Advanced Data-Only Configurations

This chapter describes how to configure the Cisco uBR905 and Cisco uBR925 cable access routers for data operation with features beyond those supported in the default operation mode of plug-and-play DOCSIS bridging. The following configurations are described:

Note To configure the Cisco uBR925 cable access router for data and voice operation, see Chapter 4, "Voice over IP Configurations."

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 cable access 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 uBR905 and Cisco uBR925 cable access routers 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. 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 uBR905 or the uBR925, 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 cable access 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 cable access router are on a private network or on a different subnet than the subnet used by the CMTS.

To configure the routing mode on the cable access router, complete the following steps:

- 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 cable access router, log in to the router, enter global configuration mode, and enter the following commands:

	Command	Purpose
Step 1	ubr9x5(config)# **int c 0**	Enters interface configuration mode for the cable interface.
Step 2	ubr9x5(config-if)# **no cable-modem compliant bridge**	Disables DOCSIS-compliant bridging.
Step 3	ubr9x5(config-if)# **no bridge group** *number*	Removes the bridge group.
Step 4	ubr9x5(config-if)# **ip address docsis**	Configures the cable interface to receive an IP address from the DHCP server.
Step 5	ubr9x5(config-if)# **exit**	Returns to global configuration mode.
Step 6	ubr9x5(config)# **int e 0**	Enters interface configuration mode for Ethernet 0.
Step 7	ubr9x5(config-if)# **no bridge group** *number*	Removes the bridge group.
Step 8	ubr9x5(config-if)# **ip address** *ip-address subnet-mask*	Enters the Ethernet interface's IP address and subnet mask.
Step 9	ubr9x5(config-if)# **exit**	Returns to global configuration mode.
Step 10	ubr9x5(config)# **int usb0**	(Cisco uBR925 only) Enters interface configuration mode for USB 0.
Step 11	ubr9x5(config-if)# **no bridge group** *number*	(Cisco uBR925 only) Removes the bridge group.
Step 12	ubr9x5(config-if)# **ip address** *ip-address subnet-mask*	(Cisco uBR925 only) Enters the USB interface's IP address and subnet mask.
Step 13	ubr9x5(config-if)# **exit**	(Cisco uBR925 only) Returns to global configuration mode.
Step 14	ubr9x5(config)# **ip routing**	Enables IP routing for the router.

	Command	Purpose
Step 15	**To use RIPv2:**	
	ubr9x5(config)# **router rip**	Enters router configuration mode.
	ubr9x5(config-router)# **version 2**	Enables RIPv2 routing.
	ubr9x5(config-router)# **network** *cable-network-number*	Enables routing on the cable interface's IP network.
	ubr9x5(config-router)# **network** *Ethernet-network-number*	Enables routing on the Ethernet interface's IP network.
	ubr9x5(config-router)# **network** *USB-network-number*	(Cisco uBR925 only) Enables routing on the USB interface's IP network.
	ubr9x5(config-router)# **exit**	Returns to global configuration mode.
Step 16	ubr9x5(config)# **n o cdp run**	(Optional) Disables 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 cable access router.
Step 17	ubr9x5(config)# **ip default-gateway** *ip-address*	Sets the default gateway for routing (typically, this is the CMTS).
Step 18	ubr9x5(config)# **ip classless**	(Optional) Enables the forwarding of packets that are destined for unrecognized subnets to the best supernet route.
Step 19	ubr9x5(config)# **ip route 0.0.0.0 0.0.0.0** *ip-address*	(Optional) Establishes 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 20	ubr9x5(config-if)# **Ctrl-z**	Returns to privileged EXEC mode.
Step 21	ubr905# **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 22	ubr905# **show startup-config**	Displays the configuration file that was just created.
Step 23	ubr905# **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 for the Cisco uBR905 and Cisco uBR925 cable access routers; 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 docsis
 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 cable access 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 cable access router then allocates to the PCs as needed.

Note The cable access 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-modem 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 cable access 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	ubr9x5(config)# **ip dhcp pool** *pool-name*	Creates an address pool for the DHCP server named *pool-name* and enters DHCP configuration mode.
Step 2	ubr9x5(config-dhcp)# **network** *IP-network-number subnet-mask*	Specifies 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	ubr9x5(config-dhcp)# **domain-name** *domain-name*	Specifies the domain name to be assigned to CPE devices (for example, **cisco.com**).
Step 4	ubr9x5(config-dhcp)# **dns-server** *ip-address*	Specifies the IP address for the DNS server provided by the service provider that services the DNS requests from the CPE devices. More than one DNS server can be specified.
Step 5	ubr9x5(config-dhcp)# **default-router** *ip-address*	Specifies 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	ubr9x5(config-dhcp)# **exit**	Returns to global configuration mode.
Step 7	ubr9x5# **show startup-config**	Displays the configuration file that was just created.

To verify that the DHCP server is enabled, enter the **show startup-config** command. The following example shows a sample configuration file for a Cisco uBR905 cable access router acting as a DHCP server. 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
!
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 docsis
 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 cable access 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 192.168.0.0) 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. NAT/PAT is not typically used for a USB interface because only one computer can be connected through the USB interface.

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	ubr9x5(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	ubr9x5(config)# **interface Ethernet0**	Enters interface configuration mode for the router's Ethernet interface.
Step 3	ubr9x5(config-if)# **ip nat inside**	Specifies that the Ethernet is the "inside" of the NAT/PAT translation.

	Command	Purpose
Step 4	ubr9x5(config-if)# **exit**	Exits interface configuration mode.
Step 5	ubr9x5(config)# **interface cable-modem0**	Enters interface configuration mode for the router's cable interface.
Step 6	ubr9x5(config-if)# **ip nat outside**	Specifies that the cable interface is the "outside" of the NAT/PAT translation.
Step 7	ubr9x5(config-if)# **exit**	Exits interface configuration mode.
Step 8	ubr9x5(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	ubr905# **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 10	ubr905# **show startup-config**	Displays 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 Cisco.com and the Documentation CD-ROM.

The following configuration for the Cisco uBR905 and Cisco uBR925 cable access routers shows an example of a cable access 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 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
!
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 (192.168.0.0).

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	ubr9x5(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	ubr9x5(config)# **interface Ethernet0**	Enters interface configuration mode for the router's Ethernet interface.
Step 3	ubr9x5(config-if)# **ip nat inside**	Specifies that the Ethernet is the "inside" of the NAT/PAT translation.
Step 4	ubr9x5(config-if)# **exit**	Exits interface configuration mode.
Step 5	ubr9x5(config)# **interface cable-modem0**	Enters interface configuration mode for the router's cable interface.

	Command	Purpose
Step 6	ubr9x5(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	ubr9x5(config-if)# **ip nat outside**	Specifies that the cable interface is the "outside" of the NAT/PAT translation.
Step 8	ubr9x5(config-if)# **exit**	Exits interface configuration mode.
Step 9	ubr9x5(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	ubr905# **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	ubr905# **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 uBR905 and Cisco uBR925 cable access routers 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 uBR905 and Cisco uBR925 cable access routers 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 uBR905 and Cisco uBR925 cable access routers, 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 uBR905 or Cisco uBR925 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 uBR905 and Cisco uBR925 cable access routers:

```
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 uBR905 and Cisco uBR925 cable access routers must meet the following prerequisites:

- The cable access router must be using a Cisco IOS image that supports the IPsec feature set.
- The cable access router must be configured for routing mode.
- The cable access 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 12.2(2)XA1, 12.2(2)T, or greater is required to support GRE IP tunnels.

The configuration of the cable access 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 cable access router should encrypt traffic to one or more than one peer end-point. A technique that works well for a small network might not scale well for a large network. For example, using preshared 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.

To configure the cable access router for IPsec encryption with one peer router and preshared keys, enter the following commands:

	Command	Purpose
Step 1	ubr9x5(config)# **crypto isakmp enable**	Enables the use of ISAKMP/IKE on the cable access router.
Step 2	ubr9x5(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	ubr9x5(config-isakmp)# **encryption des**	Specifies that 56-bit DES encryption is used to encrypt the data.
Step 4	ubr9x5(config-isakmp)# **hash md5**	Specifies the MD5 (HMAC variant) hash algorithm for packet authentication.
Step 5	ubr9x5(config-isakmp)# **group 1**	Specifies the 768-bit Diffie-Hellman group for key negotiation.
Step 6	ubr9x5(config-isakmp)# **authentication pre-share**	Specifies that the authentication keys are preshared, as opposed to dynamically negotiated using RSA public key signatures.
Step 7	ubr9x5(config-isakmp)# **lifetime** *seconds*	Defines how long each security association should exist before expiring (60 to 86,400 seconds).
Step 8	ubr9x5(config-isakmp)# **exit**	Exits ISAKMP policy configuration command mode.

	Command	Purpose
Step 9	ubr9x5(config)# **crypto isakmp key** *shared-key* **address** *ip-address*	Specifies the preshared 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 preshared key using the **crypto key public-chain dss** command. See the description of this command in the *Cisco Encryption Technology Commands* document, available on Cisco.com and the Documentation CD-ROM.
Step 10	ubr9x5(config)# **crypto isakmp identity hostname**	Sets the ISAKMP identity of the router to its host name concatenated with the domain name (for example, **ubr905.cisco.com**).
Step 11	ubr9x5(config)# **crypto ipsec transform-set** *transform-set-name transform1 transform2 transform3*	Establishes the transform set to be used for IPsec encryption. As many as three transformations can be specified for a set, such as **ah-md5-hmac esp-des esp-md5-hmac**.
Step 12	ubr9x5(config)# **crypto map** *crypto-map-name* **local-address cable-modem0**	Creates the specified crypto map and applies it to the cable interface.
Step 13	ubr9x5(config)# **crypto map** *crypto-map-name* **10 ipsec-isakmp**	Creates a crypto map numbered 10 and enters the crypto map configuration mode.
Step 14	ubr9x5(config-crypto)# **set peer** *ip-address*	Identifies the IP address for the destination peer router.
Step 15	ubr9x5(config-crypto)# **set transform**-set *transform-set-name*	Sets the crypto map to use the transform set created previously.
Step 16	ubr9x5(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 170, 171, and 172 should not be used because they are reserved for DOCSIS use.
Step 17	ubr9x5(config-crypto)# **exit**	Exits crypto map configuration mode.
Step 18	ubr9x5(config)# **int c 0**	Enters interface configuration mode for the cable interface.
Step 19	uBR905 (config-if)# **crypto map** *crypto-map-name*	Applies the crypto map created above to the cable interface.
Step 20	uBR905 (config-if)# **access-list** *access-list-number* **permit ip host** *uBR905-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	ubr9x5(config-if)# **Ctrl-z**	Returns to privileged EXEC mode.
Step 22	ubr905# **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 23	ubr905# **show startup-config**	Displays the configuration file that was just created.

Note To use IPsec encryption, the peer router must also be configured for IPsec encryption, using the identical parameters used on the cable access router.

Sample Configuration

The following configuration shows a typical IPsec configuration using these parameters:

Note IPsec encryption on the Cisco uBR905 and Cisco uBR925 cable access routers automatically uses the routers' advanced onboard hardware accelerator.

- 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
  - Preshared authentication keys
  - 768-bit Diffie-Hellman group (the default)
  - Security association lifetime of 5,000 seconds (approximately 83 minutes).
- The preshared key has the value 1234567890 (keys are much more complex than this simple example)
- IPsec encryption is being done on traffic sent from the cable interface on the cable access 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 docsis
 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 is used as part of a virtual private network (VPN), creating and configuring VPNs must also be understood.

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

- *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 Cisco.com and the Documentation CD-ROM, also provide more in-depth configuration information:

- *Cisco IOS Security Configuration Guide*, Cisco IOS Release 12.1—Provides an overview of Cisco IOS security features.

- *Cisco IOS Security Command Reference*, Cisco IOS Release 12.1—Provides a reference for each of the Cisco IOS commands used to configure IPsec encryption and related security features.
- *Cisco IOS Software Command Summary*, Cisco IOS Release 12.1—Summarizes the Cisco IOS commands used to configure all Release 12.1 security features.

Note Additional documentation on IPsec becomes available on Cisco.com and the Documentation CD-ROM as new features and platforms are added. Cisco Press also publishes several books on this subject—go to http://www.cisco.com/cpress/home/home.htm for more information.

IPsec Example (3DES)

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 the 3DES feature set; this level of encryption 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 docsis
 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 previous 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 cable access 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 that is sent between the two routers is protected from interception or modification, even when it travels across public networks such as the Internet.

Note The computer connected to the cable access 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 cable access router using the L2TP protocol (the LAC must be similarly configured).

Note Cisco IOS Release 12.2(2)XA1, 12.2(2)T, or greater is required to support GRE IP tunnels.

	Command	Purpose
Step 1	ubr9x5(config)# **vpdn enable**	Enables VPDN services so that the router will look for tunnel definitions.
Step 2	ubr9x5(config)# **vpdn-group 1**	Creates a unique VPDN group (1–3000) to which VPDN attributes can be assigned, and enter VPDN configuration mode.
Step 3	ubr9x5(config-vpdn)# **accept dialin l2tp virtual-template 1 remote L2TP_LAC**	Configures the VPDN group to accept an incoming request using the L2TP protocol from the remote peer named L2TP_LAC.
Step 4	ubr9x5(config-vpdn)# **l2tp ip tos reflect**	(Optional) Preserves the type of service (ToS) bits in the original packets.
Step 5	ubr9x5(config-vpdn)# **exit**	Returns to global configuration mode.
Step 6	ubr9x5(config)# **no l2tp tunnel authentication**	Disables L2TP tunnel authentication.
Step 7	ubr9x5(config)# **interface Virtual-Template1**	Creates a virtual access interface from the virtual template and enters interface configuration mode.
Step 8	ubr9x5(config-if)# **ip unnumbered Ethernet0**	Enables IP traffic on the virtual access interface without requiring a specific IP address for the interface.
Step 9	ubr9x5(config-if)# **no ip directed-broadcast**	Disables the forwarding of directed broadcasts on this interface to prevent some common hacker attacks.
Step 10	ubr9x5(config-if)# **peer default ip address pool dialup**	Obtains an IP address from the default dialup IP address pool.
Step 11	ubr9x5(config-if)# **ppp authentication chap**	Enables the Challenge Handshake Authentication Protocol (CHAP) on the interface to allow verification of the remote end.
Step 12	ubr9x5(config-if)# **Ctrl-z**	Returns to privileged EXEC mode.
Step 13	ubr905# **copy running-config startup-config**	Saves the configuration to nonvolatile memory so that it is not lost in the event of a reset, power cycle, or power outage.
Step 14	ubr905# **show startup-config**	Displays 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 Cisco.com and the Documentation CD-ROM.

The following example shows a sample configuration for the cable access 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 docsis
 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 This 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).