CHAPTER 3

Advanced Data-Only Configurations

This chapter describes how to configure the Cisco uBR924 cable access router for data operation with features beyond those supported in the default operation mode of "plug and play" DOCSIS bridging. The following configurations are described:

- Data-Only Routing, page 3-2
- Routing with DHCP Server, page 3-4
- NAT/PAT Configuration, page 3-6
- NAT/PAT Configuration with DHCP Proxy, page 3-8
- IPSec (56-bit) Example, page 3-11
- IPSec (3DES) Example, page 3-16
- L2TP Example, page 3-17

Depending on the Cisco IOS software image being used and the feature sets it supports, these configurations could be combined.

Tip Use the commands shown in this chapter to set up a typical Cisco uBR924 router for the desired feature. Then save the configuration into a configuration file that can be downloaded to the router during power-on or reset.

Caution Incorrectly configuring the Cisco uBR924 cable access router can cause loss of network connectivity. Before attempting to reconfigure the router, print the last working configuration, and ensure remote configuration is enabled for the site.

If the router does not connect to the network after you have reconfigured it, enter the cable downstream saved frequency from the printout, and then clear the interface. Power off and then power on the router.

If powering off the router does not correct the problem after a few minutes, give the **write erase** and **copy startup-config running-config** commands; then enter the correct saved downstream frequency. If network connectivity is not restored, contact your network management, provisioning, or billing system administrator to reload the software applicable to your network.

For an explanation of any error message that appears on the uBR924, please see the book, *Cisco Cable CPE Error Messages,* which is viewable online at www.cisco.com/univercd/cc/td/doc/product/cable/cab_modm/ubcmerrs.pdf

Data-Only Routing

The Cisco uBR924 router must be configured for routing mode to use advanced features such as IPSec encryption and firewall protection. The routing mode is also required if the PCs attached to the Cisco uBR924 router are on a private network or on a different subnet than the subnet used by the CMTS.

The following steps are required to configure the routing mode on the Cisco uBR924 router:

- Disable DOCSIS-compliant bridging on the cable interface with the **no cable modem compliant bridge** interface command.
- Remove the bridge group on the cable and Ethernet interfaces with the **no bridge group** interface command.
- Configure the RIPv2 routing protocol (or static routes) on the cable and Ethernet interfaces.

To configure the Cisco uBR924 router, log in to the router, enter global configuration mode, and enter the following commands:

	Command	Purpose
Step 1	uBR924(config)#**int c 0**	Enter interface configuration mode for the cable interface.
Step 2	uBR924(config-if)# **no cable-modem compliant bridge**	Disable DOCSIS-compliant bridging.
Step 3	uBR924(config-if)# **no bridge group** *number*	Remove the bridge group.
Step 4	uBR924(config-if)# **ip address dhcp**	Configure the cable interface to receive an IP address from the DHCP server.
Step 5	uBR924(config-if)# **exit**	Return to global configuration mode.
Step 6	uBR924(config)#**int e 0**	Enter interface configuration mode for Ethernet 0.
Step 7	uBR924(config-if)# **no bridge group** *number*	Remove the bridge group.
Step 8	uBR924(config-if)# **ip address** *ip-address subnet-mask*	Enter the Ethernet interface's IP address and subnet mask.
Step 9	uBR924(config-if)# **exit**	Return to global configuration mode.
Step 10	uBR924(config)# **ip routing**	Enable IP routing for the router.
Step 11	**To use RIPv2:**	
	uBR924(config)#**router rip**	Enter router configuration mode.
	uBR924(config-router)# **version 2**	Enable RIP version 2 routing.
	uBR924(config-router)# **network** *cable-network-number*	Enable routing on the cable interface's IP network.
	uBR924(config-router)# **network** *Ethernet-network-number*	Enable routing on the Ethernet interface's IP network.
	uBR924(config-router)# **exit**	Return to global configuration mode.
Step 12	uBR924(config)# **no cdp run**	(Optional) Disable the Cisco Discovery Protocol (CDP) on the router. CDP is a proprietary protocol for the discovery of Cisco routers running protocols other than TCP/IP; because DOCSIS cable data networks are primarily TCP/IP networks, CDP is not necessary on the Cisco uBR924 router.
Step 13	uBR924(config)# **ip default-gateway** *ip-address*	Set the default gateway for routing (typically, this is the CMTS).

	Command	Purpose
Step 14	uBR924(config)# **ip classless**	(Optional) Enable the forwarding of packets that are destined for unrecognized subnets to the best supernet route.
Step 15	uBR924(config)# **ip route 0.0.0.0 0.0.0.0** *ip-address*	(Optional) Establish a static route so that all packets without an established route are forwarded to the default gateway (typically the *ip-address* should be the IP address for the CMTS), regardless of any routing metrics.
Step 16	uBR924(config-if)# **Ctrl-z**	Return to privileged EXEC mode.
Step 17	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 18	uBR924# **show startup-config**	Display the configuration file that was just created.
Step 19	uBR924# **reload**	Resets the router and cable interface to enable IP routing mode.

To verify that routing is enabled, enter the **show startup-config** command. The following example shows a sample configuration file for basic data-only routing mode; the relevant commands are shown in bold.

```
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
clock timezone - 4
ip subnet-zero
!
voice-port 0
!
voice-port 1
!
interface Ethernet0
 ip address 172.16.0.1 255.255.0.0
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
 no cable-modem compliant bridge
!
 router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
!
ip classless
no ip http server
no service finger
!
!
line con 0
 transport input none
line vty 0 4
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

Routing with DHCP Server

When in routing mode, the Cisco uBR924 router can act as a DHCP server for the CPE devices it is connecting to the cable network. A service provider then does not have to be concerned about providing IP addresses to all of the PCs at a subscriber's site; instead, the provider supplies a pool of IP addresses that the Cisco uBR924 router then allocates to the PCs as needed.

Note The Cisco uBR924 router must be configured for routing mode to act as a DHCP server. If in bridging mode, you can configure the router to proxy DHCP client requests to the DHCP server at the headend by giving the **cable helper-address** *dhcp-server-ip-address* **host** interface configuration command. (The **ip helper-address** and **ip forward-protocol** interface configuration commands can also be used for this purpose.)

To configure the Cisco uBR924 router to act as a DHCP server, log in to the router, enter global configuration mode, and enter the following commands:

	Command	Purpose
Step 1	uBR924(config)# **ip dhcp pool** *pool-name*	Create an address pool for the DHCP server named *pool-name* and enter DHCP configuration mode.
Step 2	uBR924(config-dhcp)# **network** *IP-network-number subnet-mask*	Specify the network number and subnet mask for the IP address pool. These IP addresses should be part of the subnet provided by the CMTS cable interface. For example, **network 10.17.91.0 255.255.255.0** reserves the IP addresses 10.17.91.1–10.17.91.254 for CPE devices.
Step 3	uBR924(config-dhcp)# **domain-name** *domain-name*	The domain name that should be assigned to CPE devices (for example, **cisco.com**).
Step 4	uBR924(config-dhcp)# **dns-server** *ip-address*	The IP address for the DNS server provided by the service provider that will service the DNS requests from the CPE devices. More than one DNS server can be specified.
Step 5	uBR924(config-dhcp)# **default-router** *ip-address*	The IP address for the default router for the CPE devices (typically, this is the CMTS). More than one default router can be specified.
Step 6	uBR924(config-dhcp)# **exit**	Return to global configuration mode.
Step 7	uBR924# **show startup-config**	Display the configuration file that was just created.

To verify that the DHCP server is enabled, enter the **show startup-config** command. A sample configuration file for a Cisco uBR924 router acting as a DHCP server is shown below. The relevant commands are shown in bold.

```
version 12.1
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
clock timezone - 4
ip subnet-zero
!
ip dhcp pool Clients
 network 192.168.100.0 255.255.255.0
 domain-name cisco.com
 dns-server 192.168.100.17
 default-router 192.168.101.1
!
voice-port 0
!
voice-port 1
!
interface Ethernet0
 ip address 192.168.100.1 255.255.0.0
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 ip rip send version 2
 ip rip receive version 2
 no cable-modem compliant bridge
!
 router rip
 version 2
 network 10.0.0.0
 network 192.168.100.0
!
ip classless
no ip http server
no service finger
!
!
line con 0
 transport input none
line vty 0 4
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

NAT/PAT Configuration

When using a Cisco IOS image that supports the Easy IP feature, the Cisco uBR924 router supports Network Address Translation (NAT) and Port Address Translation (PAT). This allows a private network that is connected to the router to use the same IP address when communicating through the cable interface to the Internet or other public networks.

When NAT/PAT are enabled on the cable access router, the "inside" network is the private network connected to the router's Ethernet interface, and the "outside" network is the network accessed through the cable network (such as the Internet or a company's larger network). Each inside address is typically an IP address in the RFC1918 private network space (10.0.0.0, 172.16.0.0, and 192.168.100.0) and is translated to an external IP address that is valid in the outside network.

Note NAT/PAT can be used only in routing mode.

The following commands show a typical configuration. (These steps assume that the router has already been configured for routing mode, as described in "Data-Only Routing" section on page 3-2.)

	Command	Purpose
Step 1	uBR924(config)# **ip nat inside source list** *list-id* **interface cable-modem0 overload**	Enable translation of the inside source addresses—the "inside" addresses are translated before being presented to the "outside" network. The *list-id* specifies an access-list that defines the IP addresses that will be used, and **overload** specifies that multiple inside IP addresses can use the same outside IP address (but using different port numbers to unique identify each inside host).
Step 2	uBR924(config)# **interface Ethernet0**	Enter interface configuration mode for the router's Ethernet interface.
Step 3	uBR924(config-if)# **ip nat inside**	Specify that the Ethernet is the "inside" of the NAT/PAT translation.
Step 4	uBR924(config-if)# **exit**	Exit interface configuration mode.
Step 5	uBR924(config)# **interface cable-modem0**	Enter interface configuration mode for the router's cable interface.
Step 6	uBR924(config-if)# **ip nat outside**	Specify that the cable interface is the "outside" of the NAT/PAT translation.
Step 7	uBR924(config-if)# **exit**	Exit interface configuration mode.
Step 8	uBR924(config)# **access-list** *list-id* **permit** *address mask*	Creates the access list specified by the *list-id* parameter in the **ip nat inside source** command. The address and mask values should specify IP addresses that belong to the private IP network space being used by the Ethernet interface.
Step 9	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 10	uBR924# **show startup-config**	Display the configuration file that was just created.

Note Additional options, such as static IP address translation, are possible when using NAT/PAT. For more information about the Easy IP and NAT/PAT feature set, see the *Dial-Related Addressing Services* documentation, available on CCO and the Documentation CD-ROM.

The following configuration shows an example of a Cisco uBR924 router in routing mode that performs NAT/PAT translation on all IP addresses connected to the router’s Ethernet interface. The external IP address is overloaded so that multiple IP addresses on the internal network can use the same external IP address over the cable interface; different port numbers are used to uniquely identify each device on the Ethernet interface. The relevant commands are shown in bold.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname uBR924
!
!
ip nat inside source list 1 interface cable-modem0 overload
clock timezone - -4
!
!
interface Ethernet0
 ip address 192.168.1.1. 255.255.255.0
 ip nat inside
!
interface cable-modem0
 ip nat outside
 no cable-modem compliant bridge
!
ip routing
ip default-gateway 10.1.1.1
ip classless
no ip http server
no service finger
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
line con 0
line vty 0 4
 login
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class C private network (192.168.100.0).

NAT/PAT Configuration with DHCP Proxy

The NAT/PAT feature can also be used with the **cable-modem dhcp-proxy nat** command, so that the router obtains the IP address used for the NAT pool for the Ethernet interface from the DHCP server. This allows the service provider to dynamically provide this IP address in the same manner as for the cable interface.

In addition to using the the **cable-modem dhcp-proxy nat** command, you must also use the following NAT configuration commands:

- Use the **ip nat inside** interface command to configure the Ethernet interface as the "inside" interface.
- Use the **ip nat outside** interface command to configure the cable interface as the "outside" interface.
- Specify the **overload** option with the **ip nat** global configuration command because the NAT pool created by the **cable-modem dhcp-proxy** command contains only one IP address.

The following commands show a typical configuration. (These steps assume that the router has already been configured for routing mode, as described in "Data-Only Routing" section on page 3-2.)

	Command	Purpose
Step 1	UBR924(config)# **ip nat inside source list** *list-id* **interface cable-modem0 overload**	Enables translation of the inside source addresses—the "inside" addresses are translated before being presented to the "outside" network. The *list-id* specifies an access-list that defines the IP addresses that will be used, and **overload** specifies that multiple inside IP addresses can use the same outside IP address (but using different port numbers to unique identify each inside host).
Step 2	UBR924(config)# **interface Ethernet0**	Enters interface configuration mode for the router's Ethernet interface.
Step 3	UBR924(config-if)# **ip nat inside**	Specifies that the Ethernet is the "inside" of the NAT/PAT translation.
Step 4	UBR924(config-if)# **exit**	Exits interface configuration mode.
Step 5	UBR924(config)# **interface cable-modem0**	Enters interface configuration mode for the router's cable interface.
Step 6	UBR924(config-if)# **cable-modem dhcp-proxy nat** *pool-name*	Specifies the name of the NAT pool to be created using the IP address and subnet mask supplied by the DHCP server. The *pool-name* can be any arbitrary string. **Note** This is equivalent to giving the **ip nat pool** command, using the IP address and subnet mask supplied by the DHCP server.
Step 7	UBR924(config-if)# **ip nat outside**	Specifies that the cable interface is the "outside" of the NAT/PAT translation.
Step 8	UBR924(config-if)# **exit**	Exits interface configuration mode.

	Command	Purpose
Step 9	UBR924(config)# **access-list** *list-id* **permit** *address mask*	Creates the access list specified by the *list-id* parameter in the **ip nat inside source** command. The address and mask values should specify IP addresses that belong to the private IP network space being used by the Ethernet interface.
Step 10	UBR924# **copy running-config startup-config**	Saves the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 11	UBR924# **show startup-config**	Displays the configuration file that was just created.

Note For more information about the Easy IP and NAT/PAT feature set, see the *Dial-Related Addressing Services* documentation, available on Cisco.com and the Documentation CD-ROM.

The following configuration for the Cisco uBR924 cable access router shows an example of a cable access router in routing mode that performs NAT/PAT translation using the DHCP proxy to obtain its NAT address pool. The relevant commands are shown in bold.

Note Do not enter the **ip nat pool** command manually. The router automatically generates this command when it obtains the NAT address pool from the DHCP server.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
ip nat inside source list 1 interface cable-modem0 overload
clock timezone - -4
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
interface cable-modem0
 ip nat outside
 no cable-modem compliant bridge
 cable-modem dhcp-proxy nat nat-pool
!
ip routing
ip default-gateway 10.1.1.1
! The following command is automatically added when the router obtains
!  the DHCP-provided IP addresses for the NAT pool
ip nat pool nat-pool 10.15.0.10 10.15.0.10 netmask 255.255.0.0
! The following command must be manually entered
ip nat inside source list 1 pool nat-pool overload
ip classless
no ip http server
no service finger
ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

```
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
line con 0
line vty 0 4
 login
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class C private network (192.168.0.0).

Using NAT and DHCP Proxy and Copying Configuration Files

Most service providers typically create a standard configuration file for their cable modems, verify it, and then copy the working configuration as needed to other cable modems. This can cause problems with Cisco uBR924 cable access router when using the **cable-modem dhcp-proxy** command to create a NAT address pool for NAT/PAT translation.

The reason is that the default router configuration is for DOCSIS-compliant bridging, which includes two **bridge-group 59** commands for each interface. To use the **cable-modem dhcp-proxy** command, you must put the router into routing mode, which means removing the **bridge-group** commands with the equivalent **no bridge-group** commands.

However, because **no bridge-group** is the default for these CLI commands, they are not saved in the running configuration. So when you save the Cisco IOS configuration file and copy it to other Cisco uBR924 cable access router, the router is only partially configured for routing mode and continually resets its interfaces.

In addition, whenever you use the **cable-modem dhcp-proxy** command to create a NAT pool, the router automatically adds the appropriate **ip nat pool** commands to the configuration when it receives the actual IP addresses from the DHCP server. The IP addresses specified in this command are particular to each user and should not be copied to other routers.

To avoid this problem, use the following procedure to create a Cisco IOS configuration file that uses the **cable-modem dhcp-proxy** command to create a NAT address pool for NAT/PAT address translation:

Step 1 Create and test a working configuration on a Cisco uBR924 cable access router.

Step 2 After you have created a standardized configuration, save it to memory, and then copy the Cisco IOS configuration file to the TFTP server that will be used to copy the file to the other cable access routers.

Step 3 Open the Cisco IOS configuration file with a text editor and add the following lines underneath each interface:

```
no bridge-group 59
no bridge-group 59 spanning-disabled
```

Step 4 Remove the **ip nat pool** command.

For example, the following are the relevant lines in a typical DHCP proxy NAT configuration for the Cisco uBR924 cable access router:

```
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 load-interval 30
!
interface cable-modem0
 ip nat outside
 load-interval 30
 no cable-modem compliant bridge
 cable-modem dhcp-proxy nat nat-pool
!
ip nat pool nat-pool 10.15.0.10 10.15.0.10 netmask 255.255.0.0
```

When you copy this configuration file to the TFTP server, modify this portion of the configuration file to add the **no bridge-group** commands under each interface and to remove the **ip nat pool** command:

```
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 load-interval 30
 no bridge-group 59
 no bridge-group 59 spanning-disabled
!
interface cable-modem0
 ip nat outside
 load-interval 30
 no cable-modem compliant bridge
 cable-modem dhcp-proxy nat nat-pool
 no bridge-group 59
 no bridge-group 59 spanning-disabled
!
```

Note Be sure to remove the **ip nat pool** command.

IPSec (56-bit) Example

IPSec encryption provides end-to-end encryption of IP traffic across unprotected public networks such as the Internet. To use IPSec, the Cisco uBR924 cable access router must meet the following prerequisites:

- The Cisco uBR924 router must be using a Cisco IOS Release 12.0(5)T or higher image that supports the IPSec feature set.
- The Cisco uBR924 router must be configured for routing mode.
- The Cisco uBR924 router and endpoint must both support IPSec encryption and be configured for the same encryption policy. (The endpoint is typically an IPSec gateway such as a peer router, PIX firewall, or other device that can be configured for IPSec.)

Note Images that support encryption are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States may require an export license. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Note Cisco IOS Release 12.1(5)T, 12.2(2), or greater is required to support GRE IP tunnels.

The configuration of the Cisco uBR924 router for IPSec encryption depends on the application involved, such as whether the IPSec encryption is part of a virtual private network (VPN) and whether the Cisco uBR924 router should encrypt traffic to one or more than one peer end-point. A technique that would work well for a small network might not scale well for a large network—for example, using pre-shared authentication keys works for networks of up to 10 or so nodes, but larger networks should use RSA public key signatures and digital certificates.

Note For more information about IPSec, as well as related topics such as Internet Key Exchange (IKE), Internet Security Association Key Management Protocol/Oakley variation (ISAKMP/Oakley), and digital certificates, see the "Additional Documentation" section on page 3-15.

The following shows the commands needed to configure the Cisco uBR924 router for IPSec encryption with one peer router, using pre-shared keys.

	Command	Purpose
Step 1	uBR924(config)# **crypto isakmp enable**	Enable the use of ISAKMP/IKE on the Cisco uBR924 router.
Step 2	uBR924(config)# **crypto isakmp policy** *priority-number*	Creates an IKE policy with the specified priority-number (1–10000, where 1 is the highest priority) and enters ISAKMP policy configuration command mode.
Step 3	uBR924(config-isakmp)# **encryption des**	Specifies that 56-bit DES encryption be used. to encrypt the data.
Step 4	uBR924(config-isakmp)# **hash md5**	Specifies the MD5 (HMAC variant) hash algorithm for packet authentication.
Step 5	ubr924(config-isakmp)# **group 1**	Specifies the 768-bit Diffie-Hellman group for key negotiation.
Step 6	uBR924(config-isakmp)# **authentication pre-share**	Specifies that the authentication keys are pre-shared, as opposed to dynamically negotiated using RSA public key signatures.
Step 7	uBR924(config-isakmp)# **lifetime** *seconds*	Defines how long each security association should exist before expiring (60 seconds to 86,400 seconds).
Step 8	uBR924(config-isakmp)# **exit**	Exits ISAKMP policy configuration command mode.
Step 9	uBR924(config)# **crypto isakmp key** *shared-key* **address** *ip-address*	Specifies the pre-shared key that should be used with the peer at the specific IP address. The key can be any arbitrary alphanumeric key up to 128 characters long—the key is case-sensitive and must be entered identically on both routers. **Note** You can also specify a pre-shared key using the **crypto key public-chain dss** command. See the description of this command in the *Cisco Encryption Technology Commands* document, available on CCO and the Documentation CD-ROM.

	Command	Purpose
Step 10	uBR924(config)# **crypto isakmp identity hostname**	Sets the ISAKMP identity of the router to its host name concatenated with the domain name (for example, **ubr924.cisco.com**).
Step 11	uBR924(config)# **crypto ipsec transform-set** *transform-set-name transform1 transform2 transform3*	Establishes the transform set to be used for IPSec encryption. Up to three transformations can be specified for a set, such as **ah-md5-hmac esp-des esp-md5-hmac**.
Step 12	uBR924(config)# **crypto map** *crypto-map-name* **local-address cable-modem0**	Creates the specified crypto map and applies it to the cable interface.
Step 13	uBR924(config)# **crypto map** *crypto-map-name* **10 ipsec-isakmp**	Creates a crypto map numbered 10 and enters the crypto map configuration mode.
Step 14	uBR924(config-crypto)# **set peer** *ip-address*	Identifies the IP address for the destination peer router.
Step 15	uBR924(config-crypto)# **set transform**-set *transform-set-name*	Sets the crypto map to use the transform set created previously.
Step 16	uBR924(config-crypto)# **match address** *access-list-number*	Sets the crypto map to use the access list that will specify the type of traffic to be encrypted. **Note** Access lists 100 and 101 cannot be used because they are reserved for DOCSIS use.
Step 17	uBR924(config-crypto)# **exit**	Exits crypto map configuration mode.
Step 18	uBR924(config)# **int c 0**	Enters interface configuration mode for the cable interface.
Step 19	uBR924 (config-if)# **crypto map** *crypto-map-name*	Applies the crypto map created above to the cable interface.
Step 20	uBR924 (config-if)# **access-list** *access-list-number* **permit ip host** *ubr924-ip-address peer-ip-address filter-mask*	Creates an access list to identify the traffic that will be encrypted. (This should match the access list created above.)
Step 21	uBR924(config-if)# **Ctrl-z**	Return to privileged EXEC mode.
Step 22	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 23	uBR924# **show startup-config**	Display the configuration file that was just created.

Note To enable IPSec encryption, the peer router must also be configured for IPSec encryption, using the identical parameters used on the Cisco uBR924 router.

Sample Configuration

The following configuration shows a typical IPSec configuration with the following parameters:

- The IKE policy is defined as policy priority 1 with the following parameters:

  - 56-bit DES-CBC encryption (the default)
  - MD5 (HMAC variant) hash algorithm
  - Pre-shared authentication keys
  - 768-bit Diffie-Hellman group (the default)
  - Security association lifetime of 5,000 seconds (approximately 83 minutes).
- The pre-shared key has the value 1234567890 (normally keys would be much more complex than this simple example)
- IPSec encryption is being done on traffic sent from the cable interface on the Cisco uBR924 router (at IP address 10.1.0.25).
- One single peer is defined—the router at IP address 30.1.1.1.
- IPSec encryption is applied to all traffic that matches the contents of access list 200.

IPSec-related commands are shown in bold.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
clock timezone - 0 6
ip subnet-zero
no ip domain-lookup
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 5000
crypto isakmp key 1234567890 address 30.1.1.1
crypto isakmp identity hostname
!
crypto ipsec transform-set test-transform ah-md5-hmac esp-des esp-md5-hmac
!
 crypto map test-ipsec local-address cable-modem0
 crypto map test-ipsec 10 ipsec-isakmp
 set peer 30.1.1.1
 set transform-set test-transform
 match address 200
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 no keepalive
 no cable-modem compliant bridge
 crypto map test-ipsec
router rip
 version 2
 network 10.0.0.0
 network 192.168.100.0
!
ip classless
no ip http server
no service finger
!
access-list 200 permit ip host 10.1.0.25 30.1.1.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 login
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

Additional Documentation

Establishing IPSec encryption between two or more end-points requires a thorough understanding of the Internet Key Exchange (IKE) mechanism, which is a form of the ISAKMP/Oakley (Internet Security Association Key Management Protocol) that is used for IPSec encryption. Digital certificates must also be understood if this mechanism is going to be used for authentication. Finally, if IPSec will be used as part of a virtual private network (VPN), those concepts must be understood as well.

For general information on these subjects, see the following information in the product literature and IP technical tips sections on CCO:

- *Deploying IPSec*—Provides an overview of IPSec encryption and its key concepts, along with sample configurations. Also provides a link to many other documents on related topics.
- *Certificate Authority Support for IPSec Overview*—Describes the concept of digital certificates and how they are used to authenticate IPSec users.
- *An Introduction to IP Security (IPSec) Encryption*—Provides a step-by-step description of how to configure IPSec encryption.

The following technical documents, available on CCO and the Documentation CD-ROM, also provide more in-depth configuration information:

- *Cisco IOS Release 12.1 Security Configuration Guide*—Provides an overview of Cisco IOS security features.
- *Cisco IOS Release 12.0 Security Command Reference*—Provides a reference for each of the Cisco IOS commands used to configure IPSec encryption and related security features.
- *Cisco IOS Software Release 12.1 Command Summary*—Summarizes the Cisco IOS commands used to configure all Release 12.0 security features.

Note Additional documentation on IPSec becomes available on CCO and the Documentation CD-ROM as new features and platforms are added.

IPSec (3DES) Example

The IPSec 3DES encryption feature set is identical to the IPSec encryption feature set except that it supports the 168-bit Triple DES (3DES) standard in addition to the standard 56-bit IPSec encryption. The 168-bit encryption feature set requires a Cisco IOS image that supports it and provides a level of security suitable for highly sensitive and confidential information such as financial transactions and medical records.

Note Cisco IOS images with strong encryption (including, but not limited to, 168-bit [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States may require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, the purchaser or user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Configuration for 3DES encryption is identical to that for standard IPSec, except that the transformation set should specify **esp-3des** instead of **esp-des**. For example, the following configuration is identical to the configuration shown in "IPSec (56-bit) Example" section on page 3-11, except for the line in bold:

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
clock timezone - 0 6
ip subnet-zero
no ip domain-lookup
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 5000
crypto isakmp key 1234567890 address 30.1.1.1
crypto isakmp identity hostname
!
crypto ipsec transform-set test-transform ah-md5-hmac esp-3des esp-md5-hmac
!
 crypto map test-ipsec local-address cable-modem0
 crypto map test-ipsec 10 ipsec-isakmp
 set peer 30.1.1.1
 set transform-set test-transform
 match address 200
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
!
interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
 no keepalive
 no cable-modem compliant bridge
 crypto map test-ipsec
router rip
```

```
 version 2
 network 10.0.0.0
 network 192.168.100.0
!
ip classless
no ip http server
no service finger
!
access-list 200 permit ip host 10.1.0.25 30.1.1.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 login
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).

L2TP Example

When the Cisco uBR924 router is using a software image that supports the Layer 2 Tunnel Protocol (L2TP), the router can function as an L2TP network server (LNS), which is one part of a virtual private dialup network (VPDN). In this configuration, the router creates a secure connection with another router that is functioning as an L2TP access concentrator (LAC)—traffic sent between the two routers is protected from interception or modification, even when it travels across public networks such as the Internet.

Note The Cisco uBR924 cable access router does not support the L2TP feature in Cisco IOS Release 12.1(3)T and above.

Note The computer connected to the Cisco uBR924 router must be running software, such as Windows 98, that supports VPDN connections.

Configuration of a VPDN can be very complex, depending on the networks being used and how many peer devices will be establishing VPDN connections. The following table shows the minimum configuration needed for a typical VPDN configuration on a Cisco uBR924 router using the L2TP protocol (the LAC must be similarly configured).

Note Cisco IOS Release 12.1(5)T, 12.2(2), or greater is required to support GRE IP tunnels.

	Command	Purpose
Step 1	uBR924(config)# **vpdn enable**	Enable VPDN services so that the router will look for tunnel definitions.
Step 2	uBR924(config)# **vpdn-group 1**	Create a unique VPDN group (1–3000) to which VPDN attributes can be assigned, and enter VPDN configuration mode.
Step 3	uBR924(config-vpdn)# **accept dialin l2tp virtual-template 1 remote L2TP_LAC**	Configure the VPDN group to accept a incoming request using the L2TP protocol from the remote peer named L2TP_LAC.
Step 4	uBR924(config-vpdn)# **l2tp ip tos reflect**	(Optional) Preserve the type of service (TOS) bits in the original packets.
Step 5	uBR924(config-vpdn)# **exit**	Return to global configuration mode.
Step 6	uBR924(config)# **no l2tp tunnel authentication**	Disable L2TP tunnel authentication.
Step 7	uBR924(config)# **interface Virtual-Template1**	Create a virtual access interface from the virtual template and enter interface configuration mode.
Step 8	uBR924(config-if)# **ip unnumbered Ethernet0**	Enable IP traffic on the virtual access interface without requiring a specific IP address for the interface.
Step 9	uBR924(config-if)# **no ip directed-broadcast**	Disable the forwarding of directed broadcasts on this interface to prevent some common hacker attacks.
Step 10	uBR924(config-if)# **peer default ip address pool dialup**	Obtain an IP address from the default dialup IP address pool.
Step 11	uBR924(config-if)# **ppp authentication chap**	Enables the Challenge Handshake Authentication Protocol (CHAP) on the interface to allow verification of the remote end.
Step 12	uBR924(config-if)# **Ctrl-z**	Return to privileged EXEC mode.
Step 13	uBR924# **copy running-config startup-config** Building configuration...	Save the configuration to nonvolatile memory so that it will not be lost in the event of a reset, power cycle, or power outage.
Step 14	uBR924# **show startup-config**	Display the configuration file that was just created.

Note For more details on the L2TP feature, see the *Layer 2 Tunnel Protocol* and *L2TP Dialout* feature modules, available on CCO and the Documentation CD-ROM.

The following sections show sample configurations for the Cisco uBR924 router acting as the LNS. The relevant commands are in bold.

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
!
hostname Router
!
class-map class-default
```

```
 match any
!
!
clock timezone - 0 1
ip subnet-zero
ip tftp source-interface cable-modem0
no ip domain-lookup
!
vpdn enable
!
vpdn-group 1
 accept dialin l2tp virtual-template 1 remote L2TP_LAC
 no l2tp tunnel authentication
!
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 peer default ip address pool dialup
 ppp authentication chap
!

interface cable-modem0
 ip address dhcp
 no ip directed-broadcast
no cable-modem compliant bridge
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.100.0
!
ip local pool dialup 192.168.100.100
ip classless
no ip http server
no service finger
!
line con 0
 transport input none
line vty 0 4
 login
!
end
```

Note The above configuration assumes that the DHCP server assigns an IP address to the cable interface that is in the class A private network (10.0.0.0).