcp enable <net> <ipAddr>
dhcp disable <net> <ipAddr>
```

To enable the subnetwork 192.168.254.0, if that subnetwork exists, type:

```
dhcp enable 192.168.254.0
```

To enable the client lease 192.168.254.17 if that client lease exists, type:

```
dhcp enable 192.168.254.17
```

To disable the client lease 192.168.254.18 if that client lease exists, type:

```
dhcp disable 192.168.254.18
```

To check the results of these commands, use:

```
dhcp list
```

If the client lease does NOT exist, it must be explicitly created.

The following commands are used to add/delete subnetworks. Only one subnetwork with one pool of IP addresses may be defined for a subnet.

To add a subnetwork, use:

```
dhcp add <net> <mask>
```

To remove a subnetwork, use:

```
dhcp del <net>
```

All client leases associated with this subnetwork are automatically deleted.

The following command will create a subnetwork 192.168.254.0 with a subnet mask of 255.255.255.0:

```
dhcp add 192.168.254.0 255.255.255.0
```

The following command will delete the subnetwork 192.168.254.0 and will delete all client leases associated with that subnetwork:

```
dhcp del 192.168.254.0
```

Client leases may either be created dynamically or explicitly. Usually client leases are created dynamically when a PC boots and asks for an IP address. To add an explicit client lease, a subnetwork *must* already exist (use `dhcp add <net> <mask>` to add a subnetwork). Use the command:

```
dhcp add <ipAddr>
```

To remove a client lease, type:

```
dhcp del <ipAddr>
```

NOTE: An administrator may create a client lease that is part of a subnet, but does not fall within the pool of IP addresses.

To explicitly add the client lease 192.168.254.31, use:

```
dhcp add 192.168.254.31
```

To delete the client lease 192.168.254.31, use:

```
dhcp del 192.168.254.31
```

Dynamic client leases are created from the pool of IP addresses associated with that subnetwork. To set or change the pool, use:

```
dhcp set addresses <firstipAddr> <lastipAddr>
```

To clear the values from the pool, use:

```
dhcp clear addresses <net>
```

Any client leases that currently exist will NOT be affected.

To remove a client lease that was dynamically created, use:

```
dhcp del <ipAddr>
```

Caution: If <ipAddr> is a subnet, you will delete the entire subnet.

Setting the lease time

The information given by the DHCP server (router) to your PC is leased for a specific amount of time. The client lease has already been selected. The DHCP server will select the lease time based on the option defined for the client lease. If the client lease option is a specific number or is infinite, then the server uses the specified lease time associated with this client lease. If the client lease option is "default", then the server goes up one level (to the subnetwork) and uses the lease time explicitly specified for the subnetwork. If client and subnetwork lease options are both "default" values, then the server uses the lease time defined at the global level (server). The minimum lease time is 1 hour; the global default is 168 hours.

To set the lease time explicitly for the client lease, use:

```
dhcp set lease <ipAddr> <hours>
```

To set the lease time explicitly for the subnetwork lease, use:

```
dhcp set lease <net> <hours>
```

To set the lease time explicitly for the global lease, use:

```
dhcp set lease <hours>
```

To set the lease time to "default" for the client 192.168.254.17, use:

```
dhcp set lease 192.168.254.17 default
```

To set the subnetwork lease time to infinite for the subnet 192.168.254.0, use:

```
dhcp set lease 192.168.254.0 infinite
```

To set the global lease time to 2 hours, use:

```
dhcp set lease 2
```

Manually changing client leases

Administrators will generally NOT need to change client leases manually. However, if the need arises to do so, use the following commands.

WARNING: The client will not be aware that the administrator has changed or released a client lease!

This command will change the client lease expiration time to a given value:

```
dhcp set expire <ipAddr> <hours>
```

Setting the expiration time to "default" will cause the server to compute the lease time using the algorithm described earlier. Use this command to release the client lease so it becomes available for other assignments:

```
dhcp clear expire <ipAddr>
```

2. Setting option values

Administrators will want to set the values for global options, options specific to a subnetwork, or options specific to a client lease.

NOTE: See RFC 1533 for the description of various options.

The server returns values for options explicitly requested in the client request. It selects the values to return based on the following algorithm:

If the value is defined for the client, then the server will return the requested value for an option. If the value for the option has not been set for the client, then the server returns the value option defined for the subnetwork. If the value option does not exist for the client AND does not exist for the subnetwork, then the server returns the value defined globally. If the value option is not defined anywhere, the server will NOT return any value for that option in reply to the client request.

IMPORTANT: When replying to a client request, the server does not:

- *Return any option values NOT requested by the client.*
- *Support the definition of a "class" of clients.*
- *Return any non-default option values UNLESS the client requests the option value AND the server has a value defined for that option.*
- *Return any non-default values on the client subnet UNLESS the client requests the value for that option.*

To set the value for a global option, use:

```
dhcp set valueoption <code> <value> ...
```

The code can be a number between 1 and 61 or a keyword. To see the list of predefined and user-defined options, type: `dhcp list definedoptions`

To clear the value for a global option, use:

```
dhcp clear valueoption <code>
```

To set the global value for the domain name server option, type:

```
dhcp set valueoption domainnameserver 192.168.254.2
192.168.254.3
```

To set the value for an option associated with a subnetwork, type:

```
dhcp set valueoption <net> <code> <value>...
```

To clear the value for an option associated with a subnetwork, use:

```
dhcp clear valueoption <net> <code>
```

Examples:

```
dhcp set valueoption 192.168.254.0 gateway 192.168.254.254
dhcp set valueoption 6 192.84.210.75 192.84.210.68
```

To set the value for an option associated with a specific client, use:

```
dhcp set valueoption <ipAddr> <code> <value>...
```

To clear the value for an option associated with a specific client, type:

```
dhcp clear valueoption <ipAddr> <code>
```

Example:

```
dhcp set valueoption 192.168.254.251 winserver 192.168.254.7
```

To list the values for global options as well as subnet and client lease information, use:

```
dhcp list
```

To list options that are set for that subnet/client lease and information, type:

```
dhcp list <net>|<ipAddr>
```

This command lists all available options (predefined and user-defined options):

```
dhcp list definedoptions
```

This command lists all available options starting with the string "name".

```
dhcp list definedoptions name
```

To list the lease time use:

```
dhcp list lease
```

This command lists the subnet 192.168.254.0 including any options set specifically for that subnet:

```
dhcp list 192.168.254.0
```

Administrators may wish to specify that certain client leases AND certain subnetworks can satisfy BootP requests.

3. BootP

BootP and DHCP provide services that are very similar. However, BootP is an older service; it offers a subset of the services provided by DHCP. The main difference between BootP and DHCP is that the client lease expiration for a BootP client is always *infinite.*

Caution: Remember that when BootP is enabled, the client assumes that the lease is infinite. By default, the DHCP server will NOT satisfy BootP requests unless the administrator has explicitly enabled BootP (at the subnetwork or lease level).

To allow BootP request processing for a particular client/subnet, use the command:

```
dhcp bootp allow <net>|<ipAddr>
```

To disallow BootP request processing for a particular client/subnet, type:

```
dhcp bootp disallow <net>|<ipAddr>
```

The following commands let the administrator specify the TFTP server (boot server) and boot file name. The administrator will first configure the IP address of the TFTP server and file name (kernel) from which to boot. This is particularly useful if the kernel in the router is FLASH, corrupt, or does not exist.

To set the IP address of the server and the file to boot from, enter:

```
dhcp bootp tftpserver[<net>|<ipAddr>] <tftpserver ipAddr>
dhcp bootp file [<net>|<ipAddr>] <file name>
```

To clear the IP address of the server and the file to boot from, type:

```
dhcp bootp tftpserver [<net>|<ipAddr>] 0.0.0.0
```

To set the global BootP server IP address to 192.168.254.7:

```
dhcp bootp tftpserver 192.168.254.7
```

To set the subnet 192.168.254.0 server IP address to 192.168.254.8:

```
dhcp bootp tftpserver 192.168.254.0 192.168.254.8
```

To set the client 192.168.254.21 server IP address to 192.168.254.9

```
dhcp bootp tftpserver 192.168.254.21 192.168.254.9
```

To set the subnet 192.168.254.0 boot file to "kernel.100":

```
dhcp bootp file 192.168.254.0 kernel.100
```

To clear the global BootP server IP address and file name:

```
dhcp bootp tftpserver 0.0.0.0
```

To clear the subnet 192.168.254.0 server IP address and file name:

```
dhcp bootp tftpserver 192.168.254.0 0.0.0.0
```

4. Defining Option Types

A DHCP option is a code, length, or value. An option also has a "type" (byte, word, long, longint, binary, IP address, string). The subnet mask, router gateway, domain name, domain name servers, NETBIOS name servers, etc. are all DHCP options. Please refer to RFC 1533.

Most of the time users will not need to define their own option types. The list of predefined option types based on RFC 1533 can be shown by typing:

```
dhcp list defined options
```

The following commands are available for adding/deleting option types:

```
dhcp add <code> <min> <max> <type>
```

To list option types that are currently defined, type:

```
dhcp list definedoptions ...
```

To list the definitions for all known options, use:

```
dhcp list definedoptions
```

To get help information, enter:

```
dhcp list definedoptions ?
```

To list the definition for option 1 if option 1 is defined, use:

```
dhcp list definedoptions 1
```

To list the definition for all options that are well known *and* have a name starting with 'h', type:

```
dhcp list definedoptions h
```

To define a new option with a code of 128, a minimum number of 1 IP address, and a maximum number of 4 IP addresses, type:

```
dhcp add 128 1 4 ipAddress
```

This information implies that:

- Some DHCP client will know about the option with code 128.
- Option 128 allows IP addresses.
- The server can have a minimum of 1 IP address.
- The server can have up to 4 IP addresses.
- The administrator will still need to set the option value either globally, specific to a subnetwork, or specific to a client.

To delete the definition of the option with code 128, use:

```
dhcp del 128
```

Values for this option that have been set globally, specific to a subnetwork, or specific to a client will NOT be removed. The administrator must remove those values explicitly. Standard option codes CANNOT be changed or deleted.

5. Other Information

DHCP information is kept in the file DHCP.DAT. This file is self-contained. This file contains ALL the DHCP information including:

- Option definitions
- Subnetworks that have been added
- Client lease information
- Option values that have been set

This file can be uploaded/downloaded from one router to another.

Network Address Translation (NAT)

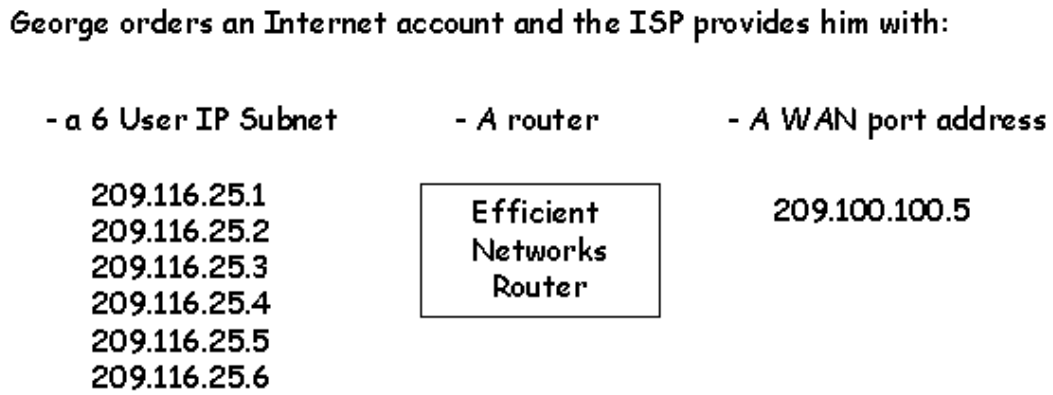
NAT is "Application Aware" of the following programs where IP address/port values *are hidden* in the data payload:

FTP
NETBIOS over IP
RTSP
PPTP
SGI Media-Base
VDO
RealAudio
CU-SeeMe
Quake and Doom

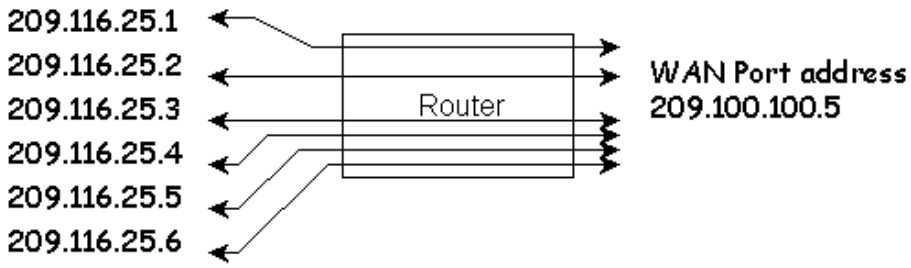
NAT supports TCP or UDP applications where IP address/port values are not buried in the data payload. This includes, but is not limited to:

Telnet
SMTP
HTTP
TFTP
L2TP
Kali gaming
StreamWorks

Routers support two forms of NAT: masquerading (single NAT IP address assigned to many workstations' IP addresses) and classic (one NAT IP address assigned to one workstation's IP address). In the following sections, some general NAT rules and concepts are discussed. The story below should give you an idea of why NAT is valuable.



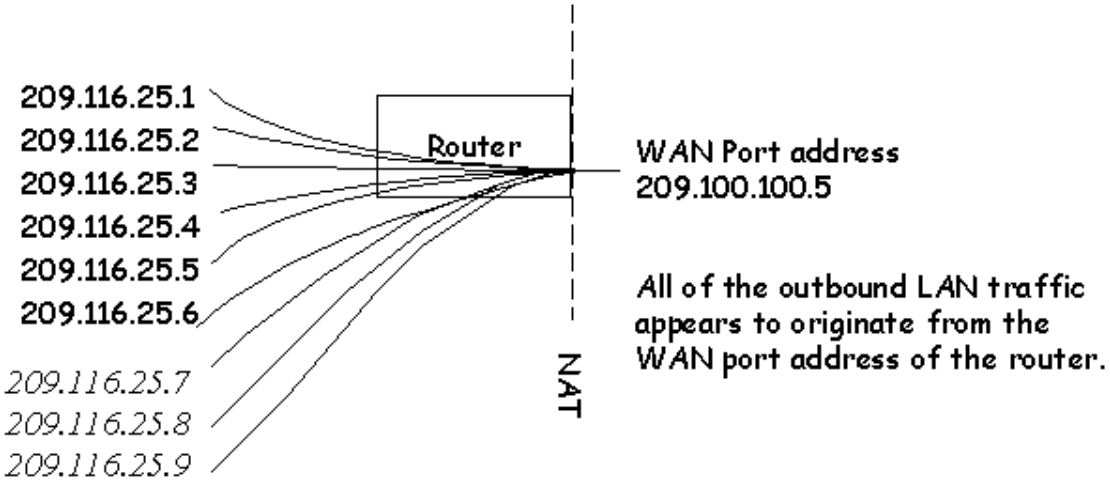
George sets up the router for standard IP routing to the Internet.
Life is good.



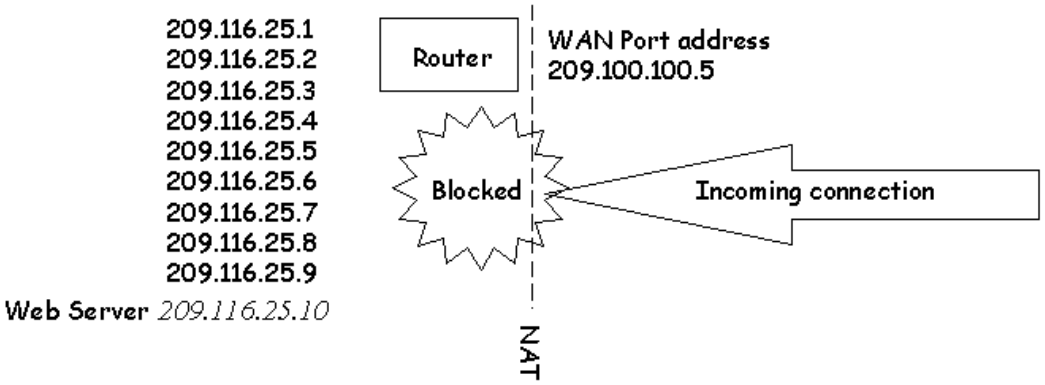
All IP addresses on George's LAN are routed to and from the Internet.

As networking needs expand, George needs to add three more computers to his LAN, but he has used up all of his IP addresses. What to do?

George reads the manual for his router and discovers a feature called "Network Address Translation". Using NAT will allow George to hide all of his workstations behind the WAN port address so it does not matter how many addresses he actually has on the LAN.

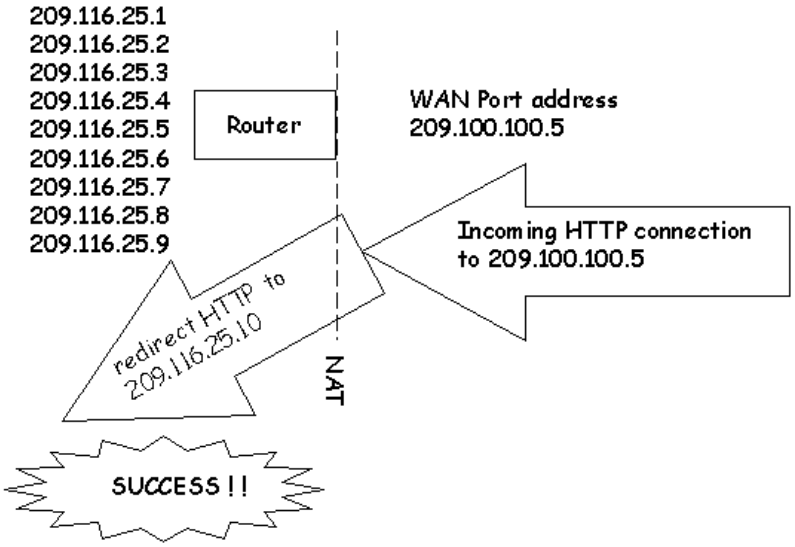


After a while George wants to really take advantage of his Internet connection by *adding a Web Server* on his LAN that can be accessed from the Internet. . . .

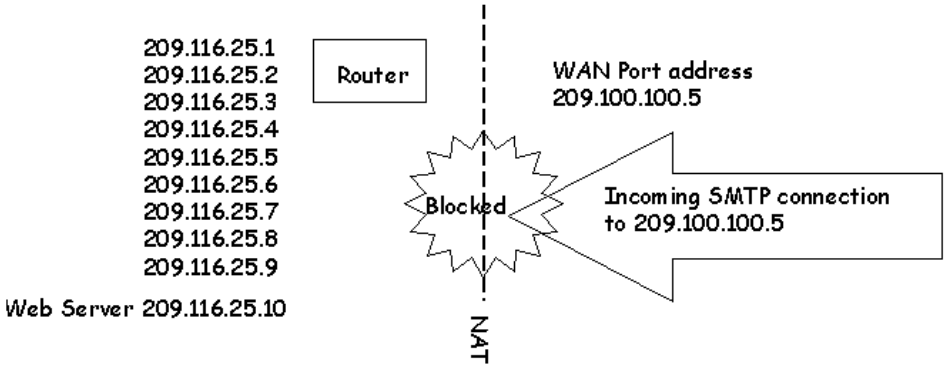


But "IP Masquerading" NAT blocks all incoming connections -- nobody on the Internet can get to George's web server!! George is now back to the documentation looking for more clues...

After a little bit more research, George finds the command for opening up the server to the Internet: `system addserver . . .`

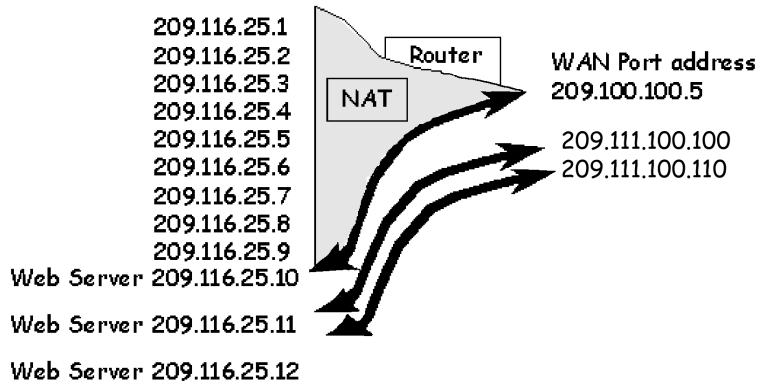


All of the other computers are still protected from incoming connections that are not specifically allowed

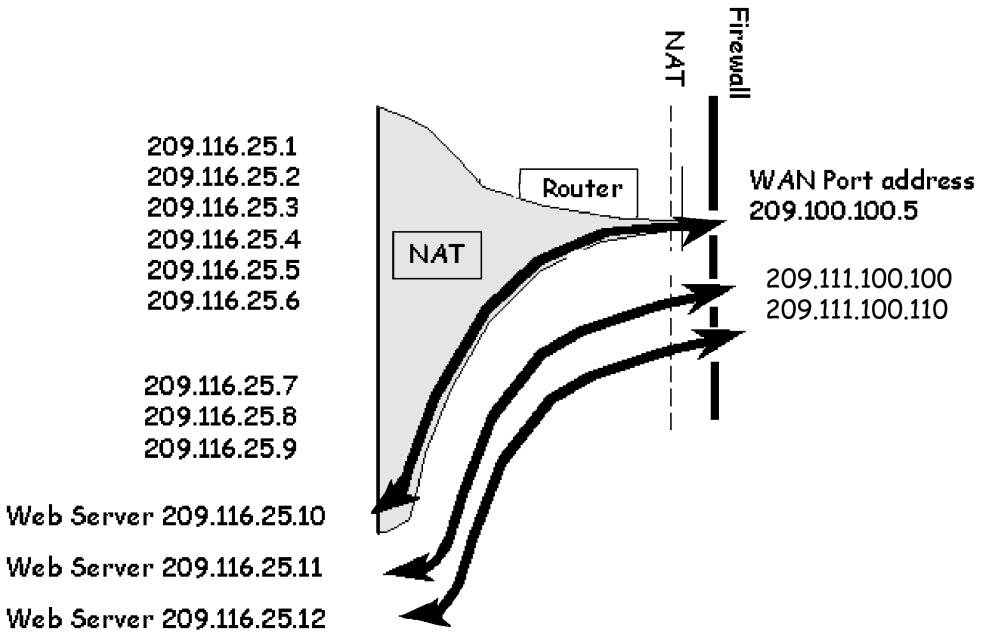


The plot thickens... George is really doing well now and he wants to *add two more web servers* to his network that can be accessed from the Internet. Since there is only one WAN port address, only one web server can be supported through that IP address. BUT... George still has 6 addresses that are being routed to his site from the Internet.... How can he use them?

Additional hosts can be added on the LAN provided they can *borrow* valid routable IP addresses



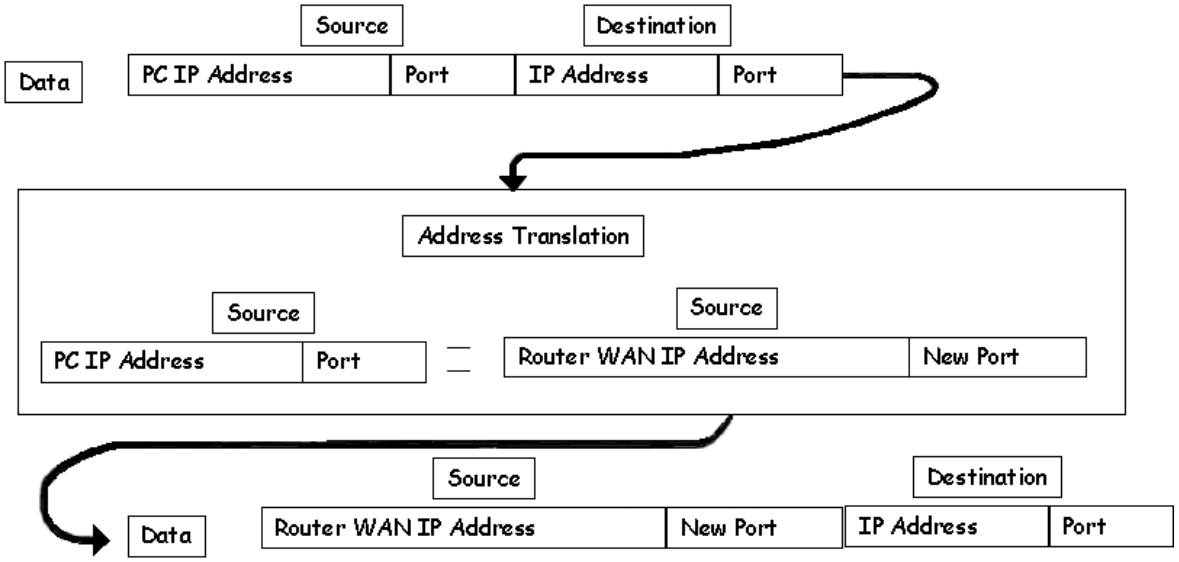
Since the new hosts are completely open to the Internet for incoming connections, it is advisable to install the IP filtering firewall to control access to these servers. NAT is no longer in control of the incoming connections on these devices.



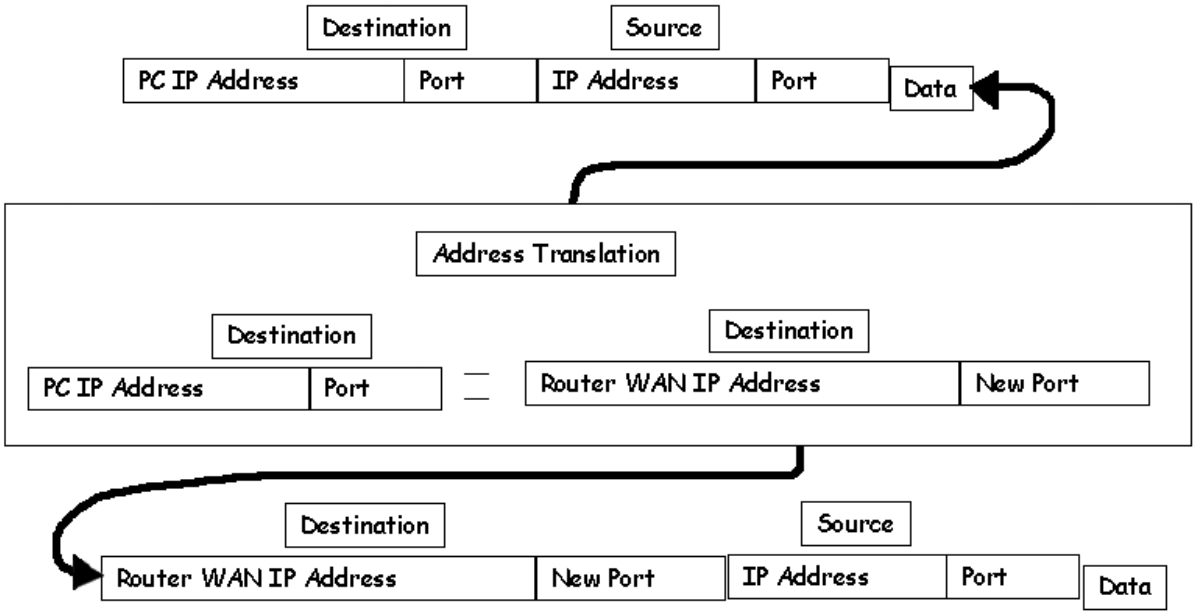
General NAT Rules

- IP Routing must be enabled.
- NAT can be run on a per-remote-router basis.
- Any number of workstations on the LAN may be going to the same or different remote routers at the same time. In reality, the number of workstations on the LAN that can be supported is limited by how much memory the router consumes maintaining table information AND by how many connections are currently active.
- Some operations will NOT work. Specifically, services that place IP address/port information in the data payload MAY NOT WORK until the router examines their packets and figures out what information in the data needs to be changed. Remember that the router is remapping both IP addresses and ports. This can be a cause of failure for some applications such as network games.
- When using NAT with a remote router, either the remote ISP must supply the IP address for NAT translation, or the user must configure the IP address for NAT translation locally.

Outgoing packets with NAT



Incoming packets with NAT



General NAT Concepts

1. The IP address that the router uses to communicate with the ISP is either obtained dynamically (with PPP/IPCP or DHCP) or is statically configured (the commands are given later in this document).
2. NAT servers are either configured globally (**system** commands) or on a per-remote basis (**remote** commands). **System** commands are global and are valid for all WAN traffic. **Remote** commands operate on (or are valid for) one remote profile only.
3. NAT command line parameters require a port value. A port is an identifier used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host. Port numbers in the range of 0 to 1024 are predefined and managed by the Internet Assigned Numbers Authority (IANA), the agency responsible for assigning numbers in the Internet suite of protocols. Some of the most common port numbers are:

24/TCP	Any private mail system
24/UDP	Any private mail system
20/UDP	File Transfer [Default Data]
21/TCP	File Transfer [Control]

   If you do not know which port value to use, contact your network administrator or applications developer.
4. The commands given in the following sections can be issued either via a Telnet session or a Console cable and logging into the router's Terminal Window (found in the Tools section of the Configuration Manager).

Masquerading -- Single NAT IP Address Shared by Many Workstations

With this form of NAT, multiple local (workstation) IP addresses are mapped to a single global IP address. Many local (workstations) IP addresses are therefore hidden behind a single global IP address. The advantage of this type of NAT is that LAN users only need one global IP address, but the entire local LAN can still access the Internet.

Each workstation on the LAN side has an IP address and mask. When connecting to an ISP, the router appears to be a HOST with one IP address and mask. When the workstation connects to the ISP, the IP address used by the workstation is remapped to the IP address assigned to the router. This remapping is done dynamically.

Enabling NAT on your LAN

To enable NAT, use the commands:

```
remote setIPTranslate <on|off> <remoteName>
save
```

Obtain a WAN IP Address for NAT Translation

The IP address (the IP address "known" by the remote ISP) used for this type of NAT translation can be assigned in two ways. If the ISP dynamically assigns the IP address, use the commands:

```
remote setSrcIpAddr 0.0.0.0  0.0.0.0 <remoteName>
save
```

If the ISP assigns a static IP address of ww.xx.yy.zz, use the commands:

```
remote setSrcIpAddr ww.xx.yy.zz  255.255.255.255 <remoteName>
save
```

Server Configuration

This section is intended for users and network administrators who wish to allow WAN access to a webserver, FTP server, SMTP server, etc., on their local LAN, while using NAT. NAT needs a way to identify which local workstation IP address(es) should receive these server requests. As mentioned earlier, the servers can be configured on a per-remote-router basis as well as globally.

To enable redirections that are valid only for specified remote routers, use the remote commands. To enable redirections that are valid for all remote routers (globally), use the system commands.

Remote Commands

The following commands are used to enable/disable a local IP address (on your LAN) as the server for a particular protocol for the remote router <remoteName>. This is a valid redirection *only* for the <RemoteName> connection.

```
remote addServer <ipaddr> <protocol> <port> <remoteName>
remote delServer <ipaddr> <protocol> <port> <remoteName>
```

This command is used to view all of the remote entries, including the changes:

```
remote list
```

Remember to type `save` *to make the changes persistent across boots.*

Example 1:

Assume that the local LAN network is 192.168.1.0 255.255.255.0. The following commands are used to enable the Telnet server on the local LAN with the IP address 192.168.1.3, and an FTP server with the IP address 192.168.1.2.

```
remote addServer 192.168.1.3  tcp telnet router1
remote addServer 192.168.1.2  tcp FTP router1
```

When receiving a request from *router1* to communicate with the local Telnet server, the local router will send the request to 192.168.1.3. If *router1* asks to talk to the local FTP server, the local router will send the request to 192.168.1.2.

Example 2:

Assume that the local LAN network is 192.168.1.0 255.255.255.0. When the port value of 0 (zero) is used, it directs all ports of the specified protocol to the IP address specified.

```
remote addServer 192.168.1.4  tcp 0 router1
```

Note: AddServer commands using specific port numbers take priority over the port #0 setting. 192.168.1.4 will be asked to serve requests coming from router1 to the local router. If the local router also has the same Telnet and FTP entries as in the previous example, 192.168.1.3 will serve the Telnet request, 192.168.1.2 will serve the FTP request, and 192.168.1.4 will serve any other request, including HTTP, SMTP, etc.

System Commands

The following two commands are used to globally enable/disable a local IP address (on your LAN) as the server for that particular protocol.

```
remote addServer <ipaddr> <protocol> <port>
remote delServer <ipaddr> <protocol> <port>
```

This command is used to view all of the global system entries, including the changes:

```
system list
system addServer 192.168.1.5  tcp  SMTP
system addServer 192.168.1.6  tcp  0
system addServer 192.168.1.6  udo  0
```

The router sends a server request for SMTP to 192.168.1.5 when such a request comes from any remote router running NAT. The router sends any other server request (tcp or udp) to 192.168.1.6.

Keep in mind that the `remote addServer` command only affects the specified remote router, while `system addServer command` will affect all devices connected to the router.

Note: Remember to type `save` *to make the changes persistent across boots.*

Server Request Hierarchy

When handling a request from a remote router (to which the local router has NAT enabled), the local router selects a server with the following priority:

remote addServer – The local router selects a server for the remote router that handles that particular protocol/port.
system addServer – The local router selects a global server that handles that particular protocol/port.
remote addServer with port 0 – The local router selects a global server that handles that particular protocol (tcp/udp) and ANY port
system addServer with port 0 – The local router selects a global server that handles that particular protocol and ANY port.
router IP address – The local router elects itself (the local router) as the server.

Setting up a Local HTTP or Mail Server with NAT

This is possible if the ISP statically or dynamically assigns the *same* IP address and mask every time. Users who wish to communicate with the server need to have an IP address that remains constant.

You can configure an HTTP server by issuing the following commands to the router:

```
system addserver 192.168.100.3 tcp smtp
save
```

This tells NAT to send any SMTP client requests from the WAN to 192.168.100.3 on the LAN. Only SMTP connections will be directed by this command.

Classic NAT (one NAT IP address assigned per one workstation IP address)

With classic NAT, one workstation IP address is translated to one NAT IP address. This NAT technique is primarily used to make certain hosts on a private LAN globally visible and give them the ability to remap these IP addresses as well. Classic NAT requires that you first enable NAT masquerading as described in an earlier section.

Host Remapping

As with the previous implementation of NAT, the commands are either used per remote (**remote** commands) or globally (**system** commands).

Remote Commands

Use the remote `addHostMapping` command when a host on the local LAN is known by different IP addresses to different remote routers. Use these commands to enable or disable host remapping on a per-remote-basis:

```
remote addHostMapping <first private addr> <second private addr>
<first public addr> <remoteName>
remote delHostMapping <first private addr> <second private addr>
<first public addr> <remoteName>
```

System Commands

Use the system **addHostMapping** command when a host on the local LAN is known by the same IP address on all remote routers. Use these commands to enable or disable host remapping globally:

```
system addHostMapping <first private addr> <second private addr>
<first public addr>
system delHostMapping <first private addr> <second private addr>
<first public addr>
```

IP Address Range

The range of local LAN IP addresses to be remapped is defined by <first public addr> to <first public addr> inclusive. These addresses are mapped one to one to the public addresses.

The range of public IP addresses is defined by <first public addr> only. The rest of the range is computed automatically, equaling the same number as assigned in the private address range (from <first public addr> to <first public address> + the number of addresses remapped – 1) inclusive.

Multiple Host Remapping Entries

Users may have as many host-remapping entries as they wish.

Examples:

```
remote addHostMapping 192.168.207.40  192.168.207.49  10.0.20.11
<remoteName>
remote addHostMapping 192.168.207.93  192.168.207.99  10.0.20.4
<remoteName>
remote addHostMapping 192.168.209.80  192.168.207.49  10.12.14.16
<remoteName>
```

The above entries create three mappings:

```
192.168.207.40 through 192.168.207.49 are mapped to 10.0.20.11
through 10.0.20.20
192.168.207.93 through 192.168.207.99 are mapped to 10.0.20.4
through 10.0.20.10
192.168.209.71 through 192.168.209.80 are mapped to 10.12.14.16
through 10.12.14.25
```

Range Overlap Rules

With remote addHostMapping, private IP address ranges cannot overlap for a remote router.
With remote addHostMapping, public IP address ranges cannot overlap for a remote router.
With system addHostMapping, private IP address ranges cannot overlap for a system.
With system addHostMapping, public IP address ranges cannot overlap for a system.

If a private IP address range for a remote router and a private IP address range for the system overlap, the private IP address range for the remote has precedence. If a public IP address range for a remote and the public IP address range for the system overlap, the public IP address range for the remote has precedence.

Private IP addresses and public IP addresses can be the same. For example, to enable IP/port translation to a remote router and make the IP addresses 10.1.1.7 through 10.1.1.10 globally visible, it is permissible to use either one of the following commands:

```
remote addHostMapping 10.1.1.7  10.1.1.10  10.1.1.7 <remoteName>
system addHostMapping 10.1.1.7  10.1.1.10  10.1.1.7
```

If the host's remapped IP address (classic NAT, one-to-one IP address translation) and the "masquerading" IP address (many-to-one IP address translation) are the same, then NAT masquerading has precedence over classic NAT.

Customizing NAT for Specific Applications

PPTP (Point-to-Point Tunneling Protocol) uses the protocol GRE, represented by the number 47, and any unassigned port during the authentication phase. A tunnel is then established with the protocol TCP and port 1723. The following commands will allow a client on the Internet to establish a connection to a PPTP server on a LAN behind a router using NAT.

```
system addserver <PPTP server IP address> tcp 1723
system addserver <PPTP server IP address> 47 0
```

PCanywhere uses protocols TCP and UDP with ports 5631 and 5632. The following commands allow a user on the Internet to connect with a workstation on the LAN. The server commands are required to have a unique port and protocol profile for every entry. This restricts PCanywhere users to the limit of one workstation on the LAN that can be accessed from the Internet.

```
system addserver <LAN workstation IP address> tcp 5631
system addserver <LAN workstation IP address> udp 5632
```

CU-SeeMe uses the following protocols and ports in what is called "CU-SeeMe mode".

```
system addserver <LAN workstation IP address> tcp 7648
system addserver <LAN workstation IP address> tcp 1503
system addserver <LAN workstation IP address> udp 7648
system addserver <LAN workstation IP address> udp 24032
```

CU-SeeMe uses the following protocols and ports for "H.323 mode" that allows voice traffic.

```
system addserver <LAN workstation IP address> tcp 7648
system addserver <LAN workstation IP address> tcp 1720
system addserver <LAN workstation IP address> tcp 1503
```

Note: Efficient Networks has not tested CU-SeeMe server commands. If you have success with these or other server commands for popular applications, please relay that information to us so that we can add it to this guide.

NAT Frequently Asked Questions

1. Can I access the webserver on my LAN from the Internet when I am using NAT?

Yes, however, you must set up server mapping in the router so that it will know that a LAN HTTP server should be made available to the WAN.

2. Can two PCs on my LAN access the same site on the Internet at the same time?

Yes. Since the router manages TCP connections as well as IP addresses, it can differentiate between two different PCs, even if they are targeting the same destination.

3. How many PCs will the router support with NAT?

The translation table uses "connections" as its reference points instead of IP addresses. Each PC can have multiple connections at the same time. Each of these connections times out if it is not used in a certain period. The address translation table can accommodate up to 1500 simultaneous connections. Only active connections are maintained.

4. How does the router manage all of the translations?

Each connection that is established by a workstation on the LAN is recorded in the translation table. The destination IP address, protocol type, and port number are noted. Additionally, the source IP address, protocol type, and port are noted. The packet goes through the translation table, the source IP address is replaced with the routers WAN port address, the protocol type is maintained, and the port address is changed. The port number that is used in the source information is the table "key" for finding the proper mapping when a response is received. Each connection gets its own port number for mapping purposes.

5. What types of services can I make available to the WAN through NAT?

All types of services can be made available to the WAN through NAT. The router is sensitive to three protocol types: TCP, UDP, and ICMP. The router is also sensitive to the port number used on the inbound connection. All standard services have "assigned numbers" for the port values. For example, SMTP mail is on TCP port 25, FTP is usually port 21, Telnet is usually TCP port 23, POP3 is usually at TCP port 110, and HTTP is usually port 80, etc.

6. Can I still manage the router from the WAN when NAT is enabled?

Yes. If you wish to manage the router with SNMP or Telnet from the WAN, you may since the router traps those services. But if there is a server mapping those services to a device on the LAN, then the router will not be able to trap them, and management is not possible.

7. Can I Telnet through NAT to a LAN device and still manage the router with Telnet?

Yes. You can reassign the Telnet port on the router to another port, and manage the router using that new Telnet port. Then all other Telnet connections are directed to the workstation on the LAN that you map.

To redirect incoming Telnet sessions on port 23 to the workstation that is identified:

```
rem addserver <workstation ip address> tcp telnet internet
```

To change the router's Telnet port to 2001:

```
system telnetport 2001
```

Another method is to leave the router at Telnet port 23 and re-map incoming connections on an unprivileged port to the workstation on port 23:

```
rem addserver <workstation ip address) tcp 2001 2001 23 internet
```

8. How do I get PPTP to work with NAT?

The router software must be above 2.5.2. Enter the following commands:

```
system addserver x.x.x.x tcp 1723
system addserver x.x.x.x 47 0
```

9. How does the router manage all of the LAN's translation?

Each connection that is established by a workstation on the LAN is recorded in the translation table. The destination IP address, protocol type, and port number are noted. Additionally, the source IP address, protocol type, and port are noted. When the packet goes through the translation table, the source IP address is replaced with the routers WAN port address, the protocol type is maintained, and the port address is changed. The port number that is used in the source information is the table "key" for finding the proper mapping when a response is received. Each connection gets its own port number for mapping purposes.

There are two options for LAN servers when NAT is enabled:

Option 1. Redirect packets of a specific profile sent to the router address:

```
system addserver <LAN IP address of server> <protocol> <port>

system addserver x.x.x.x tcp 110

system addserver x.x.x.x tcp smtp

system addserver x.x.x.x tcp http

system addserver x.x.x.x tcp ftp
```

The protocol field may contain TCP, UDP or any protocol number. The port field may contain FTP, Telnet, SMTP, HTTP, SNMP or any port number. The port number 0 will open all ports.

Option 2. Map a public address other than the router's to a private LAN address.

```
system addhostmapping <1st private addr> <last private addr>
<1st public addr>

system addhostmapping 192.168.254.200 192.168.254.200
209.209.209.209

system addhostmapping 192.168.254.200 192.168.254.205
209.209.209.209
```

The first example would map 192.168.254.200 to 209.209.209.209.

The second example would map (.200 to .209), (.201 to .210), (.202 to .211), (.203 to .212), (.204 to .213), and (.205 to .214).

10. How can server commands support multiple webservers?

Since the router will not let you duplicate protocol and port profiles, you may type the following to support multiple servers of the same type:

```
system addserver 192.168.254.2 tcp 80

system addserver 192.168.254.3 tcp 2048

system addserver 192.168.254.4 tcp 2049

system addserver 192.168.254.5 tcp 2050

system addserver 192.168.254.6 tcp 2051

system addserver 192.168.254.7 tcp 2052
```

The above commands will forward any packets that meet a profile port and protocol to the webserver's local IP address.

To allow an HTTP request to enter the router using the private port and be redirected to the local server on port 80, you must set the range of public ports as 1 and the internal port as 80:

```
system addserver

<LAN IP addr of server> <protocol> <1st port> [last port]
[private port]
```

```
system addserver 192.168.254.2 tcp 80
system addserver 192.168.254.3 tcp 2048 2048 80
system addserver 192.168.254.4 tcp 2049 2049 80
system addserver 192.168.254.5 tcp 2050 2050 80
system addserver 192.168.254.6 tcp 2051 2051 80
system addserver 192.168.254.7 tcp 2052 2052 80
```

WAN Protocols

Efficient Network routers support PPP, RFC 1483 SNAP, and RFC 1483 MER link protocols.

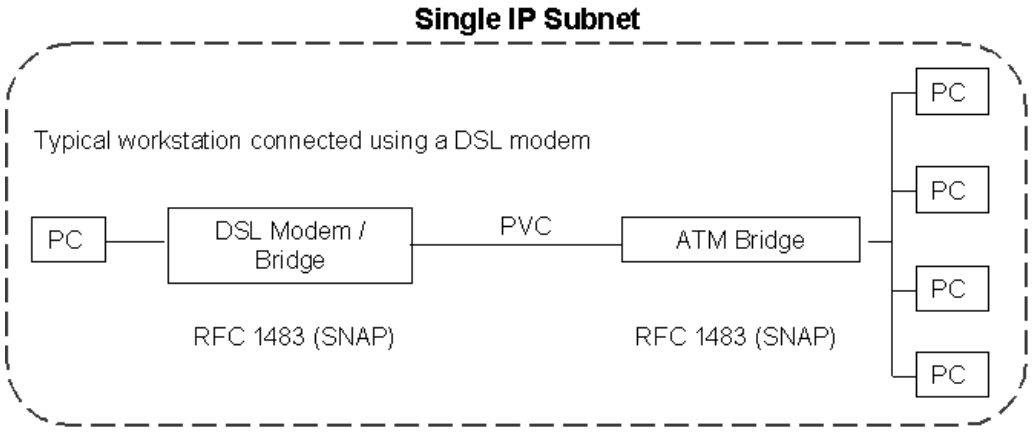
PPP (Point–to-Point Protocol) enables TCP/IP traffic to be carried over an ATM network without being translated, however, each workstation that links with a DSL bridge or router requires an ATM adapter card.

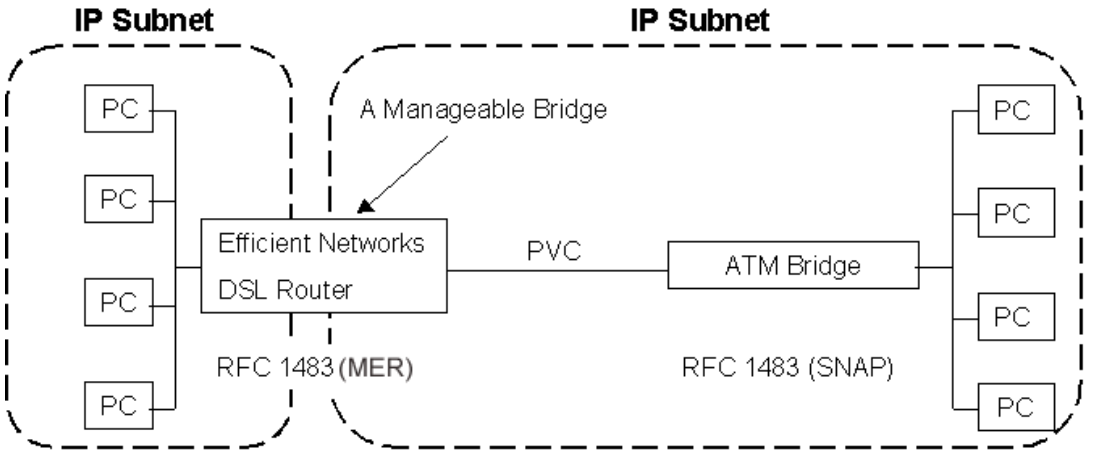
When **RFC 1483 SNAP** is used as the WAN protocol on an ATM PVC, each peer must have the same encapsulation settings. If the settings vary, then one peer is sending ATM cells with the wrong type of header for the receiver, so the signals are lost.

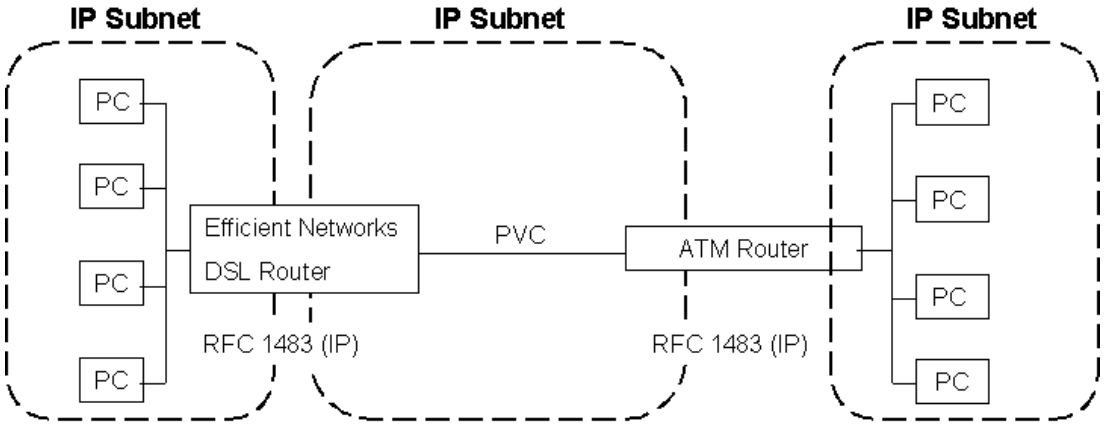
When **RFC 1483 MER** (MAC Encapsulated Routing) is enabled on a router, it allows configuration of an ATM Access Concentrator for both modem and router deployment since it supports bridge encapsulation as well as IP encapsulation. ATM cells are encapsulated with an IP address header when routing; ATM cells are encapsulated with a MAC address header when bridging. If IP routing is enabled, then IP packets are prepended with the sequence 0xAAAA0300 0x80c20007 0x0000 and sent as bridged frames.

What all this techno-speak means is that RFC 1483 MER allows you to do IP routing with NAT on the LAN side of the CPE router and bridging on the WAN side. And when NAT and MER are enabled on the CPE router, a customer network of many workstations will appear the same as a single workstation behind a modem.

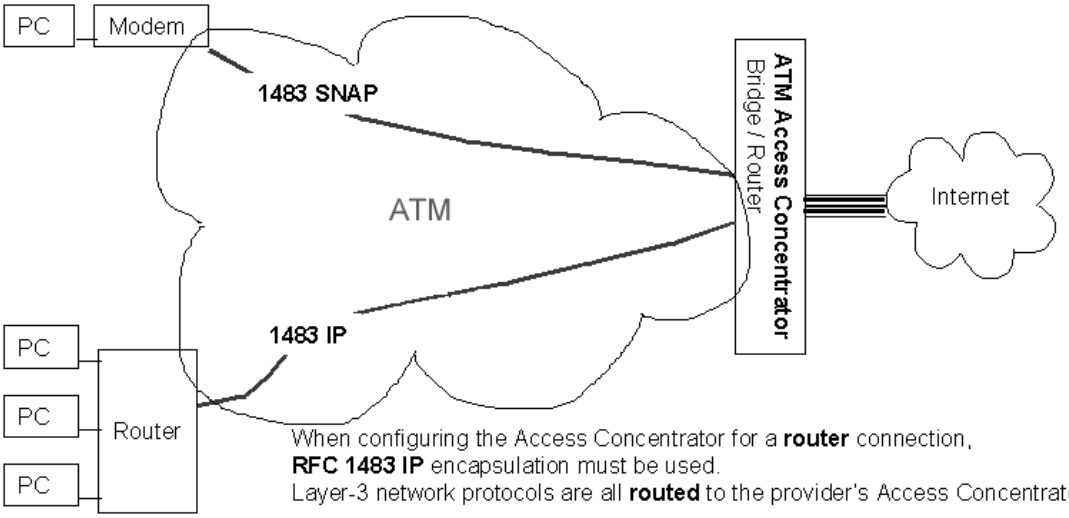
The following diagrams show the relationships of CPE, ATM hardware, and subnets.



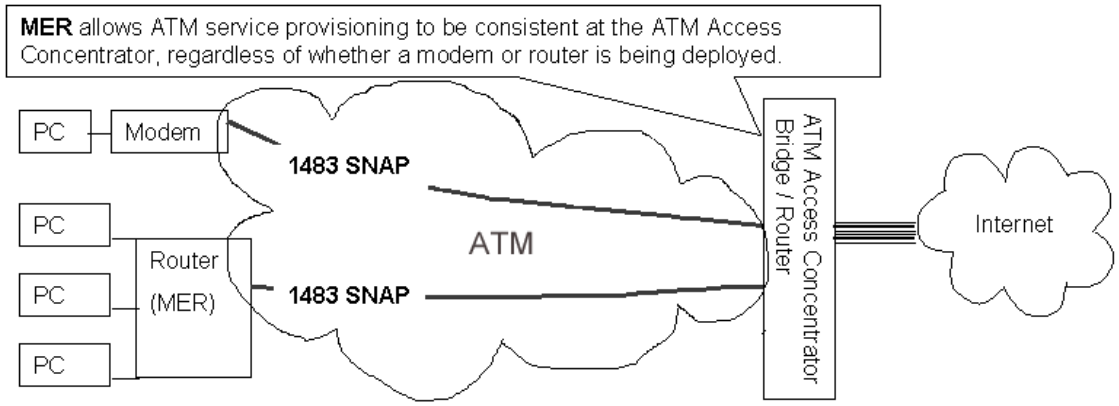




When configuring the Access Concentrator for a **modem (bridge)** connection,
RFC 1483 SNAP encapsulation must be used.
Layer-3 network protocols are all **bridged** to the provider's Access Concentrator.



When configuring the Access Concentrator for a **router** connection,
RFC 1483 IP encapsulation must be used.
Layer-3 network protocols are all **routed** to the provider's Access Concentrator.



When configuring the Access Concentrator for a **router** connection, **RFC 1483 SNAP** encapsulation may be used by enabling **MAC Encapsulated Routing (MER)** on the customer premise router. Layer-3 network protocols are all **routed** to the provider's Access Concentrator even though they are configured to use bridged encapsulation.

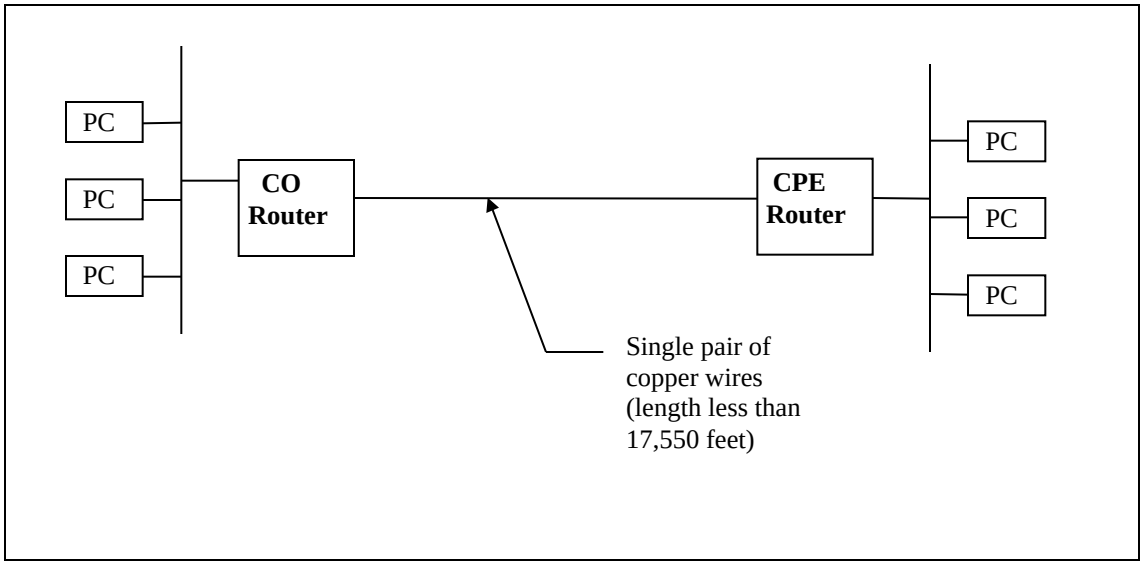
To configure a router for MER, Telnet to it, login, then enter commands – they *must* be entered in the order presented below:

```
remote deliproute 0.0.0.0 255.255.255.255 <remote name>
```
(deletes old default route)
```
remote disbridge <remote name>
```
(disable bridging)
```
eth ip ena
```
(enable ip routing)
```
remote setproto mer <remote name>
```
(enable MER protocol)
```
remote addiproute 0.0.0.0 255.255.255.255 1 209.31.225.1 <remote name>
```
(new default route)
```
remote setiptranslate on <remote name>
```
(enable NAT)
```
remote setsrcipaddr 209.31.225.8 255.255.255.0 <remote name>
```
(set source IP addr)
```
eth ip addr 192.168.254.254 255.255.255.0
```
(set router Ethernet addr)
```
dhcp enable 192.168.254.0
```
(enable dhcp)
```
save
```
(stores new configuration)
```
reboot
```
(activates new configuration)

Router Pair Point-to-Point Setup

Two identical routers are used in a "point-to-point" configuration. Each router is configured according to local network needs. The following instructions and scripts are provided to assist you in getting a point-to-point installation up and running in just a few easy steps.

Connecting two 10Base-T LANs using a single pair of copper wires



One of the point-to-point routers must be the master controller for the clocking of DSL traffic. The controller is referred to as the "Central Office" or "CO" router. The peer router ("Customer Premises Equipment" or "CPE") will look to the controller for clock synchronization. In this process, we will configure the CO router first, then we will configure the CPE router.

Configuring the First Router (Central Office)

STEP 1:

Connect the cables.

STEP 2:

Designate the first one of your routers as "CO" by placing an identifying mark or sticker indicating "CO" on it.

STEP 3:

Install Quick Start software on the PC connected to the CO router.
Follow the on-screen instructions to install the software.
Select NO when asked if you want to run the Quick Start program (you will be prompted to run this program later).

STEP 4:

Open the README.TXT file contained in the directory where the Quick Start software is installed (default directory is "C:\DSL").
Locate the appropriate script for your type of installation. The scripts can be found in Section I under the heading "Sample Configurations". There are two pairs of scripts. One is for IP routing (CO/CPE router for IP/PPP, no NAT) and the other is for Bridging (CO/CPE device for RFC 1483/Bridging).
Copy the appropriate script to a new text file called COSCRIPT.TXT. Save it in the directory where the Quick Start software is installed.
To modify the standard script, just edit the "C:\DSL\COSCRIPT.TXT file before moving on to Step 5. The only items you might want to change are the Ethernet IP address/mask and the default route. All of the other settings should remain the same.

Sample Script

```
sys name co
```
(Name the router --optional)
```
sd term co
```
(Set this router as the Central Office)
```
sd speed 1152
```
(Set the line speed to maximum capability)
```
eth ip addr 192.168.1.254 255.255.255.0
```
(Set the Ethernet port IP address and mask)
```
eth ip enable
```
(Enable IP routing)
```
rem add cpe
```
(Add a routing profile for the peer router)
```
rem setproto ppp cpe
```
(Set the WAN protocol to PPP)
```
rem setpvc 0*38 cpe
```
(Set the VPI/VCI)
```
rem disauthen cpe
```
(Disable authentication)
```
rem addiproute 0.0.0.0 255.255.255.255 1 cpe
```
(Add a default IP route to the peer router)
```
save
```
(Save the settings)
```
reboot
```
(Reboot the router)

STEP 5:

Start the Quick Start program on your computer.

If you are running Quick Start for the first time, you will be asked if you have been supplied with an installation script. Click **YES** and select the C:\DSL\COSCRIPT.TXT file that you created in Step 4. To execute a script, select the **Tools** menu, then select **Execute A Script**.

Configuring the Second Router (Customer Premises)

STEP 1:

Connect all but the DSL cables (you will attach the DSL cable after the CPE router has been configured).

STEP 2:

Designate the first one of your routers as "CPE" by placing an identifying mark or sticker indicating "CPE" on it.

STEP 3:

Install Quick Start software on the PC connected to the router.
Follow the on-screen instructions to install the software.
Select NO when asked if you want to run the Quick Start program (you will be prompted to run this program later)

STEP 4:

Open the README.TXT file contained in the directory where the Quick Start software is installed.
Copy the appropriate script to a new text file called CPESCRIPT.TXT. Save it in the directory where the Quick Start software is installed.
To modify the standard script, just edit the "C:\DSL\CPESCRIPT.TXT file before moving on to Step 5.

STEP 5:

Start the Quick Start program on your computer.
If you are running Quick Start for the first time, you will be asked if you have been supplied with an installation script. Click **YES** and select the C:\DSL\CPESCRIPT.TXT file that you created in Step 4.
If this is not your first time running Quick Start, you will not be prompted for a script. To execute a script, select the **Tools** menu, then select **Execute A Script**.

STEP 6:

Connect the DSL cable from the wall jack to the DSL port on the back of the router.

STEP 7:

To verify that the DSL link is up, watch the router lights as it executes the script and reboots.

If the lights are not in a "ready" state (see p. 6 of this guide) within a minute, check the loop length chart below to see if you might need to use a lower speed setting. If so, then you need to change the speed setting on the CO router. To make this change, Telnet to the router's Ethernet IP address and type the following commands:

```
sd speed 384
save
reboot
```

Once this setting is made on the CO router, the CPE router will automatically attempt to match the speed setting of the CO router. For more information on speed settings, see the README.TXT file.

Loop Length

DSL uses two wires connected from one point to another to transmit/receive data at high rates. These two wires must be free from repeaters and bridge taps, and in the case of SDSL, no further than 19,300 feet (5938 meters) from the Access Concentrator.

SDSL Speed and Loop Lengths

Kbps	Meters	Feet
2320	2492	8,100
1744	3092	10,050
1536	3261	10,600
1152	3846	12,500
768	4215	13,700
384	4800	15,600
192	5938	19,300

Firewall

Firewall software is embedded in the kernel of newer routers (software releases above 3.0.1).

First line of defense -- NAT
NAT (IP masquerading) allows all of the workstations on the LAN to be hidden behind a single public address so that incoming connections can be blocked. It can provide a level of "security by obscurity" that is acceptable for many users since it can block LAN access to casual hackers. However, a determined hacker is likely to gain access to LAN services behind NAT.

Second line of defense -- IP Filtering
Firewall software provides the ability to specifically protect some services on the LAN while providing external access to other services. It provides a highly flexible means by which to control exactly which network traffic will be allowed into or out of your LAN and which traffic should be denied. It will protect against Denial of Service attacks and log suspicious activities. It can also be used to keep certain users on the LAN from accessing the Internet. And it can be used in conjunction with NAT, so you don't have to change an existing configuration to add more security.

Since a router can support multiple PVCs over the same DSL line, there are actually *virtual* interfaces separate from physical interfaces. One virtual WAN interface might go to the Internet and another virtual interface might go to a Corporate LAN, but both of these are carried over the same physical WAN interface. So, in addition to applying a single filter on a physical interface, filters should be created for each virtual interface.

Firewall Software Features

- A filter set can be built for each IP interface (physical or virtual PVC)
- Existing filter sets can be displayed
- New filters can be easily inserted into existing filter sets
- Test packets can be generated to test filter sets
- Previous configuration can be restored in the event that a new configuration is in error
- Up to 30 complex filters possible using AND / OR logic
- Input, Output, and Forward filters on each interface

IP filtering will allow and deny IP packets on each IP interface based on:

Direction of traffic
Protocol (TCP, UDP, ICMP, or protocol number)
Source IP address and port
Destination IP address and port
SYN and ACK flags

Local and Remote Management Ease of Use

A firewall can be configured and managed from the LAN or WAN with ease. Once a filter is added, it takes effect immediately and can be tested. If the filter is acceptable, then it can be saved permanently. Otherwise, it can be easily removed and the old configuration restored.

A firewall is easy to set up because its function is transparent upon initial installation, that is, it can be installed on a functioning router without any interruption of activity. As the filters are configured and tested, they can be brought on line one at a time.

When configuring the firewall remotely, there are certain key features that make life easier. Since all filters take effect immediately, they can be tested on the fly. If a filter is added and remote management goes away or the testing of that filter reveals that it was incorrect, then it can be easily taken back to the last acceptable configuration. In the event that remote management gets blocked due to an incorrect filter addition, a simple power cycle of the router will restore the last saved configuration. So keep in mind that filters will become active before they are saved, but they need to be saved by a command line to be permanent.

Filter Scripting

Efficient Networks provides standard configuration scripts that protect against the most common LAN attacks. You can also create custom scripts and load them from the LAN or WAN to one or more routers. You may even want to copy existing filters from one router and use them as a script on other routers.

It's possible to use several "generic" scripts in succession to build a custom configuration. For example, you might create one script containing Denial of Service filters, another script containing information to open up a webserver, another one with mailserver allowances, etc. Simply running these scripts together can create a complex filter set.

Logging

Logging can be turned on so that all denied packets are reported. This is useful when the firewall is preventing certain applications from operating properly or there is suspicious network activity. You can look at real-time drops of packets as they occur or review counter totals on how many times an interface filter caused a *deny* action on certain days or weeks. By watching the log, it becomes clear which filters are essential and which need to be removed in order to allow network applications to run properly.

Testing

You can quickly determine if your firewall is doing what you want it to do without waiting for an attack. Test packets can be generated to simulate attacks from the LAN or WAN side of the router. This gives you the ability to discover possible security breaches that may not have been obvious.

Troubleshooting

If a particular application is not working, you can locate the problem by turning on the `watch` feature and looking for the packets being dropped as the application is being run. Once the

packet is identified, it can be copied into the `allow` filter to remove the restriction that was causing the application to fail.

Another handy troubleshooting tool is the `test` feature. This will generate a packet that will offend the filter and you can observe whether it gets through or not. You can define the test packet with the same granularity as the filter rules -- source and destination IP address and port values, protocol type, SYN flag and/or ACK flag. And all of these tests can be performed locally or remotely.

Rule Structure

An IP filter "rule " has the following structure:

<command> <type> <action> <parameters>[port]

Command options are detailed below.

command = append, insert, delete, clear, flush, check, list, watch on|off

type = input, output, forward

action = accept, drop, reject

parameters

-*p* = protocol
-*sa* = source address
-*sm* = source mask
-*sp* = source port
-*da* = destination address
-*dm* = destination mask
-*dp* = destination port
-*b* = swap source and destination
-*c* = count
-*tcp* = syn|ack|noflag
-*q* = quiet rule
-*v* = verbose rule

port = 0 or 1 (used on Ethernet to Ethernet routers only)

Other IP Filtering Requirements

1. **IP filtering REQUIRES IP routing to be enabled** (`eth ip enable`). Bridge configurations will require a change to the MER protocol to allow IP filtering.

2. **IP filters can be placed on the Ethernet (LAN) interface, and/or the remote (WAN) interface.** Commands vary by interface.

   LAN vs. WAN Syntax:

   `eth ip filter <rule>` = LAN Interface

   `rem ipfilter <rule> <rem name> =` WAN Interface

   Dual Ethernet vs. DSL Routers:

   Dual Ethernet routers must identify the interface with either a 0 or 1 in the "port" portion of the command.

   DSL routers do not need to use the "port" portion of the command.

   Inbound vs. Outbound Packets:

   `eth ip filter input` = LAN to router

   `eth ip filter output` = router to LAN

   `remote ipfilter output` = router to WAN

   `remote ipfilter input` = WAN to router

3. **The COMMAND portion of the filtering command has 8 options. Those options are append, insert, delete, clear, flush, check, list, watch.** You should know the following:

   `insert` places a rule at the start of the list.

   `append` places a rule at the end of the list.

   Packets are filtered through the list from start to end.

   A rule may be placed in any place on the list using the `insert` command with a line number as viewed on the list command, between the term insert and input or output.

A rule may be deleted from any place on the list.

The entire list or any rule matching the parameters is lost when the flush command is used.

`clear` is used on one interface to reset the counters using the following syntax `eth ip fil clear count 1.`

4. **IP filtering through these routers is stateless.** All rules are static, they are not capable of taking action based on the condition of the connection. You may configure a rule based on the SYN and/or ACK flags of TCP packets.

5. **IP filtering works seamlessly with NAT.** Consideration must be given to the correct address at the time the filter is applied as NAT will change the IP address during translation.

   IP filtering with NAT is applied in the following manner:

   Input Phase - When an IP packet comes in through the Input interface, the router tries to recognize the packet. The router then examines the Input filters for this interface, and based on the first Input filter that matches the IP packet, it decides how to handle the packet (accept, drop or reject it). If NAT is enabled for the Input interface, NAT translation is performed, changing the destination IP address.

   Forward Phase - At this stage, the router determines to which interface packets will be sent out using its routing table; it then applies the Forward filters based on the Input interface information. Forward filters based on the Output interface information are applied next.

   Output Phase - If NAT translation is enabled for the Output interface, then NAT translation is performed changing the source IP address. The router examines the Output filters for this interface, and based on the first Output filter that matches the IP packet, it decides how to handle the packet.

6. **The firewall default action is to accept all packets.** If an incoming IP packet does not match any rule, it is accepted.

   To change the default action to deny all packets, you may enter the following rule:

   ```
   append input drop
   append output drop
   ```

   This will reject all packets until you build rules that allow certain types of packets into your network.

NOTE: Be aware that the "deny" rules that you create determine how many "accept" rules will need to be created. For every "remote append input drop" rule, there will be a list of "remote insert input accept" rules. Since there can be 5 drop filters (rem, eth, input, output, forward), there can be five similar lists of accept rules.

7. **The firewall needs to address packets in both directions.** It may be easier to build your rules for each application as a pair -- one rule for the input, the next for the output -- then move on to the next application.

Sample IP Filtering Scripts

LAN Interface

```
eth ip filter
command
type
action
parameters
port 0 | 1
```

WAN Interface

```
remote ip filter
command
type
action
parameters
remote name
```

Commands that are the same for LAN and WAN:

`append`	Append a filter to the end of a type
`insert`	Insert a filter at the front of this type
`delete`	Delete the first filter matching this filter
`flush`	Delete all filters of this type
`check`	Check action to take based on parameters
`list`	List all filters of a type
`watch`	On | Off
`-P`	TCP | UDP | ICMP | protocol #
`-SA`	Source Address 0.0.0.0:255.255.255.255
`-SM`	Source Mask 255.255.255.255
`-SP`	Source Port 0:0xffff 65535
`-DA`	Destination Address Same as Source
`-DM`	Destination Mask, Same as source
`-DP`	Destination Port, Same as source
`-TCP`	`SYN | ACK | NOFLAG`

Flush

The following script will allow you to flush all existing filters before building a new set of rules.

```
eth ip filter flush forward

eth ip filter flush input

eth ip filter flush output

remote ipfilter flush forward <remote name>

remote ipfilter flush input <remote name>

remote ipfilter flush output <remote name>
```

Denying Packets from Internet

The following script will deny all packets from both the WAN and the LAN. These should be the first rules that are entered. These drop filters will force you to create a list of accept rules for both the input and output. Without a deny rule, all packets will be accepted.

```
remote ipfilter append input drop <remote name>

remote ipfilter append output drop <remote name>
```

Note: All other examples in this document will be based on drop filters. If you chose to enter drop rules using the Ethernet or forward filters, you will have to add an appropriate list of Ethernet and forward accept rules.

Allow ICMP Replies and Errors

The following example will allow the router to send and reply to a ping from the Internet. The first rule will allow any ICMP packet from the LAN. The other rules allow ping, ICMP style trace-route, as well as ttl and host unreachable messages to the WAN address of the router. The remote input filters allow packets to the router, e.g., an `eth ip` filter rule could be used to restrict the ICMP packets from going to the LAN.

Note: To secure the router, do not enter rules for port 8 to prevent a ping/trace route to the router and thus a reply from the router.

ICMP port numbers: (0 = echo reply)
(3 = host unreachable)
(8 = echo)
(11 =time exceeded)
(30 = trace-route)

```
remote ipfilter insert output accept -p icmp <remote name>

remote ipfilter insert input accept -p icmp -sp 0 <remote name>

remote ipfilter insert input accept -p icmp -sp 3 <remote name>

remote ipfilter insert input accept -p icmp -sp 8 <remote name>

remote ipfilter insert input accept -p icmp -sp 11 <remote name>

eth ip filter insert output drop -p icmp
```

Telnet Access

The following rules allow Telnet access to the router from the LAN or the WAN. The first two rules allow Telnet access from the LAN to the WAN. The second two rules allow Telnet access from the WAN to the LAN. The last rule is used to prevent Telnet access to the router or WAN from users of a specific or a range of IP addresses on the LAN.

```
remote ipfilter insert output accept -p tcp -dp 23 <remote name>
remote ipfilter insert input accept -p tcp -sp 23 <remote name>

remote ipfilter insert input accept -p tcp -dp 23 <remote name>
remote ipfilter insert output accept -p tcp -sp 23 <remote name>

eth ip filter insert input drop -p tcp -dp 23 -sa <1st lan
ip>:<last lan ip>
```

Allow LAN Access to HTTP

The following rules will allow access to the web based on LAN IP address. These two rules define a range of contiguous LAN IP addresses:

```
remote ipfilter insert output accept

-dp 80 -sa <1st LAN ip addr>:<last LAN IP addr> <remote name>

remote ipfilter insert input accept

-sp 80 -da <1st LAN ip addr>:<last LAN IP addr> <remote name>
```

Control WAN Access to a LAN WebServer

The following rules allow HTTP requests from the WAN. The first two rules allow HTTP requests using a public IP address and a reply from the HTTP server.

The second two rules allow HTTP requests from the WAN using the router's WAN address. In this case, the router has NAT enabled and a server command configured.

```
remote ipfilter insert input accept

-p tcp -dp 80 -da <HTTP server ip addr> <remote name>

remote ipfilter insert output accept

-p tcp -sp 80 -sa <HTTP server ip addr> <remote name>

remote ipfilter insert input accept -p tcp -dp 80 <remote name>

remote ipfilter insert output accept -p tcp -sp 80 <remote name>
```

Control WAN Access to a LAN FTP Server

The following rules allow FTP services to and from the LAN. The first four rules allow any TCP packet using ports 20 or 21 from the LAN. The second four rules allow any TCP packet using ports 20 and 21 from the WAN

Note: Do not use `-da` *or* `-sa` *parameter if the router has NAT enabled.*

```
remote ipfilter insert input accept
-p tcp -sp 21 -dp 1024:65535 <remote name>

remote ipfilter insert output accept
-p tcp -dp 21 -sp 1024:65535 <remote name>

remote ipfilter insert input accept
-p tcp -sp 20 -dp 1024:65535 <remote name>

remote ipfilter insert output accept
-p tcp -dp 20 -sp 1024:65535 <remote name>

remote ipfilter insert input accept
-p tcp -dp 21 -da <FTP server addr> <remote name>

remote ipfilter insert output accept
-p tcp -sp 21 -sa <FTP server addr> <remote name>
```

```
remote ipfilter insert input accept
-p tcp -dp 20 -da <FTP server addr> <remote name>

remote ipfilter insert output accept
-p tcp -sp 20 -sa <FTP server addr> <remote name>
```

Allow DNS Service from the LAN

The following rules will allow a DNS request from the LAN to the WAN.

```
remote ipfilter insert output accept -p udp -dp 53 <remote name>

remote ipfilter insert input accept -p udp -sp 53 <remote name>
```

PPTP

The following commands will allow PPTP through your firewall. The first two commands allow any packet using the protocol GRE to or from the PPTP server. The third command allows TCP packets to the server, using port 1723 with the server's IP address. The last command allows any TCP packet from the PPTP server.

Note: Do not use `-da` *or* `-sa` *parameter if the router has NAT enabled.*

```
remote ipfilter insert input accept
-p 47 -da <pptp server ip addr> <remote name>

remote ipfilter insert output accept
-p 47 -sa <pptp server ip addr> <remote name>

remote ipfilter insert input accept
-p tcp -dp 1723 -da <pptp server ip addr> <remote name>

remote ipfilter insert output accept
-p tcp -sp 1723 -sa <pptp server ip addr> <remote name>
```

Scripting, Listing, Testing, and Troubleshooting a Firewall

To load a script onto a router, follow this procedure.

1. List the commands using any text editor, i.e., Notepad.

2. Open the Quick Start program and connect to the router.

3. Click on "TOOLS", then "EXECUTE SCRIPT".

4. Select the script file and click "OK".

5. The script will be loaded after you verify the file to use.

6. The router will prompt you to reboot, click "OK".

Note: By Telneting to the router and entering the command "system history" after completing the instructions above, you may view any errors that occurred while the script was executed. This is a critical step as your firewall will not act properly if it was not completely configured.

Filter List Command

To view a router's filter configuration, use the following commands:

```
eth ip filter list
remote ipfilter list <remote name>
```

These commands will list all the input, output, and forward filters in separate fields.

To reset the counters on a given interface, type `eth ip fil clear count 1`. This is a great tool to debug your filter functions. Reboot your router, execute the test function, list the filters, and view the count to verify which filters were activated.

Counters use the convention `-c 0.` In the example below, you can see that the filter for destination port 21 was activated once and the filter for destination port 20 was not activated.

```
eth ip filter append 0 input drop -c 1 -dp 21 1
eth ip filter append 1 input drop -c 0 -dp 20 1
```

Filter Check Command

The filter check command will allow the user to enter a packet profile and have the router respond with the action that would be taken. The example below shows that the packet being checked will be dropped.

```
eth ip filter check input -p udp -sp 53 -sa 10.10.10.10
```

The input list action is drop.

Filter Check Command

The `watch` command will allow you to view the important information about packets that are being acted upon by a filter. To view this information, issue the `watch` command, then enter `system log start.` You will be able to view the time stamp, protocol, source address, source port, destination address, destination port, and the action taken by the filter followed by any flags that were set. See the example below.

```
eth ip filter watch on  or remote ipfilter watch on <remote name>

system log start

02/07/2000-16:25:59: UDP packet from 10.10.10.2/138 to
192.168.254.254/138 dropped SYN Flag

02/07/2000-16:25:59:UDP packet from 10.10.10.2/1033 to
192.168.254.254/53 dropped SYN Flag

02/07/2000-16:25:59: UDP packet from 10.10.10.2/1033 to
192.168.254.254/53 dropped SYN Flag
```

This information will help you understand why a specific service is not able to get through your firewall.

When you have a drop rule specified for both interfaces, it can be difficult to tell if a packet is being acted upon by the input or output filters. To overcome this, simply view the count number using the filter list. Alternatively, delete one of the drop rules, then retest the function with `watch` on.

Sample Firewall Script

Copy the following to a text file. You can then load it as a basic firewall script using the Configuration Manager.

```
#flush all existing filters

remote ipfilter flush input internet

remote ipfilter flush output internet

#drop all packets

remote ipfilter append input drop internet

remote ipfilter append output drop internet

#icmp from LAN to WAN will be accepted

remote ipfilter insert output accept -p icmp internet

remote ipfilter insert input accept -p icmp -sp 0 internet

remote ipfilter insert input accept -p icmp -sp 3 internet

remote ipfilter insert input accept -p icmp -sp 8 internet
```

```
remote ipfilter insert input accept -p icmp -sp 11 internet

#telnet from LAN to WAN will be accepted

remote ipfilter insert output accept -p tcp -dp 23 internet

remote ipfilter insert input accept -p tcp -sp 23 internet

#http from LAN to WAN will be accepted

remote ipfilter insert output accept -p tcp -dp 80 internet

remote ipfilter insert input accept -p tcp -sp 80 internet

#ftp from LAN to WAN will be accepted

remote ipfilter insert input accept -p tcp -sp 21 -dp 1024:65535
internet

remote ipfilter insert output accept -p tcp -dp 21 -sp
1024:65535 internet

remote ipfilter insert input accept -p tcp -sp 20 -dp 1024:65535
internet

remote ipfilter insert output accept -p tcp -dp 20 -sp
1024:65535 internet

#dns from LAN to WAN will be accepted

remote ipfilter insert output accept -p udp -dp 53 internet

remote ipfilter insert input accept -p udp -sp 53 internet

save
```

VPN

VPN (Virtual Private Network) is a term used to describe the connection between two or more private (or trusted) networks when the connection is carried across a public (non-trusted) network. A VPN will isolate the private traffic while it is on the public network so that the connection *seems* private.

A VPN can be created in many ways using many different technologies. In this section, we will briefly discuss the difference between physical (Layer-1), transport (Layer-2), and network (Layer-3) methods of creating a private network. Then we will discuss the protocols and equipment standards of a Layer-3 VPN.

Physical (Layer-1) VPNs

ISDN, analog dial-up

Most of us don't think of dial-up services as VPNs, but they have many of the same characteristics. For example, analog dial-up allows a user to connect to a private network (Corporate LAN) by using a public network (PSTN) as the transport.

Advantages

Accessible: The biggest advantage of using the PSTN is that the network reaches almost every location on the planet. Almost anyone can place a phone call to his/her data center because there are telephones all over the world. The network is established and accessible.
Connect to multiple sites: Using the PSTN allows a person to connect to multiple locations by simply dialing different phone numbers. It is very flexible.

Disadvantages

Long distance charges: If the locations being dialed are not local, then connection costs can get very expensive and run up a large bill quickly.
Data throughput limitations: The data throughput using the PSTN has limits due to the technology that is used to pass traffic. If high bandwidth is required, then analog or ISDN dial-up is not an option.

Transport (Layer-2) VPNs

Virtual Circuits

A Layer-2 VPN is typically an ATM or Frame Relay (FR) link over a high-speed DSL, T1, or a T3 line. With both of these protocols (ATM and Frame Relay), a dedicated line can actually be connected to multiple sites simultaneously by means of PVCs (Permanent Virtual Circuits). A PVC allows multiple dedicated (point-to-point) connections to exist over a single dedicated (physical) line.

ATM or Frame Relay transport

When using ATM or Frame Relay (FR) as the transport for network traffic, connections between two (or more) locations are managed with ATM switches. These switches make each PVC

appear like a single point-to-point connection from one ATM router (or bridge) to another. Here again, the ATM network is a public network, and it is used to transport private network traffic.

Advantages

Higher bandwidth: ATM and FR are used as Layer-2 transport on higher speed physical connections. Generally, the lowest speed for FR connections are 56 Kbps dedicated. Speeds go up from there to well over 45 Mbps.
Permanent connections: Each PVC is permanently mapped through the ATM network from one LAN to another. This gives the perception that all of the local networks are connected together and are private.
Quality of Service: The quality of the network service can be guaranteed because of the nature of the ATM protocol.

Disadvantages

Expensive long haul: Connecting a PVC from one location to another will often incur "mileage" charges if the PVC endpoints are not within a few miles of each other.
Permanent connections: The PVC connections are indeed permanent and must be provisioned through the ATM network. Users cannot simply choose to call up another location when they want. This can be a problem if a company needs to add connectivity to multiple sites on a sporadic basis.
Expensive to install: Using permanent connections can be expensive to install, and may not be available in all locations. It requires a commitment to long term quality access from LAN-to-LAN through a WAN connection.

Network (Layer-3) VPNs

Tunneling

Tunneling has been in existence for many years and recently has become the answer to cutting long distance WAN access costs. This is what most of us think of as "VPN". Tunneling uses some Layer-1 and Layer-2 technology already in place. It also uses a public (or private) IP network to connect multiple sites together.

IP Network transport (public or private)

Using a public IP network to transport private LAN data would not have been practical had there not been public IP network on which to transport data. Since the Internet is a public IP network and is now accessible to a majority of users, it is now practical to use it as the transport mechanism for private data.

Advantages

CHEAP: The most compelling reason for using the Internet for a VPN is that it can cut long-distance charges dramatically. The common disadvantage of both Layer-1 and Layer-2 transport is the cost of long distance. Internet long distance is FREE!
Easy to set up: Both networks must have tunneling equipment, but once that is in place, connecting from one network to another is just like placing a phone call.
Flexible: Since it is not cost-prohibitive to install a new tunnel through the Internet, new locations can be brought online quickly.

Disadvantages

No Quality of Service guarantees: The quality of the transport is usually NOT guaranteed and we all know how the Internet can slow down at times. There can be latency and slow throughput if the Internet slows down.
Protocol support: TCP/IP protocol is well suited for running effectively on error-prone networks. However, protocols like Bridging, Appletalk, Novell IPX, and other LAN protocols do not perform well on a highly latent and error-prone network like the Internet.
Interoperability (standards): Current implementations of tunneling protocols are not highly interoperable between vendors due to the young age of the technology. However, there are several tunneling protocol standards that are settling in and this will not remain an issue for long. The standardized protocols for tunneling are IPSec and L2TP.

Technology Standards

IPSec

This protocol encrypts each IP packet that is destined for a tunnel and puts new header information on it to transport it to its destination. The new header information is what creates the "tunnel" effect. This protocol can create a tunnel and encrypt data, but only IP packets can be encrypted and transported. No other protocols are transported through the tunnel.

L2TP (Layer-2 Tunneling Protocol)

Cisco (L2F) and Microsoft (PPTP) agreed to standardize their two tunneling protocols by joining them into a common standard protocol. That protocol is L2TP. The L2TP protocol creates a tunnel between two endpoints and allows a PPP session to be created within it. The L2TP protocol manages the tunnel in a way that makes it transparent to the PPP session inside of it. L2TP clients are like "dial-up" users, and L2TP servers are like access concentrators (modem banks). Once the connection is "dialed", authenticated, and connected, data starts to flow through the tunnel in much the same manner as a modem dial-up, except that the call is placed through the Internet (IP network) instead of the PSTN (telephone network).

PPP (Point-to-Point Protocol)

PPP is used primarily for dial-up access right now because it allows for the dynamic negotiation of link parameters during the link establishment phase. This simplifies interoperability among dial-up devices. PPP provides the following benefits:

Authentication*:* Tunnel users can be authenticated, so that only authorized tunnel clients are accepted by the tunnel server.

Dynamic IP*:* An IP address can be dynamically assigned to the tunnel client when the tunnel is created. This conserves IP addresses because they can be issued out of a pool and recycled. PPP is currently used in this manner with dial-up users.

Multiple protocol support: Multiple LAN protocols (IP, IPX, Appletalk, and Bridging) can be transported on the same link.

***Data and header compression**:* Van Jacobson header compression and STAC data compression can only be used in conjunction with PPP. Up to 5 times more data can be transferred by using compression.

DES Encryption
IPSec has encryption built into it, therefore, the data being transported is kept private while it is on the public Internet. L2TP does not encrypt the data as part of the tunnel management, so the data being transported in an L2TP tunnel must be encrypted before entering the tunnel. DES encryption is a United States Department of Defense standard for encryption that is widely deployed and comes in different strengths (40 bit, 56 bit, 128 bit, and triple DES). DES can encrypt any LAN protocol.

Tunnel Server

Function
The L2TP tunnel server receives tunnel "calls" and controls the tunnel once it is created. It is responsible for multiple tunnels simultaneously. The server can run as a service on a network server or as a stand-alone device on the network.

Location
The L2TP tunnel server is usually located at the edge of a LAN where it connects to the WAN. Generally, the tunnel server will be attached on both sides of the firewall. This allows tunnel traffic to access the tunnel server from the exposed WAN and be transported to the private LAN without going through the firewall. Sometimes tunnel servers are placed completely behind the firewall and only tunnel traffic is allowed through the firewall for access to the private LAN.

LAN-based Tunnel Client

Function
The LAN-based L2TP tunnel client initiates "calls" to the tunnel servers to which it needs to connect. Once the tunnel is established, the server takes control of the tunnel management. The L2TP tunnel client can be a stand-alone device or run as a service on a network server. This type of tunnel client must initiate calls to the tunnel server whenever LAN traffic needs to be forwarded and disconnect the call when the traffic stops. The LAN-based tunnel client manages the tunnel creation on behalf of the workstations on the LAN and is transparent to them.

Location
It is usually located on the boundary where the LAN and WAN meet, but it can reside anywhere on the LAN. This device can initiate calls, but cannot receive calls, so it can be located either inside of the firewall or across it.

Workstation-based Tunnel Client

Function
The workstation-based L2TP tunnel client initiates "calls" to the tunnel servers to which it needs to connect, but it can only support the workstation creating the tunnel. This type of tunnel client can only support one workstation unlike the LAN-based client which supports multiple workstations. This is software that runs on a workstation and is ideal for remote users who carry laptop computers and need access to the tunnel from different locations.

Location
This software is installed on the workstation for the purpose of creating a tunnel to a LAN.

Service Provider-based VPNs

Tunneling from a POP or access concentrator
VPN services can be provided to users by creating and terminating the tunnels at the Internet Service Provider (ISP) Point of Presence (POP) on the Internet. This allows dial-in users to place a normal call to the POP, which in turn creates a tunnel to a Corporate site. The tunnel is not created from the dial-up device, but instead from the device that receives that call. Before the data can get to the Internet, it is encapsulated into the tunnel and sent to the Corporate LAN.

Types of VPNs used
All of the technologies listed above are used to create these tunnels. The ISP might have a PVC connection to a Corporate site, or an L2TP tunnel, or even an IPSec connection. Whatever the choice, it is transparent to the end user. The user simply places the modem call to the ISP POP and logs onto the Corporate network.

Advantages

ISP manages the service: The end user uses traditional dial-up devices and is connected to the Corporate network. If it does not work, then the ISP has to fix the problem as part of the service.
ISP can offer a valuable service: The ISP can add value for the customer and sell a managed VPN service. This can be a win / win situation for both the ISP and the end user.
Dedicated access: This solution can work for dedicated access as well. The end user does not know if the data connection is running over ATM or L2TP once it leaves the customer premises. The ISP can use this in lieu of an ATM PVC.

Disadvantages

Workstation-client to LAN-server Service cost: The cost for the VPN service might be fairly high because it is a recurring monthly cost.
No Quality of Service guarantee: ISPs do not offer any guarantees for the Quality of Service (QoS) on these accounts. QoS guarantees come with dedicated services only.
Limited mobile access: The user cannot dial into just *any* ISP and expect to be connected to the Corporate Network. There will be a limited number (and location) of POPs that will provide the desired access.

Workstation Client to LAN Server

Tunneling from a Workstation to a Server on the Enterprise LAN
This is a common approach to VPN. The workstations at the remote offices or homes have special software installed that allows them to connect to the tunnel server on the Corporate LAN. The connection is transparent to the Internet and each workstation is authenticated and managed independently on its own tunnel. Each workstation can have a different means of accessing the Internet (modem, LAN router, etc).

Types of VPNs used
Typically, only tunneling VPN solutions are used in this environment. It is used when there are a lot of mobile users who need to connect to the corporate office. All they need to do is have

access to the Internet, and the software on the workstation will be able to connect to the Corporate LAN.

Advantages

Mobile access: Accessing the Corporate network is as simple as finding a phone to plug into and dialing the Internet. The user is not limited to any particular ISP or modem technology, but the workstation must have the tunnel client software installed and configured.
Do it yourself: This type of VPN can be installed and configured quickly. Then it can be easily added to when new users come online.

Disadvantages
Software must be installed on each workstation: Each workstation that accesses the Corporate LAN through VPN needs to have the tunneling software installed and configured on it. This can be a problem if the client software is not available for all operating systems. This can also be a problem if the workstation gets lost or stolen -- the thief can access the Corporate LAN.
Large number of tunnels to service: Since each workstation is its own tunnel, this can create a high volume of tunnels for the Corporate tunnel server to manage. It can also add to LAN traffic if LAN-based workstations are tunneling over the LAN on the way to the Corporate network.

LAN client to LAN server

Tunneling from LAN/WAN edge to LAN/WAN edge at Enterprise
Creating tunnels at the edge of a LAN, just before data leaves the trusted network, is a practical approach when the whole LAN needs to gain access to another LAN that is also attached to the Internet. This approach is ideal for small offices and telecommuters that do not require mobile access to the Corporate network.

Types of VPNs used
Both ATM PVCs and tunneling VPNs can be practical for LAN-to-LAN connections. If all of the LANs are local and the connections don't need to vary, then ATM might be the best solution. If even one location is far away from the others or if many different connection possibilities must be present, then tunneling makes more sense.

Advantages
Simultaneous connections to multiple sites: Multiple sites can be connected together using this VPN strategy because each LAN-attached tunnel device can connect to multiple locations.
Fewer tunnels to manage: By creating only one tunnel for each LAN, the number of tunnels that have to be managed is reduced.
No workstation software required: By creating a tunnel as the LAN data sent to the Internet, there is no need to create tunnels from each workstation and therefore no need to install special software on each workstation.
Cost: This solution can cost far less in equipment and management since it centralizes the tunneling functions on each LAN and is transparent to other devices on the LAN.

Disadvantages
Mobile users still need workstation software: Even with the LAN-to-LAN approach, mobile users still need to have software installed on their laptops if they wish to have access to the LAN.

SpeedStream Secure VPN Option

SpeedStream Secure VPN software has been designed to provide maximum flexibility and function.

Embedded system: Secure VPN software runs on the router without any additional hardware. It is a software-only upgrade.

Client AND server: Each router has the capability of being a tunnel client and a tunnel server *simultaneously*. If a call comes in, then the router will be a server. If a call needs to be placed outbound, then the router will be a client. When connecting two LANs together using L2TP, it is common for both networks to need a tunnel server and a tunnel client, so that they can place and receive tunnel calls.

Dial-on-Demand: Tunnels are created and destroyed dynamically based on network traffic and an inactivity timer. This allows multiple tunnels to be available, and only the required ones are active. Tunnels can be run ***with or without encryption***.

Multiple protocols supported: IP routing, IPX routing, and bridging are supported to allow for Microsoft Networking, Novell networks and other non-IP protocols to function properly through the tunnel(s).

DES Encryption with Dynamic Key Exchange: When running an encrypted tunnel, the encryption keys are dynamically exchanged to make it almost impossible to expose the data.

Each tunnel is a virtual interface: All elements of NAT, DHCP, Firewall, routing, bandwidth thresholds, inactivity time-outs, etc. can be configured on a per-tunnel basis, and are independent "virtual" interfaces.

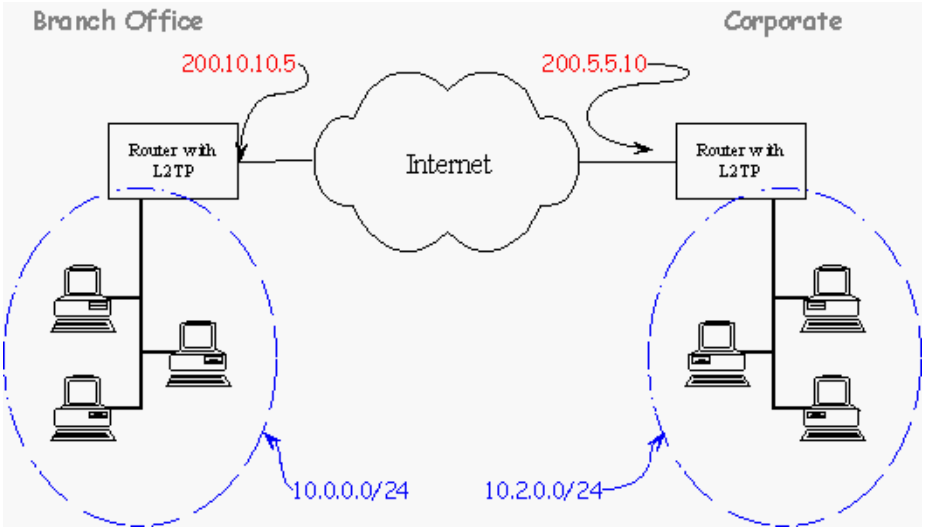
SpeedStream Secure VPN is ideally suited for "do-it-yourself" setup of LAN-to-LAN VPNs using existing remote access hardware. Tunneling, multi-protocol support, encryption, compression, flexibility, and a smart design will make you think that you are configuring a dial-up device.

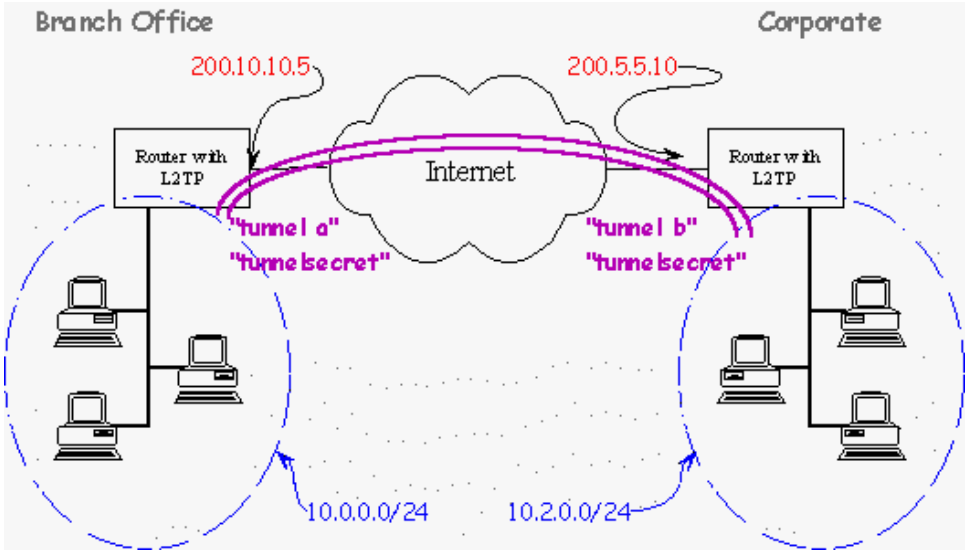
When it is necessary to connect several sites together with tunneling, there are two options:

- Set up a central tunnel server as the hub for all tunnel clients to communicate with other sites.
- Set up capability for each site to connect to all sites without going through a central server.

The latter will distribute the load of network traffic based on site requirements and connections will never suffer from a congested central server.

The following example describes how to configure two DSL routers for LAN-to-LAN connectivity using the Internet as transport. L2TP Tunneling is used to create a PPP session between the two WAN port IP addresses of the DSL routers. For data security, DES Encryption with Diffie-Hellman key exchange is used to encrypt the data that is sent into the L2TP tunnel. IP datagrams are routed between Corporate and Branch Office. Other protocols can be transported, but are not considered in this example. The diagram below depicts the setup.


Branch Office
Corporate
200.10.10.5
200.5.5.10
Router with L2TP
Internet
Router with L2TP
10.0.0.0/24
10.2.0.0/24


Branch Office
Corporate
200.10.10.5
200.5.5.10
Router with L2TP
Internet
Router with L2TP
"tunnel a"
"tunnelsecret"
"tunnel b"
"tunnelsecret"
10.0.0.0/24
10.2.0.0/24

Step 1: Configure Both Routers for Internet Connectivity

This configuration example assumes the routers are already configured to connect to the Internet. The configuration uses PPP for the link protocol and has IP routing only.

Branch Office Configuration:
This router has an IP address of 10.0.0.1 on the LAN and 200.10.10.5 on the WAN. NAT is on and it tunnels to another network (10.2.0.0). It is set as an L2TP Server and Client -- it can place a tunnel call to its peer or receive a call from a peer. The IP address of the peer tunnel device is 200.5.5.10.

NOTE: You cannot ping the tunnel endpoint, only the LAN behind it.

The `eth ip addr 10.0.0.1 255.255.255.0` command sets the Ethernet address of the branch office router. You may not need to change this setting unless both LAN subnets of the VPN are identical. Each LAN of a VPN solution must be a unique subnet.

Corporate Configuration:
This router has an IP address of 10.2.0.1 on the LAN and 200.5.5.10 on the WAN. NAT is on and it tunnels to another network (10.0.0.0). This device is set as an L2TP Server and Client. It can receive a tunnel call from its peer or place a call to a peer. The IP address of the peer tunnel device is 200.10.10.5

NOTE: You cannot ping the tunnel endpoint, only the LAN behind it.

The `eth ip addr 10.2.0.1 255.255.255.0` command sets the Ethernet address of the corporate router. You may not need to change this setting unless both LAN subnets of the VPN are identical. Each LAN of a VPN solution must be a unique subnet.

Step 2: Configure the L2TP Tunnel Connections

Branch Office Configuration:
Set up the tunnel to Corporate with:

```
l2tp add tunnelb
```

The name "tunnelb" is the name that is expected from the tunnel peer when challenged to identify itself. The Branch Office router asks "Who are you?" and Corporate says "I am tunnelb" and the Branch Office authenticates. This command must match the Corporate router name in the command:

```
l2tp # set ourtunnelname <name> <tunnel name>
```

Next, define the common authentication secret used between the two devices. This tunnel device will use the password of "tunnelsecret" for the tunnel peer when challenged to identify itself. Both peers use the same secret:

```
l2tp set chapsecret tunnelsecret tunnelb
```

Define the name of the our end of the tunnel for authentication purposes. The name "tunnela" is sent to the tunnel peer when challenged to identify yourself. Corp says "who are you" Branch replies "I am tunnela" Corporate authenticates. This setting must match the command "l2tp add <name>" on the Corporate router.

```
l2tp set ourtunnelname tunnela tunnelb
```

Define the sysname of this router for authentication purposes. This tunnel device sends the name "cust" when challenged to identify itself. This must match the command "remote add <name>" on the Corporate router.

```
l2tp set oursysname cust tunnelb
```

Define the password of this router for authentication purposes. This tunnel device sends the password "custpass" when challenged to identify itself. This must match the password in the command "rem setpasswd <password>" on the Corporate router.

```
l2tp set ourpassword custpass tunnelb
```

Set the IP address of the other end of the tunnel, that is, the WAN IP address of the Corporate router.

```
l2tp set address 200.5.5.10 tunnelb
```

Set LAC and/or LNS. In this case, both will allow this router to establish and receive a tunnel.

```
l2tp set type all tunnelb
```

Add the remote profile for the IP network on the other end of the tunnel. This name must match the name in the command "l2tp set oursysname <name> <tunnelname>" on the Corporate router.

```
remote add corp
```

Define the authentication password expected for this PPP link. This must match the password used in the command "l2tp set ourpassword password> <tunnel name>" on the Corp router.

```
remote setpasswd corppass corp
```

Define the other tunnel device as the LNS. This must match the tunnel name in the command "l2tp add <tunnel name>" on the Branch router. This links the l2tp settings to the remote settings for this tunnel profile.

```
remote setlns tunnelb corp
```

Set authentication to CHAP for the PPP link.

```
remote setauthen chap corp
```

Add an IP route to the LAN on the other end of the tunnel PPP link, aroute must be added for each subnet that exist on the Corp LAN.

```
remote addiproute 10.2.0.0 255.255.255.0 1 corp
save
reboot
```

Corporate Configuration:
Set up the tunnel to the Branch Office. The name "tunnela" is the name that is expected from the tunnel peer when challenged to identify itself. Corporate asks "Who are you?" and Branch Office says "I am tunnela" and Corporate authenticates. This setting must match the command "l2tp setourtunnelname <name> <tunnelname>" on the Branch Office router.

```
l2tp add tunnela
```

Define the common authentication secret used between the two routers in the VPN. This tunnel device will use the password of "tunnelsecret" for the tunnel peer when challenged to identify itself. Both peers use the same secret.

```
l2tp set chapsecret tunnelsecret tunnela
```

Define the name of our tunnel for authentication purposes. This tunnel device sends the name "tunnelb" when challenged to identify itself by the tunnel peer. Branch Office asks "Who are you?" and Corporate says "I am tunnelb" and Branch Office authenticates. This setting must match the name in the command "l2tp add <name>" on the Branch Office router.

```
l2tp set ourtunnelname tunnelb tunnela
```

Define the sysname of this router, for authentication purposes. This tunnel device sends the name "corp" when challenged to identify itself. This setting must match the name in the command "remote add <name>" on the Branch Office router.

```
l2tp set oursysname corp tunnela
```

Define the password of this router for authentication purposes. This tunnel device sends the password "corppass" when challenged to identify itself. This must match the password in the command "rem setpasswd <password>" on the Branch Office router.

```
l2tp set ourpassword corppass tunnela
```

Set the IP address of the other end of the tunnel, that is, the WAN IP address of the Branch router.

```
l2tp set address 200.10.10.5 tunnela
```

Set LAC and/or LNS. In this case both, this will allow this router to establish and receive a tunnel.

```
l2tp set type all tunnela
```

Add the remote profile for the IP network on the other end of the tunnel. This must match the name in the command "l2tp set oursysname <name> tunnel name>" on the Branch Office router.

```
remote add cust
```

Define the authentication password expected for this PPP link. This must match the password used in the command "l2tp set our password <password> <tunnel name>" on the Branch Office router.

```
remote setpasswd custpass cust
```

Define the other tunnel device as the LNS. This must match the tunnel name in the command "l2tp add <tunnel name>" on the Corp router. This command ties the l2tp settings to the remote settings for this tunnel profile.

```
remote setlns tunnela cust
```

Set authentication to CHAP for the PPP link.

```
remote setauthen chap cust
```

Add an IP route to the LAN on the other end of the tunnel PPP link. A route must be added for each subnet that exists on the Branch Offfice LAN.

```
remote addiproute 10.0.0.0 255.255.255.0 1 cust
save
reboot
```

Step 3: Configure Encryption and Key Exchange

Branch Office Configuration:

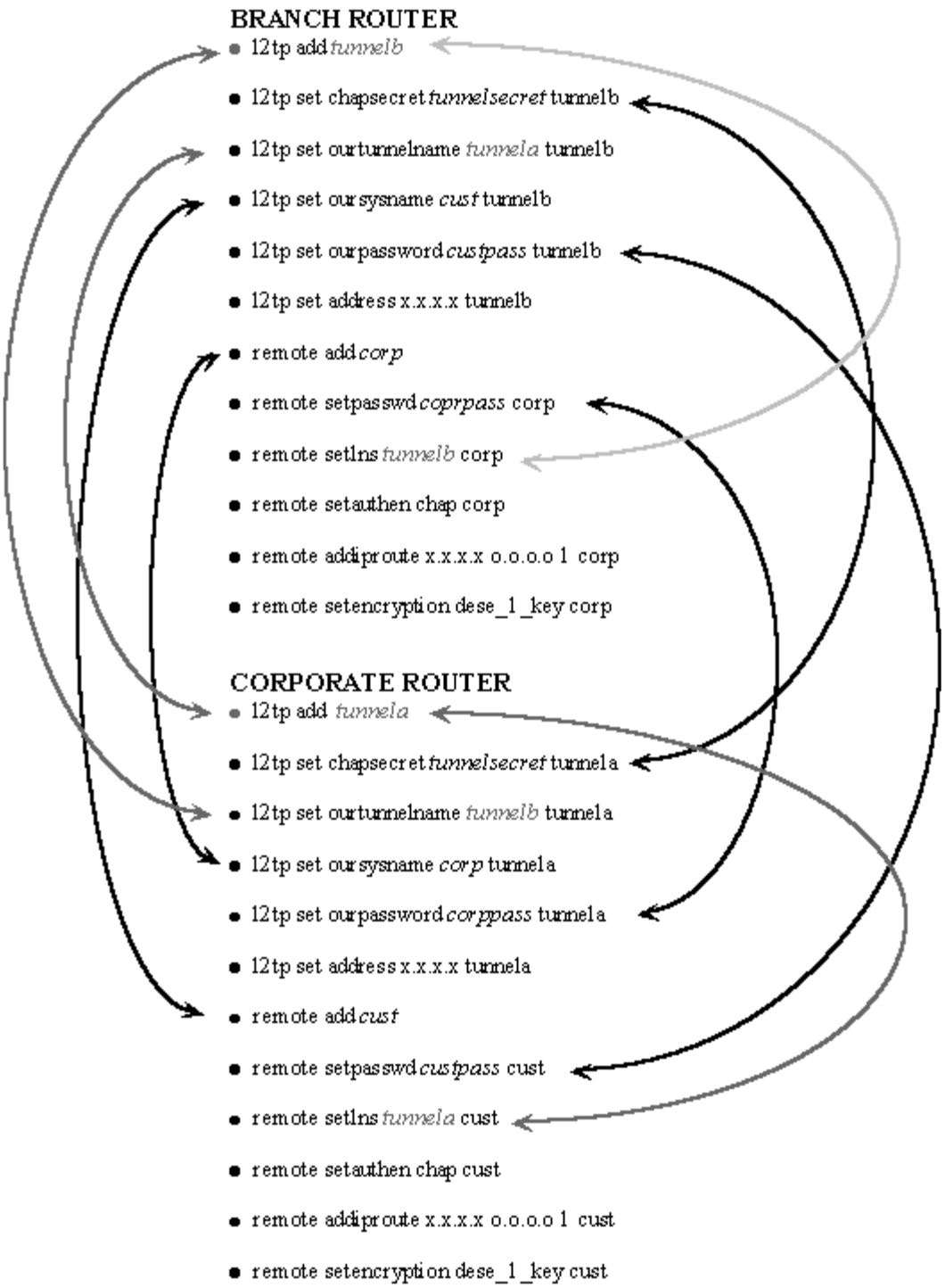
Enable encryption on the PPP link that goes through the tunnel.

```
remote setencryption dese_1_key corp
save
reboot
```

Corporate Configuration:

Enable encryption on the PPP link that goes through the tunnel.

```
remote setencryption dese_1_key cust
save
reboot
```


BRANCH ROUTER
l2tp add tunnelb
l2tp set chapsecret tunnelsecret tunnelb
l2tp set ourtunnelname tunnela tunnelb
l2tp set oursysname cust tunnelb
l2tp set ourpassword custpass tunnelb
l2tp set address x.x.x.x tunnelb
remote add corp
remote setpasswd coprpass corp
remote setlns tunnelb corp
remote setauthen chap corp
remote addiproute x.x.x.x o.o.o.o 1 corp
remote setencryption dese_1_key corp
CORPORATE ROUTER
l2tp add tunnela
l2tp set chapsecret tunnelsecret tunnela
l2tp set ourtunnelname tunnelb tunnela
l2tp set oursysname corp tunnela
l2tp set ourpassword corppass tunnela
l2tp set address x.x.x.x tunnela
remote add cust
remote setpasswd custpass cust
remote setlns tunnela cust
remote setauthen chap cust
remote addiproute x.x.x.x o.o.o.o 1 cust
remote setencryption dese_1_key cust

VPN with IP Filtering and MS Networking

When setting up Secure VPN and Firewall functions, the configuration of routers is not complete until each user can log onto the corporate domain controller for access to all resources on the LAN. UDP relay and WINS server commands will allow MS networking to function through a VPN tunnel. The following items must be configured:

1. Domain controller must be configured for networking using IP.
2. Client workstations must be configured for networking using IP.
3. A router must have UDP relay configured.
4. A router must be configured to serve the primary and secondary WINS server IP addresses.
5. A firewall must accept packets to and from the IP address of the far end.

For instructions on items 1 and 2, consult a Windows manual. A script for items 3, 4, and 5 appears below.

```
system addudprelay
<server IP address> <first port> <last port>
system addudprelay 192.168.254.50 137 139

dhcp set valueoption 44
<primary wins server ip address> <secondary>
dhcp set valueoption 44 192.168.254.50 192.168.254.60

remote ipfilter insert input accept
-sa < IP address of far end> <remote name>
remote ipfilter insert output accept
-da < IP address of far end> <remote name>
remote ipfilter insert input accept -sa 200.x.x.x internet
remote ipfilter insert output accept -da 200.x.x.x internet
```

System Level Commands

These commands are online action and status commands. They allow you to perform the following:

- Log into and log out of configuration update mode
- Display the router's configuration, the version and level numbers
- List running tasks, memory, communication interfaces
- Connect to a remote router to test the line
- List IP routes, IPX routes, SAPs, root bridge
- Save the new configuration image
- Reboot the system

`arp delete`
Deletes the IP address of the entry in the ARP table.

`arp list`
Lists ARP table entries in an IP routing environment. ARP (Address Resolution Protocol) is a tool used to find the appropriate MAC addresses of devices based on the destination IP addresses.

`bi`
Lists the root bridge.

`bi list`
Lists MAC addresses and corresponding bridge ports as learned by the bridge function. This list includes several flags and the number of seconds elapsed since the last packet was received by the MAC address.

`call`
Dials a remote router. This command can be used to test the ISDN link and the remote router configuration settings.

`exit`
Has the same function as logout, but will disconnect you from a Telnet session.

`ifs`
Lists the communications interfaces installed in the router and the status of the interfaces.

`ipifs`
Lists the IP interface.

`iproutes`
Lists the current entries in the IP routing table.

`ipxroutes`
Lists the current entries in the IPX routing table.

`ipxsaps`
Lists the current services in the IPX SAPs table.

`logout`
Logs out to reinstate administrative security after you have completed changing the router's configuration.

`mem`
Lists memory and buffer usage.

`mlp summary`
Lists the status of the any protocols negotiated for an active remote connection. The following lists the most common protocols:

- MLP (PPP Link Protocol)
- IPNCP (IP routing Network Protocol)
- CCP (Compression Network Protocol)
- BNCP (Bridging Network Protocol)
- IPXCP (IPX Network Protocol)

"Open" indicates that the protocol is in ready state.
"Stopped" means that the protocol is defined but did not successfully negotiate with the remote end.
No message means that the link is not active.

`ping`
An echo message, available within the TCP/IP protocol suite, sent to a remote node and returned; it is used to test connectivity to the remote node and is particularly useful for locating connection problems on a network. By default, the router will try to "ping" the remote device for five consecutive times and will issue status messages.

`ps`
Lists all of the tasks (processes) running in the system and the status of the tasks.

`reboot`
This command causes a reboot of the system. You must perform a reboot after you have configured the router the first time or when you modify the configuration. Reboot is *always* required when the following configuration settings are modified:

- System Settings Ethernet IP Address
- Ethernet IPX Network Number
- TCP/IP and IPX Routing
- Remote Router Default Bridging Destination
- TCP/IP Route Addresses
- IPX Routes
- SAPs and Bridging

Reboot is also required when adding a new remote entry in the remote database.
Reboot also ensures that all file system updates are completed. There is a time lag between the **save...** commands and the time the data is safely stored in FLASH memory. If the power goes off during this time, data can be lost.

Always reboot before powering off the router. Alternatively, use the **sync** command.
Caution: This command erases all of the configuration data in the router.

`tcp stats`
Displays the TCP statistics and open connections.

`vers`
Displays the software version level, source, software options, and amount of elapsed time the router has been running.

List Commands

These commands can be used as a quick reference when checking or making changes to a router's configuration.

Sample output messages are also provided in this section. For your convenience, "associated commands" for changing individual parameters have been placed to the right of each message.

`system support`
This command provides a comprehensive status report of your router's activity.

`system history`
This command creates a 12,000-character buffer that is maintained in the router's memory. This buffer contains all the messages that normally appear on the Console screen and gives you a snapshot of the router's recent activity. The buffer is cleared when power is cycled on the router. It is maintained across soft reboots. You must be logged in to view this information.

`vers`
This command gives the router's hardware description, BOOT/POST version (Boot), software (kernel) version, and the available software options currently running on the router.

Sample Output:

FlowPoint/144 IDSL Router
FlowPoint-100 BOOT/POST V2.1.0 (07-02-97 15:25)
Software version v2.7.1 built Wed May 13 18:34:55 PDT 1998
Options: FRAME RELAY, IP, IP TRANS, HOST MAPPING, DHCP
Up for 0 days 0 hours 13 minutes (started 7/15/1998 at 16:44)

`mem`
Provides a snapshot of current memory utilization.

`ps`
Lists the processes currently running.

system list

Lists the global configuration elements for the router.

Sample Output:	**Associated Commands:**
GENERAL INFORMATION FOR <router>	`system name <system name>`
System started on... 7/15/1998 at 16:44 *(Date and time that system was started)*	
Authentication override..... none	`system authen none|pap|chap`
WAN to WAN Forwarding..... yes	`system wan2wanforwarding on|off`
BootP/DHCP Server address.....none	`system bootpServer <ipaddr>`
Telnet Port..... default (23)	`system telnetport default|disabled|<port>`
SNMP Port..... default (161)	`system snmpport default|disabled|<port>`
System message: Configured_by_Internet_Quick_Start	`system message <message>`

eth list

Lists the Ethernet LAN port number, status of bridging and routing, IP protocol controls, and IP address and subnet mask.

Sample Output:	**Associated Commands:**
GLOBAL BRIDGING/ROUTING SETTINGS: GLOBAL ETHERNET SETTINGS	
Bridging enabled..... yes	`remote disBridge <remoteName>`
IP Routing enabled..... yes	`eth ip enable|disable`
Multicast forwarding enabled.....no	
Firewall filter enabled .....yes	`eth ip firewall on|off|list`
RIP Multicast address.... default	`eth ip ripmulticast <ipaddr> <port#>]`
ETHERNET INFORMATION FOR <ETHERNET/0>ETHERNET/0 INTERFACE SETTINGS	
Hardware MAC address....00:20:6F:02:CC:3A	
Send IP RIP to the LAN..... no	`eth ip options txrip on|off [<port#>]`
Advertise me as default router...yes	`eth ip options txdef on|off [<port#>]`
Process IP RIP packets received... no	`eth ip options rxrip on|off [<port#>]`
Receive default route by RIP.... yes	`eth ip options rxdef on|off [<port#>]`
IP address/subnet mask..... 192.84.210.43/255.255.255.128	`eth ip addr <ipnet> <ipnetmask> [<port#>]`
Static Ethernet routes defined..... none	`eth ip defgateway <ipaddr> [<port#>]` `eth ip addroute<ipaddr><ipnetmask><gateway><hops>[<port#>]`

dhcp list

This command lists global information on the router's DHCP server configuration.

Sample Output:

```
bootp server ..... none
bootp file ..... n/a
Subnet 192.84.210.0, disabled by user
When DHCP servers are active…..stop
Mask ..... . ..... 255.255.255.128
first ip address . 192.84.210.2
last ip address ..... 192.84.210.20
lease ..... default
bootp ..... not allowed

bootp server..... none

ipaddr>bootp file ..... n/a
```

Associated Commands:

```
all|<net>|<ipaddr>
dhcp set otherserver <net> continue|stop
dhcp set mask <net> <mask>
dhcp set addresses <first ipaddr> <last ipadd
dhcp set lease [<net>|<ipaddr>]<hours>|default|infini
dhcp bootp allow <net>|<ipaddr>
dhcp bootp disallow <net>|<ipaddr>
dhcp bootp tftpserver [<net>|<ipaddr>]<tftpserver
dhcp bootp file [<net>|<ipaddr>] <name>
```

Client IP	State	Host Name	Expires (yy/mm/dd)
192.84.210.2	enabled	NAME UNKNOWN	expired

remote list

This command lists configuration information associated with each Virtual Circuit (Virtual WAN Interface). The following is the default profile that is created when `remote add <remoteName>` is used:

Sample Output:

```
INFORMATION FOR <default>
Status..... enabled
Interface in use..... FR
Protocol in use..... FR - Frame Relay
Data Link Connection Id (DLCI).....
IP address translation..... off
Send/Receive Multicast..... off
Source IP address/subnet mask..... 0.0.0.0/0.0.0.0
Remote IP address/subnet mask..... 0.0.0.0/0.0.0.0
Send IP RIP to this dest..... no
Send IP default route if known..... no
Receive IP RIP from this dest..... no
Receive IP default route by RIP.... no
Keep this IP destination private..... yes
Total IP remote routes..... 0
Bridging enabled..... no
Exchange spanning tree with dest... yes
```

This is a modified configuration:

Sample Output:	**Associated Commands:**
INFORMATION FOR <internet2>	`remote add <remoteName>`
Status..... enabled	`remote enable|disable <remoteName>`
Interface in use..... FR	`isdn set switch FR64|FR128|FR144`
Protocol in use.. FR-Frame Relay	`remote setprotocol PPP|FR|MER <remoteName>`
Data Link Connection Id (DLCI).. 17	`remote setDLCI <dlci number> <remoteName>`
IP address translation..... on	`remote setIPTranslate on|off <remoteName>`
Send/Receive Multicast..... off	`remote setipoptions multicast on|off <remoteName`
Source IP address/subnet mask.... 1.1.1.1/255.255.255.0	
Remote IP address/subnet mask.. 2.2.2.2/255.255.255.0	
Send IP RIP to this dest..... no	`remote setipoptions txrip on|off <remoteName>`
Send IP default route if known..no	`remote setipoptions txdef on|off <remoteName>`
Receive IP RIP from this dest. No	`remote setipoptions rxrip on|off <remoteName>`
Receive IP default route by RIP. No	`remote setipoptions rxdef on|off <remoteName>`
Keep this IP destination private.yes	`remote setipoptions private on|off<remoteName`
Total IP remote routes..1	`remote addIproute <ipNet> <ipNetMask><hops><remoteNam`
`192.168.100.0/255.255.255.0/1`	
Bridging enabled..... no	`remote enaBridge <remoteName>`
Exchange spanning tree with dest. yes	`remote setBrOptions stp on|off <remoteName>`

NOTE: If MER is the selected link protocol, use the following command to add IP routes:

`remote addIproute <ipNet> <ipNetMask> <hops> <ipGateway> <remoteName>`

`ifs`

Provides status information for all of the router interfaces (physical and logical).

Sample output:

Interface	Speed	In %	Out %	Protocol	State	Connection
ETHERNET/0	10.0mb	0%/0%	0%/0%	(Ethernet)	OPENED	
FR/3	128kb	0%/0%	0%/0%	(HDLC/FR)	STANDBY	
FR-VC/1	0 b			(FR)	OUT-OF-SERVICE	
CONSOLE/0	9600 b	0%/0%	100%/20%	(TTY)	OPENED	

`mlp show`

This command gives information on the current state of PPP negotiation.

`bi`

This command lists the current bridge filters that are defined.

`iproutes`

Current routing table (Dynamic and Static routes)

Sample output:

IP route/Mask	--> Gateway	Interface	Hops	Flags
0.0.0.0/ffffffff	--> internet	[down]	1 NW FW	PERM DOD
192.84.210.0/ffffff80	--> 0.0.0.0	ETHERNET/0	1 FW DIR	PERM
192.84.210.43/ffffffff	-->0.0.0.0	ETHERNET/0	0 ME	
224.0.0.9/ffffffff	--> 0.0.0.0	[none]	0 ME	
255.255.255.255/ffffffff	-->0.0.0.0	[none]	0 NW PERM	

Static Routes Pointing to the WAN

```
remote addiproute <ipNet> <ipNetMask> <hops> <remoteName>
```

Example: `remote addiproute 192.168.100.0 255.255.255.0 1 internet`

When using MER:

```
remote addIproute <ipNet> <ipNetMask> <hops> <ipGateway> <remoteName>
```

Example: `remote addiproute 192.168.100.0 255.255.255.0 1 207.65.65.1 internet`

Note: Once added, they will not take effect until the "save" and "reboot" commands are issued.

Static Ethernet Routes

Static Ethernet route:

```
eth ip addroute <ipaddr> <ipnetmask> <gateway> <hops> [<port#>]
```

Example: `eth ip addroute 192.168.25.0 255.255.255.0 192.168.100.1 1`

Default Ethernet route:

```
eth ip defgateway <ipaddr> [<port#>]
```

Example: `eth ip defgateway 192.168.100.1`

Note: Once added, they will not take effect until the "save" and "reboot" commands are issued.

Dynamic WAN Routes

```
remote setipoptions txrip on|off <remoteName>
remote setipoptions rxrip on|off <remoteName>
```

Dynamic Ethernet Routes

```
eth ip options txrip on|off [<port#>]
eth ip options rxrip on|off [<port#>]
```

Basic Debug Tools

Route Print

When a networked PC is operating strangely, it is possible that certain tasks are relying on routes that are no longer valid. Entering `route print` after a DOS command will show the routing table that is controlling that PC. It is best to compare the output of a working PC to that of the failed unit on the same LAN to troubleshoot this type of routing problem.

IP Routes

The command `ipr` is roughly equivalent to the route print command, however, both WAN and LAN routes will be indicated.

IP Configuration

The Windows 95/98 DOS command `winipcfg` and the Windows NT command `ipconfig` will display the current IP configuration of the PC, which includes the IP address, subnet mask and default gateway. If the PC is configured to receive its IP address dynamically, the buttons "release all" and "renew all" will be active. Those buttons will allow a PC to receive a new IP address without rebooting the PC.

Ping

All routers are capable of generating a ping through a Console or Telnet connection. A router can ping any address on the LAN or WAN, but not itself. If you Telnet to the router's LAN IP address, you will not be able to ping the router's WAN address. When testing a router from a DOS prompt on a LAN PC, you cannot ping the router's WAN address until the router lights are in a "ready" state (DSLAM connection established). When a VPN is established, any IP address on the remote LAN of a tunnel connection will reply to a ping, but you will not be able to ping the target end of a tunnel from a router or a PC on the LAN.

To test connectivity, enter `ping` in the Command Line Interface (or after a DOS Prompt) followed by the IP address that you wish to test.

The response below indicates a good connection:

```
ping 1.1.1.2
ping: reply from 1.1.1.2: bytes=56 (data), time <5 ms
```

The following response indicates a lack of connectivity:

```
ping 1.1.1.3
ping: 1.1.1.3 - no response
```

Telnet

Telnet facilitates an Ethernet connection to the Command Line Interface of routers. To open a Telnet session, go to a DOS prompt and enter the command `telnet` followed by the IP address of the target router. Once connected to the router, you will be prompted to login. The default password is `admin`. Once the password is accepted, the router's configuration may be listed or changed. When the command `reboot` is entered, the Telnet session will be terminated. If you wish to re-establish a Telnet session, simply close the window, then reconnect when the router has rebooted

The default Telnet buffer is not large enough to support the output of many of the router commands. To increase buffer size, click "terminal" then "preferences" in the Telnet widnow, then set the buffer from 25 to 200. Advanced router configurations -- Server, firewall, VPN, encryption, host-mapping, and debug commands -- are performed through Telnet only.

Traceroute

A traceroute command is similar to a ping, except that the output will tell the user much more about the path. To perform a traceroute, go to a DOS prompt and enter the command `tracert` followed by the target IP address. The output will indicate every hop (routing device), from the starting point to the destination or target IP address. This is useful in determining which devices have delayed responses or will not respond to a ping.

Other Debug Commands

The following commands are available for debugging purposes. Please use them with caution because they are not fully supported and are subject to change.

General Debug Commands

`ifs` Shows which interfaces are configured or active.

`mlp debug` <LCP | NCP | BNCP | IPCP | IPXCP | CCP | ECP | MLP | AUTH | NCPSTATES> [<0>]

BNCP is for bridging, ECP for encryption, and NCPSTATES for state table changes.
To turn off the trace, enter the command with the optional **0** at the end.

```
ipdebug icmp 1
ipdebug nat 1
```

These commands show data received. The ipdebug icmp 1 command is useful for verifying that the router can receive cells.

`dod whycall 80`

Prints out the packet that is causing the link to come up. This is useful when `system onewan on` is set. The latter command makes PVCs look like dial-up links, that is, the link comes up only if user traffic exists and the link times out on inactivity.

`dod debug <1 | 0>`

Shows a trace of when the link was brought up or timed out due to inactivity. Specify 1 to turn on the trace; specify 0 to turn off the trace.

`system log [start | stop | status]`

Starts event logging when logged in via Telnet. Otherwise, you do not see any event messages. It is not needed if you are using a Console cable.

`system support`

Dumps all tables. If you capture and send this output to Efficient Networks Technical Support, it can be useful in debugging problems. The information dumped includes the history log and information about the version, memory, processes, the file system, general system information, Ethernet, DHCP, Voice, remote database, interfaces, bridging, the ARP table, IP routes, IPX routes, IPX SAPs, L2TP tunnels, and IP filters.

`copy /RAW-IMAGE ttp@192.4.210.171:test`

Uses the special file name /RAW-IMAGE to copy all of FLASH memory to a backup file for system debugging.

ATM Debug Commands

`atom findPVC <on | off>`

Shows VPI*VCI of cells received. This important command can be used to find the ATM VPI*VCI number necessary for configuring a remote when the Service Provider either has supplied the wrong value or simply is not able to supply one. This command should only be used when there are *no* remotes defined or when the remote entries are disabled.

The command output is directed to the Console. If Telnet is used to log into the router, then issue the `systemlog start` command to direct the console output to the Telnet session.

Sample Output:

atom findPVC on
No remote entry found with PVC (VPI*VCI) 1*2

In this case, an ATM VPI*VCI is found for which there is no remote defined (1 is the number of the VPI as found in the ATM stream, 2 is the number of the VCI as found in the ATM stream). The discovered number may be used as the VPI*VCI value in the remote and allows you to determine whether communications are possible.

`atom echoPVC <vpi number>*<vci number>`

Enables an echo PVC (use `atom echo 0*21`). This is configured automatically and can be disabled with `atom echo 0*0`. The echoPVC will echo back any ATM cell received on the PVC exactly as received. This is useful when an administrative service wishes to ensure ATM connectivity, but cannot use ATM OAM F5 cells to achieve this function.

`atom pls <on | off>` Changes payload scrambling.

`atom empty <ATMF | ITU>`

Changes type of ATM empty cell sent or expected. It is useful if ATM sync delination errors when combined with atom stats command.

`atom dumpunknowncells [on | off]`

Looks at the content of an ATM cell. It will not affect normal router performance.

Web GUI Debug Commands

Using a browser pointed to the router's IP address, you can display special pages in the web GUI, such as:

`time.htm` Displays time.

`quick.htm` Displays all Easy Setup parameters.

`factory.htm` Resets all values to factory defaults.

`dump.htm` Shows all values.

SDSL Debug Commands

`sdsl *` Displays all available SDSL commands.

`sdsl btstat` Displays available status values.

Sample Output:
sdsl bts
Available status:
SLM .....……... Input Signal Level
DC_METER ....…….....Input DC Offset
FELM .....…….....Far-End Signal Attenuation (Cal'd at 1168 Kbs)
NMR .....……..... Noise Margin
TIMING_RECOVERY_CONTROL ..... Timing Recovery Control
STARTUP_STATUS .....……... Bit-Pump Status
BIT_PUMP_PRESENT .....……..... Bit-Pump Present
SELF_TEST .....…….. Self Test
REGISTER .....……..... Read Register
CONFIGURATION .....…….. Big-Pump Configuration
STAGE_NUMBER .....……. Stage Number
AAGC_VALUE .....…….. AAGC
READ_TX .....……..... Read Tx Gain
BER_METER_STATUS .....……..... BER Meter Status

`sdsl btstat *` Displays available SDSL status commands.

`sdsl bts felm`

Displays Far-End Signal Attenuation. It gives an estimate of the length of the loop.

Sample Output:
SDSL: FELM: 63 [0x3f]

`sdsl bts nmr`

Displays noise margin. Large values are symptoms of a bad or excessively lengthy loop.

Sample Output:
SDSL: NMR: 224 [0xe0]

`sdsl states trace [<all>]`

Turns on trace of line changes. To turn off the trace, append **all** to the command.

Sample Output:
sdsl states trace
SDSL State Trace [00000001]: states => s
sdsl states trace all
SDSL State Trace [00000000]: off

`sdsl huh` Dumps various registers.

Sample Output:

sdsl huh
SDSL:
Bitpump: 8973
CPE -- ACTIVATING
Line Rate: [AUTO] 192 Kb/s [3072 KHz]
Activation Interval: 99 [AUTO:20] [symbol_rate: 24]
AutoSpeed:
FastSearchAttemptsPerPass: 2
FastSearchPasses.....: 2
SlowSearchAttemptsPerPass: 5
SaveDelayInSeconds.....: 45
Two Symbol Time: 23 uS
FW: V4.3 CS 5: BR = 80000401 OR = fffff8f66
Ints -- On : 1228462 Mask: 0b00 IRQ: 02
BP Status Reads: 0
BT assumed on other end!
BT - Self Test will run
SDSL CONFIGURATION: 0x03f9 20 LOST: 10 [0x0a] Sym Rate: 24 [0x18]

Voice Router Debug Commands

Voice PVC Configuration

When using the Web GUI, be sure to verify the VPI/VCI or DLCI numbers for the data PVC connection. The VPI/VCI is automatically set to 0*39 for ATM routers and DLCI is set to 22 for Frame Relay routers. Some versions use 0*37 for voice.

Voice Features Currently Supported:

Jetstream and CopperCom gateways
Voice over ATM or Frame Relay
Upstream traffic shaping (bandwidth management) of data when voice is active
Automatic configuration of voice PVC
PCM voice encoding or ADPCM (compressed)
Local echo canceling (G.168)
AAL2 voice statistics

After the router WAN link activates (LINK light is green) you should get a dial tone, even if the IP and bridge network settings are not configured. If this fails, the DSLAM may not be configured for your voice PVC to the voice gateway.

You can use the WAN Port Monitor GUI program to see the voice PVC and the last event message. Each voice call takes about 80 Kb of bandwidth when the phone goes off hook.

Key Debug Commands

`ifs`	Shows if the data and Voice PCVs are configured and percent loading
`atom voice`	Displays the voice PVC (ATM routers)
`atom voice x*y`	Used to change the voice PVC (ATM routers)
`frame voice`	Displays the voice DLCI (Frame relay routers)
`frame voice x`	Used to set the DLCI for voice (Frame relay routers)
`sd stats`	Shows CRC and line errors for SDSL
`frame stats`	Shows LMI statistics (Frame relay routers)
`voice l2stats`	Shows AAL2 statistics to Voice gateway (Jetstream voice only)
`voice 12stats clear`	Resets values
`dsp <NOEC | ECON>`	Turns echo canceller on (ECON) or off (NOEC).

The following commands can be used for lab or bench verification of a standalone phone:

`ds init nobort` Starts DSP for this test.
`ds cas x` Connects and rings port x.
`ds ploop x-y` Connects port x to y.
`ds init` Reinitialize after testing.

For example, to connect port 1 to port 2, use this command sequence:

```
ds init nobort
ds cas 1
ds cas 2
ds ploop 1-2
```

A Class 5 switch via the voice gateway provides the actual dial tone and voice features to the phone set. Subscriptions to features such as call forwarding, caller ID, transfer, etc. are all supported. The Voice Provider sets the actual phone number for each port.

If you don't get a dial tone, it could be due to one of the following conditions:

- Router is powered off or lost power
- Local phone cord is not plugged in
- Voice PVC is not set in the router or is wrong
- WAN link is down (LINK light should be solid green)
- DSLAM is not provisioned for the second PVC
- Voice gateway is not connected or provisioned
- ATM network is down between the DSLAM and voice gateway

If you hear a surging sound, the gateway may be sending compressed data (ADPCM). Have the Service Provider change it to PCM. If you hear clicking during heavy data downloads, check that the DSLAM supports quality of service (QoS) and the ATM switch has the voice PVC provisioned for vRT with data at a lower priority. If you hear a 3-stage tone instead of a dial tone, the WAN link is down.

ADSL DMT Router Debug Commands

`dmt *`	Displays available commands
`dmt ver`	Displays code version of line driver
`dmt speed`	Displays speed link
`dmt ms`	Shows modem status

Frame Relay Debug Commands

`frame stats` Displays statistics

ATM Tracing Commands

`atom print` Shows a count of good and bad ATM cells and frames.

`atom rx <on | off>` Shows AAL5 frames received.

`atom promisc on` Turns on promiscuous mode (rx ATM cells no matter what VPI*VCI).

`atom cellrx <on | off>` Traces ATM cells received.

`atom tx <on | off>` Traces ATM cells sent.

`atom stats <n>` Prints the ATM statistics every *n* seconds. It shows good and bad cells and frames.

IP Filtering Debug Commands

The following commands can start and stop an IP filter watch:

```
eth ip filter watch <on | off>
remote ipfilter watch <on | off>
```

A message is displayed on the Console if a packet to or from the remote is dropped, rejected, or verbose.

Line Speed Problems

Problem: The customer is getting 200 Kbps performance when paying for a 1.1 Mbps line.

The problem could be any of the following:

1) the DSL line
2) LAN activity
3) local client PC (hardware or software)
4) Internet traffic
5) LAN server (hardware or software)

Solution: The entire data path must be examined to find the bottleneck.

1) Always start with router configuration. Issue command `system support`.

2) Next, you must try to divide the data path into pieces to determine the location of the bottleneck(s). You might start with the following:

- Ask the ISP to try to get a very large file. The goal is to go up the line to see if the performance problem is between the server containing the large file and the ISP.

- Ask the ISP to set up a file server. Have the customer try to get files from this file server and monitor the performance. If the customer can get a good speed from this file server, a bottleneck exists between the customer's server and the ISP.

If the customer can connect the client PC directly to the router, the customer can help rule out any local LAN problems.

Status Messages

The router offers a few commands that will reveal status and performance. Use the command `ifs` to display the link status. When all the interfaces show a status of opened, you have a good connection to the DSLAM

Interface	Speed	In %	Out %	Protocol	State	Connection
ETHERNET/0	10.0mb	0%/0%	0%/0%	(Ethernet)	OPENED	
FR/3	128kb	0%/0%	0%/0%	(HDLC/FR)	STANDBY	
FR-VC/1	0 b			(FR)	OUT-OF-SERVICE	
CONSOLE/0	9600 b	0%/0%	0%/0%	(TTY)	OPENED	

Remote Stats

The command `remote stats` will provide the following information:

STATISTICS FOR <test>:
Current state..... not connected
Current output bandwidth..... 0 bps
Current input bandwidth..... 0 bps
Current bandwidth allocated..... 0 bps
Total connect time..... 0+00:00:00
Total bytes out..... 0
Total bytes in..... 0

The command `remote stats clear` will reset all the numbers.

xDSL Stats

The command `sdsl stats` or `adsl stats` will produce the following.

Statistics:
Framer Interrupts..... 0 Framer error "out of sync"
Out of frame errors.... 0 Can't determine start/end of packet
HEC errors received.... 0 Header Error Correction
CRC errors received.... 0 Cyclic Redundancy Check
FEBE errors received... 0 Far End Bit Errors
Remote Out-of-frame.... 0 Far end can't determine start/end of packet
Remote HEC errors..... 0 Far end HEC error

The command `sdsl stats clear` or `sdsl stats clear` will reset the counter.

Display PVC

A classic DSL failure is when a customer can sync to the DSLAM and not ping the gateway. Check the state of the interfaces, then ping the WAN gateway. If you get no reply, the command below will tell you the PVC that is being used.

```
atom dumpunknowncells [on:off]
```

Compare this to the PVC configured using the command `remote list.`

Once the router has `atom dumpunknowncells on`, someone from the Internet must ping the router's WAN address. This command will produce the following output that indicates PVC settings. In this example, 8*35 is the correct VPI/VCI. These numbers were originally entered using the `remote set pvc` command.

ATOM DUMPUNKNOWNCELLS ON
Atom unknown cell tracing is ON
Atom promisc cell receive is ON
ARP: never found 216.101.252.254
No remote entry found with PVC (VPI*VCI) 8*35
00800231 AAAA0300 80C20007 00000020
7812D497 00106700 1C350800 4500003C
B8B20000 1601420D D11F042D D865FC4F 080015D2

Password Bypass

DIP Switch Routers

IDSL and some DSL routers have 6 DIP switches on their back panels. By positioning switches 5 and 6 down, you can bypass an unknown password, using the original default password of `admin.` You may then set another password using the `command system admin <new password>`. Be sure to set switches 5 and 6 up before you reboot the router, otherwise, it will boot to the boot screen and not function from a customer perspective.

Reset Pin Routers

For routers with the reset button on the rear panel and no DIP switches, you must push the button and hold it for 5 seconds until the TEST light turns amber. At that time, the router will accept the 6 numbers from the serial number label as the password. The router will not need to be rebooted after you have logged on, and the light will change back to green in a few minutes.

Other issues

1. Once you activate the reset pin on a router, you will also need to activate the router's DHCP server.

2. If a customer reboots a DIP switch router with all six switches down, it will boot to the boot menu. Advise them to set switches 5 and 6 up, then reboot the router to recover.

3. Routers will timeout a Telnet or SNMP session in 5 minutes. If you wish to extend this time, use the command `system securitytimer <minutes>.`

Upgrading Routers Using a GUI

STEP 1: Download the upgrade file (kernel) from our website support page. Place the file in the same location as other software files, e.g., C:\DSL

STEP 2: Start the Configuration Manager"program

Click [Start] [Programs] [DSL tools] Configuration Manager
Click [Connect]
Enter the router's Ethernet IP address
Click [OK]
Enter your login password (default is `admin`)
Click [Login]
Click on [Tools]
Click on [Upgrade/backup]
Select "firmware"
Click on [Upgrade]

When asked which file to use, select the new one that you downloaded.

When the upgrade is complete, you will be asked to reboot the router. Click [OK]

The reboot will take about 30 seconds and you will be asked for a login password. At this point, you are done. Verify that there is a new software version number in the top right-hand corner of the Configuration Manager screen.

Changing the Date and Time on Routers

Routers with software version 3.8.0 or newer can have the time and date changed to match the settings of a PC connected to it. Launch Configuration Manager and click on "store" to allow the router to reboot.

The Configuration Manager will use the time and date settings of the PC to update the router. The time and date settings of the router can be verified with the Telnet command `system list.`

Corrupted Kernel

When a router is upgraded using an incorrect kernel file, its kernel may become corrupted. For example, a router with kernel v.2.6.4 or higher must have a minimum boot file v.2.1.0, otherwise, it will not work and will boot to a screen with 8 options.

To fix the router, you will need a Console cable with adapter, correct kernel file, and a TFTP server (see DSL Tools directory). You must upgrade via a Console connection since the router's Ethernet connection cannot function in this situation.

To repair mismatched kernel and boot files, the boot must be upgraded first, followed by a kernel upgrade.

Repairing the Boot

1. Reboot the router
2. Open the TFTP server and confirm that the kernel file is in the TFTP root directory.
3. Open the Console connection and choose Option 4 (Boot from specific file).
4. Enter the server's IP address, router IP address and file name -- don't change the boot location.
5. The router should be working now, but will not have a good copy of the kernel loaded on its FLASH yet. Issue the copy command below, were the workstation IP address is the server IP and the source file name is that of the file existing on the C: drive. This name must not be the same as the destination file name. The destination file name for IDSL routers is `kernel.fp1` and for other DSL routers is `kernel.f2k.`

   ```
   copy tftp@<servers ip addr>:<sourcefile> <destination file>
   copy tftp@192.168.254.2:newkernel.128 kernel.f2k
   ```

6. Type `save` and `reboot` to store the changes.

Repairing the Kernel

Routers with DIP Switches

1. Set the DIP switches on the back of the router to 1,2,3,4,6 down and 5 up.
2. Reboot the router
3. Open the TFTP server and confirm that the kernel file is in the TFTP root directory.
4. Open the Console connection and choose Option 4 (Boot from specific file).
5. Enter the server's IP address, router IP address and file name -- don't change the boot location.
6. Reset DIP switches to (1,2,3,4 down & 5,6 up).
7. Copy and save the file to the router:

   ```
   copy tftp@serveripaddr:kernel.xxx kernel.xxx
   ```

(The destination file name for IDSL routers is `kernel.fp1` and for other DSL routers is `kernel.f2k`)

8. Type `save` then `reboot` to finish repairing the kernel.

Routers without DIP Switches

You will need an instrument to press against the recessed button on the back of the router while it is booting up. After the router flashes all of its lights, release the button and the router will send a request for the BootP server. Be sure that the BootP server has a path specified to retrieve a working kernel. If you're running Configuration Manager v3.8.0, click TOOLS, then BOOTP SETTINGS. This will allow you to recover from a corrupt kernel.

Feature Activation Keys

There are 2 kinds of feature upgrade keys. For kernels before v.3.6.0, software options have to be installed by booting the router on the LAN from a special file.

Possible feature upgrades include: FRAME RELAY, SDSL, RFC1490, +IP ROUTING, IP FILTERING, WEB, ~L2TP, ~ENCRYPT, BRIDGE, IPX, CMMGMT

For routers 3.6.0 and higher, the bridge function is controlled by the presence of a key file in FLASH or a bit set in CMOS. Both values are checked and if either flag says "route", you get routing.

The `version` command will show:

- ~ if a feature is disabled
- + if enabled by a key file
- no prefix if enabled

Software options can be added by purchasing a key (string of numbers) from Efficient Networks. This string is added to the router with the `key add <string>` command via Console or Telnet.

A key can also be added via the web GUI by selecting the Upgrade Features button and entering a 44-character key. Any angle brackets, e.g. < >, are stripped.

Key files have the format "123456.ext", where "123456" is the serial number of the router that is to be upgraded, and ".ext" indicates the feature that is to be activated (.l2t = L2TP, .des = Encryption, .flt = IP Filtering).

The following instructions describe how to activate features within the router's kernel using upgrade keys:

STEP 1
After purchasing and downloading key file(s), save in an empty directory on the PC that is being used to perform the upgrade.

STEP 2
From your PC desktop, click Start /Programs/DSL Tools/Quick Start.

Note: If Quick Start is not able to connect to your router, you will be prompted with a message "Do you want to quit?" If you get this message, click on "NO" and enter the IP address of your router. Click "OK" to connect.

STEP 3
If you are prompted with the "Login" dialog box, enter your password and click "Login".
If you are prompted with a "Change login password" dialog box, click "Cancel".

STEP 4
Select the "Tools" menu.
Select "REBOOT FROM THE NETWORK" (Ctrl+ N).

WARNING: DO NOT USE THE "UPGRADE / BACKUP" FUNCTION TO PERFORM FEATURE ACTIVATION because it will corrupt the router's operating system files!!

When prompted: "Are willing to discard your changes?" Select "YES".

STEP 5
The "Select the file to boot from" dialog box will appear. Select the Activation File that matches the Serial Number on your router. Click OK.

"Rebooting from the network" will appear. This process will take about 90 seconds --***DO NOT CANCEL THIS PROCESS !!***

STEP 6
If you are prompted with the "Login" dialog, enter your password and click "Login".
Or if you are prompted with a "Change login password" dialog, click "Cancel".

If you are installing more than one feature, repeat Steps 1-5 for each additional feature.

Use the file <serial #>.des for the Encryption feature
Use the file <serial #>.l2t for the VPN feature
Use the file <serial #>.ipf for the IP Filtering Firewall feature

STEP 7
Check your router firmware version to see if it supports the features that you have just activated:
- Start the Quick Start program.
- Look for the "Software" version in the top right-hand corner of the Quick Start screen.

If your Firmware version is 3.0.2 or higher, then you are not required to upgrade your firmware. If your Firmware version is below 3.0.2 then you need to upgrade your router firmware in order to use the new features.

Downgrading to a Bridge

Some customers may order routers and field downgrade them to bridges. They can do this by deleting the keyfile.dat file in FLASH and then rebooting. Note that a downgrade won't work if IP routing is set in CMOS FLASH.