

uBR7100 All-In-One Configuration in Bridge Mode

Document ID: 29243

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Description

- Routing and Bridging Operation
- Integrated Routing and Bridging (IRB)
- Bridge-Group Virtual Interface
- The Cisco IOS DHCP Service on a CMTS
- Further DHCP Server Functionality
- The Cisco IOS TFTP Service
- The Cisco IOS ToD Service
- The Internal DOCSIS Configuration File Generator

Configure

- Network Diagram
- Configurations

Basic All-in-one Configuration

- Verification Tips for Basic Configuration

Advanced All-in-one Configuration

- Verification Tips for Advanced Configuration

Related Information

Introduction

This document provides a sample configuration for a Cisco uBR7100 Cable Modem Termination System (CMTS) that acts as a Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and TFTP server. It also explains how to build the Data-over-Cable Service Interface Specifications (DOCSIS) configuration file using the command-line interface (CLI) on the CMTS. This configuration is known as all-in-one configuration for a Cisco CMTS while the CMTS is configured in bridging mode. Presently the uBR7100 platform is the only CMTS platform that supports bridging.

Prerequisites

Requirements

Reader of this document must have a basic understanding of bridging, the DOCSIS, DHCP, ToD, and TFTP protocols.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco uBR7100 Cable Modem Termination System
- DOCSIS-compliant cable modems
- Cisco IOS® Software Release 12.1(7)EC or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Description

A DOCSIS-compliant cable modem requires access to three types of servers in order to successfully come online.

- A DHCP server, which provides the cable modem with an IP address, a subnet mask, and other IP related parameters.
- An RFC-868-compliant ToD server, which tells the modem know the current time. A cable modem needs to know the time in order to be able to properly add accurate timestamps to its event log.
- A TFTP server, from which a cable modem is able to download a DOCSIS configuration file containing cable-modem-specific operational parameters.

Most cable operators use Cisco Network Registrar (CNR) as the DHCP, Domain Name Server (DNS), and TFTP servers. The ToD server is not a part of the CNR. The ToD server that is used depends upon the platform on the cable operator s system. The ToD should be RFC-868-compliant. For UNIX systems, it is included in Solaris; it is only necessary to make sure that the inetd.conf file in the /etc directory contains these lines:

```
# Time service is used for clock synchronization.
#
time    stream  tcp      nowait  root    internal
time    dgram   udp      wait    root    internal
```

For Windows, the most commonly used software is Greyware .

This table shows the Cisco IOS Software Releases in which different server capabilities have been added to the CMTS:

Server Capabilities	Cisco IOS Software Release
DHCP	12.0(1)T
ToD	12.0(4)XI
TFTP	11.0 (for all platforms)

This document explains each of these features. The configuration on the CMTS that contains all of these capabilities is called the all-in-one configuration for the CMTS. With this configuration, you do not need any additional servers to test your cable plants and provide high speed internet access.

It is also possible to configure a DOCSIS configuration file residing on the CMTS instead of the TFTP server. According to the release notes, you need at least Cisco IOS Software Release 12.1(2)EC1 to use this feature.

Although this all-in-one configuration is very convenient for lab environments, initial testing, small deployments, and troubleshooting, it is not scalable to support a very large number of cable modems. So it is *not* recommended that you use this configuration in operational cable plants with large deployments of cable modems.

Cisco Technical Support engineers often use this configuration to eliminate variables while troubleshooting cable problems.

Routing and Bridging Operation

The Cisco uBR7100 series routers support these modes of operation:

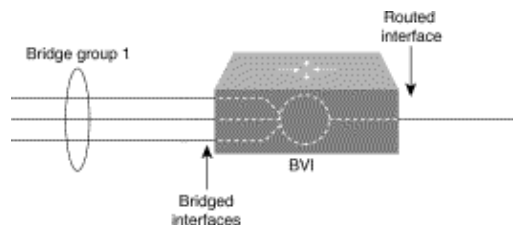
- **Routing mode** Routing operation is the typical default mode for Cisco CMTS routers. It provides a wide spectrum of Cisco IOS Software routing features, such as a DHCP server and control over which packets are sent over each interface.
- **Transparent Bridging mode** Bridging operation between the cable interface and port adapter interfaces is typically not used in DOCSIS CMTS installations because of potential performance and security problems. Bridging is very effective, however, in CMTS environments with a limited number of customer premise equipment (CPE) devices as in a typical multidwelling unit (MDU) or multitenant unit (MTU) environment especially if the CMTS is replacing an existing bridging network.

Integrated Routing and Bridging (IRB)

Integrated Routing and Bridging (IRB) operation allows bridging within a specific segment of networks or hosts, yet also allows those hosts to connect to devices on other, routed networks without having to use a separate router to interconnect the two networks.

Note: Transparent bridging and IRB operation are supported only when using Cisco IOS Software Release 12.1(7)EC and later. For complete details on transparent bridging and IRB operation, see the Bridging chapters in the Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.1, available on Cisco.com and the Documentation CD-ROM.

Bridge-Group Virtual Interface



Because bridging operates in the data-link layer and routing operates in the network layer, they follow different protocol configuration models. Taking the basic IP model as an example, all bridged interfaces would belong to the same network, while each routed interface represents a distinct network.

In IRB, the bridge-group virtual interface is introduced to avoid confusing the protocol configuration model when a specific protocol is both bridged and routed in a bridge group.

The bridge-group virtual interface is a normal routed interface that does not support bridging, but does represent its corresponding bridge group to the routed interface. It has all the network layer attributes (such as a network layer address and filters) that apply to the corresponding bridge group. The interface number assigned to this virtual interface corresponds to the bridge group that this virtual interface represents. This number is the link between the virtual interface and the bridge group.

When you enable routing for a given protocol on the bridge-group virtual interface, packets coming from a routed interface but destined for a host in a bridged domain are routed to the bridge-group virtual interface

and are forwarded to the corresponding bridged interface. All traffic routed to the bridge-group virtual interface is forwarded to the corresponding bridge group as bridged traffic. All routable traffic received on a bridged interface is routed to other routed interfaces as if it is coming directly from the bridge-group virtual interface.

To receive routable packets arriving on a bridged interface but destined for a routed interface or to receive routed packets, the bridge-group virtual interface must also have the appropriate addresses. MAC addresses and network addresses are assigned to the bridge-group virtual interface in this manner:

- The bridge-group virtual interface borrows the MAC address of one of the bridged interfaces in the bridge group associated with the bridge-group virtual interface.
- To route and bridge a given protocol in the same bridge group, you must configure the network layer attributes of the protocol on the bridge-group virtual interface.
- No protocol attributes should be configured on the bridged interfaces, and no bridging attributes can be configured on the bridge-group virtual interface.

Because there can be only one bridge-group virtual interface representing a bridge group and the bridge group can be made up of different media types configured for several different encapsulation methods you may need to configure the bridge-group virtual interface with the particular encapsulation methods required to switch packets correctly.

The Cisco IOS DHCP Service on a CMTS

Cisco routers running Cisco IOS Software Release 12.0(1)T or later have the ability to act as DHCP servers. This DHCP service may be configured to provide DHCP leases to cable modems and CPE, such as PCs and workstations.

There is a minimum set of DHCP options that *cable modems* typically require in order to come online:

- An IP address (The **yiaddr** field in the DHCP packet header)
- A subnet mask (DHCP Option 1)
- The local time offset from Greenwich Mean Time (GMT) in seconds (DHCP Option 2)
- A default router (DHCP Option 3)
- The IP address of a ToD server (DHCP Option 4)
- The log server (DHCP Option 7)
- The IP address of a TFTP server (The **siaddr** field in the DHCP packet header)
- The name of a DOCSIS configuration file (The **file** field in the DHCP packet header)
- A DHCP lease time in seconds (DHCP Option 51)

In the router, those options can be configured with these commands:

```
!  
ip dhcp pool cm-platinum  
network 10.1.4.0 255.255.255.0  
bootfile platinum.cm  
next-server 10.1.4.1  
default-router 10.1.4.1  
option 7 ip 10.1.4.1  
option 4 ip 10.1.4.1  
option 2 hex ffff.8f80  
lease 7 0 10  
!
```

These are explanations of each of those commands:

- **dhcp pool** Defines the name of the cable modem scope (`cm-platinum`).

- **network** Provides the IP address and the subnet mask (DHCP Option 1).
- **bootfile** Provides the boot file name which, in this case, is platinum.cm.
- **next-server** Specifies the TFTP server IP address which, in this case, is the primary IP address in the interface c4/0.
- **default-router** Defines the default gateway which, in this case, is the primary IP address of interface c4/0 (DHCP Option 3).
- **option 7** Defines the Log server DHCP Option.
- **option 4** Provides the ToD server IP address (primary IP address of interface c4/0).
- **option 2** Provides the time offset option for GMT 8 hours (8 hours equals 8800 seconds, which equals **fff.8f80** in hexadecimal numbers).

Note: To learn more about how to convert an offset time decimal value into hexadecimal, refer to How to Calculate the Hexadecimal Value for DHCP Option 2 (time offset).

- **lease** Sets the lease time (7 days, 0 hours, 10 minutes).

For CPE devices, these options are the minimum required to operate successfully:

- An IP address (The **yiaddr** field in the DHCP packet header)
- A subnet mask (DHCP Option 1)
- A default router (DHCP Option 3)
- The IP address of one or more DNSs (DHCP Option 6)
- A domain name (DHCP Option 15)
- A DHCP Lease time in seconds (DHCP Option 51)

In the router, those options can be configured with these commands:

```
!
ip dhcp pool pcs-irb

!--- The scope for the hosts.

    network 172.16.29.0 255.255.255.224

!--- The IP address and mask for the hosts.

    next-server 172.16.29.1

!--- TFTP server; in this case, the secondary address is used.

    default-router 172.16.29.1
    dns-server 172.16.30.2

!--- DNS server (which is not configured on the CMTS).

    domain-name cisco.com
    lease 7 0 10
!
```

Further DHCP Server Functionality

These are some other features which can be used from the Cisco IOS Software DHCP server:

- **ip dhcp ping** Ping before lease function, which ensures that the DHCP server does not issue leases for IP addresses that are already in use.
- **ip dhcp database** A function which stores DHCP bindings in an external database in order to maintain MAC-address-to-IP-address relationships during a CMTS power cycle.
- **show ip dhcp** A suite of commands which can be used to monitor the operation of the DHCP server.

- **debug ip dhcp server** A suite of commands which can be used to troubleshoot the operation of the DHCP server.

All of these extra functions and features are described in the Cisco IOS Software DHCP server feature release notes in the Cisco IOS DHCP Server document.

The Cisco IOS TFTP Service

After a cable modem has attempted to contact a ToD server, it proceeds to contact a TFTP server in order to download a DOCSIS configuration file. If a binary DOCSIS configuration file can be copied to a flash device on a Cisco CMTS then the router can act as a TFTP server for that file.

This is the procedure to download a DOCSIS configuration file into flash:

1. Issue this **ping** command to ensure that the CMTS can reach the server where the DOCSIS configuration file is located.

```
Ubr7111# ping 172.16.30.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.2, timeout is 2 seconds:

!--- Output suppressed.

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

2. Copy the file (in this case, it is called silver.cm) into the flash of the CMTS.

```
Ubr7111# copy tftp flash

Address or name of remote host []? 172.16.30.2
Source filename []? silver.cm
Destination filename [silver.cm]?

Accessing tftp://172.16.30.2/silver.cm...
Loading silver.cm from 172.16.30.2 (via Ethernet2/0): !
[OK - 76/4096 bytes]

76 bytes copied in 0.152 secs
```

3. Check the flash and verify that the size of the file is correct, using the **dir** command.

```
Ubr7111# dir

Directory of disk0:/

 1  -rw-          74  Feb 13 2001 16:14:26  silver.cm
 2  -rw-    10035464  Feb 14 2001 15:44:20  ubr7100-ik1s-mz.121-11b.EC.bin

47890432 bytes total (17936384 bytes free)
```

4. To enable the TFTP service on the CMTS, issue this command in global configuration mode:

```
tftp-server slot0:silver.cm alias silver.cm
```

5. Confirm Step 4 by checking for these lines in the configuration:

```
!
tftp-server slot0:silver.cm alias silver.cm
tftp-server server
!
```

For more information about the configuration of a TFTP server in a router, refer to the Additional File Transfer Function Commands document.

The Cisco IOS ToD Service

After a cable modem successfully acquires a DHCP lease, it then attempts to contact a ToD server. Cisco CMTS products running Cisco IOS Software Release 12.0(4)XI or later are able to provide an RFC 868 ToD service.

A common misconception is that the ToD service that cable modems need to use to come online is the same as the Network Time Protocol (NTP) service which is commonly configured on Cisco routers. The NTP service and the ToD service are incompatible. Cable modems can not talk to an NTP server. While cable modems must attempt to contact a ToD server as a part of the process of coming online, modems compliant with the latest revisions of the DOCSIS 1.0 radio frequency interference (RFI) specification still proceed to come online even if a ToD server cannot be reached.

According to the most recent releases of the specification, if a cable modem is unable to contact a ToD server then it may continue with the process of coming online. It should, however, periodically try to contact the ToD server until it is successful. Earlier versions of the DOCSIS 1.0 RFI specification mandated that, if a cable modem could not contact a ToD server, then the modem could not come online. It is important to be aware that cable modems running older firmware may comply with this older version of the specification.

Note: The cable modems of some vendors do not interoperate with the Cisco IOS Software ToD service. If these modems are compliant with the most recent versions of the DOCSIS 1.0 RFI specification then they should continue to come online regardless. This interoperability issue is being addressed by Cisco bug ID CSCdt24107 (registered customers only) .

To configure ToD on a Cisco CMTS, issue these global commands:

```
service udp-small-servers max-servers no-limit
!
cable time-server
!
```

The Internal DOCSIS Configuration File Generator

Cisco CMTS products running Cisco IOS Software Release 12.1(2)EC or later (in the EC release train) can be configured to generate and internally store DOCSIS configuration files. Doing so is useful because it takes away the requirement of having access to an external DOCSIS configuration file generation tool. When a DOCSIS configuration file is created using the internal configuration tool, the file becomes automatically available through TFTP. Furthermore, only cable modems on directly connected cable interfaces are able to download these configuration files.

These configuration samples show the creation of two DOCSIS configuration files.

The first is called `disable.cm`, which allows a cable modem to come online but prevents connected CPE devices from accessing the network of the service provider. In this case, there is an **access-denied** command. Notice that the downstream and upstream speeds in this case are 1 Kbps, and the maximum burst size is 1600 bytes.

```
cable config-file disable.cm
access-denied
service-class 1 max-upstream 1
service-class 1 max-downstream 1600
timestamp
!
```

A cable operator uses this `disable.cm` DOCSIS configuration file to deny access to CPE behind the cable

modem while still allowing the cable modem to come online. This is a more efficient way to deny a CPE service than using the **exclude** option in CNR, which does not allow the cable modem to come online: the cable modem repeatedly tries to come online and wastes bandwidth.

Cable modems with this DOCSIS configuration file show this output, when the **show cable modem** command is issued:

```
Cable1/0/U0 10 online(d) 2287 0.50 6 0 10.1.4.65 0010.7bed.9b45
```

The Verification Tips for Advanced Configuration section of this document gives more details about this output. The status **online(d)** means that the cable modems is online but access is denied.

In the second example, a DOCSIS configuration file called platinum.cm is created. In this case, the maximum upstream value is 1 Mbps, the guaranteed upstream value is 100 Kbps, the maximum downstream is 10 Mbps, and it allows up to 30 CPE devices to be connected.

```
cable config-file platinum.cm
  service-class 1 max-upstream 1000
  service-class 1 guaranteed-upstream 100
  service-class 1 max-downstream 10000
  service-class 1 max-burst 1600
  cpe max 30
  timestamp
!
```

Notice that, while configuring the DOCSIS configuration file in the CMTS, you do not need the statement **ftt server slot0:platinum.cm alias platinum.cm** because there is no **.cm** file stored in memory; it resides within the configuration.

Further details on the internal DOCSIS configuration file tool can be found in the document Cisco CMTS Configuration Commands.

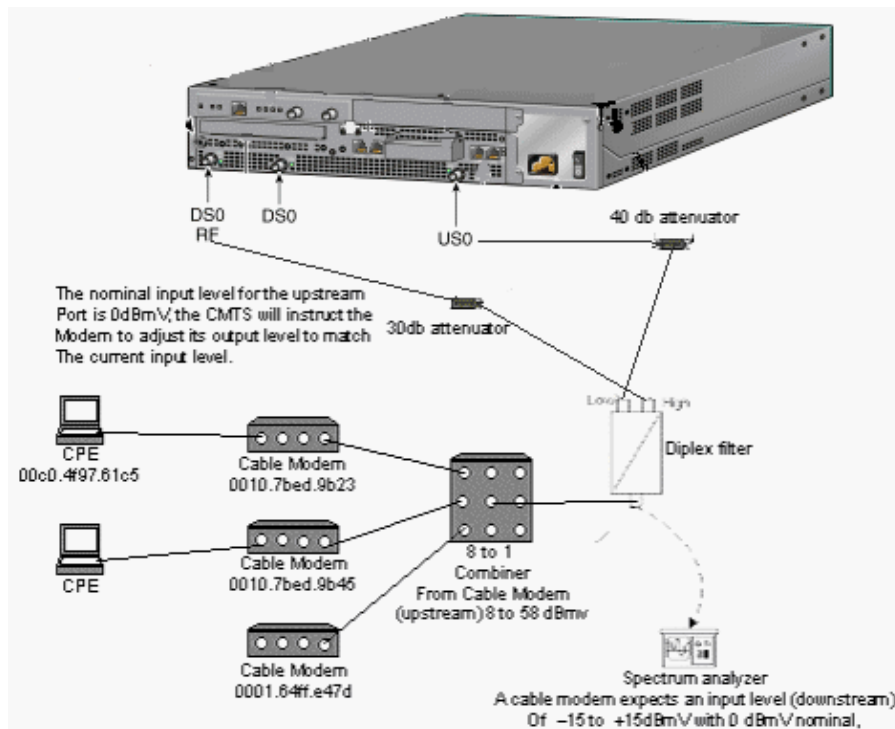
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

A typical lab setup topology is shown in this image:



Configurations

This document uses these configurations:

- Basic All-in-one Configuration
- Advanced All-in-one Configuration

This configuration is supported only on uBR7100 CMTS platforms.

The Cisco IOS Software Release that supports all-in-one configuration, including the configuration of the DOCSIS configuration file, is Cisco IOS Software Release 12.1(2)EC and the subsequent EC train releases. The Cisco IOS Software train that was used in this configuration is ubr7100-ik1s-mz.121-11b.EC.bin.

Basic All-in-one Configuration

This configuration summarizes all the pieces explained so far. It has two DHCP scopes: one for the cable modems and another one for the hosts behind the cable modems.

One DOCSIS configuration file is created, called platinum.cm. This file is applied to the DHCP pool called **cm-platinum**. The other DOCSIS configuration file, called disabled.cm, is not applied to anything at the moment.

Comments are in blue, after the related commands. All-in-one configuration commands are in **bold**.

Basic All-in-one Configuration

```
ubr7100# show run
Building configuration...

Current configuration : 3511 bytes
!
! Last configuration change at 01:12:37 PST Mon Sep 3 2001
!
```

```
version 12.1
no service pad
service timestamps debug datetime msec localtime

!--- Provides useful timestamps on all log messages.

service timestamps log datetime localtime
no service password-encryption
service linenummer
service udp-small-servers max-servers no-limit

!--- Supports a large number of modems or hosts attaching quickly.

!
hostnameubr7111
!
boot system flash disk0:ubr7100-ik1s-mz.121-11b.EC.bin
!
cable spectrum-group 3 frequency 4080000
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable timeserver

!--- Allows cable modems to obtain ToD from the uBR7100.

!
cable config-file platinum.cm
  service-class 1 max-upstream 128
  service-class 1 guaranteed-upstream 10
  service-class 1 max-downstream 10000
  service-class 1 max-burst 1600
  cpe max 8
  timestamp
!
clock timezone PST -9
clock calendar-valid
ip subnet-zero
no ip routing

!--- Disables routing on the CMTS.

no ip domain-lookup

!--- Prevents the CMTS from looking up domain names or attempting
!--- to connect to machines (for example, when mistyping commands).

ip hostubr7111 172.16.26.103
ip domain-name cisco.com
ip name-server 171.68.10.70
ip name-server 171.69.2.132
ip name-server 171.68.200.250
no ip dhcp relay information check

ip dhcp excluded-address 10.45.50.1 10.45.50.5
!
ip dhcp pool cm-platinum

!--- Name of the DHCP pool. This scope is for the cable modems attached
!--- to interface cable 4/0.

  network 10.1.4.0 255.255.255.0

!--- Pool of addresses for scope modems-c1/0.
```

```
bootfile platinum.cm

!--- DOCSIS configuration file name associated with this pool.

next-server 10.1.4.1

!--- IP address of the TFTP server which sends the boot file.

default-router 10.1.4.1

!--- Default gateway for cable modems; necessary to get DOCSIS files.

option 7 ip 10.1.4.1

!--- Log Server DHCP option.

option 4 ip 10.1.4.1

!--- ToD server IP address.

option 2 hex ffff.8f80

!--- Time offset for ToD, in seconds (HEX), from GMT.
!--- Pacific Standard Time offset from GMT = 8,000 seconds = ffff.8f80

lease 7 0 10

!--- Lease 7 days 0 hours 10 minutes.

!
ip dhcp pool pcs-irb

!--- Name of the DHCP pool. This scope is for the CPE attached to
!--- the cable modems that are connected to interface cable 1/0.

network 172.16.29.0 255.255.255.0

!--- Pool of addresses for scope pcs-c4 (associated with the secondary address).

next-server 172.16.29.1
default-router 172.16.29.1
dns-server 172.16.29.1
domain-name cisco.com
lease 7 0 10

!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
!
bridge irb
!
!
interface FastEthernet0/0
ip address 14.66.1.2 255.255.255.0
no ip route-cache
no ip mroute-cache
no keepalive
duplex half
speed auto
no cdp enable
bridge-group 1
bridge-group 1 spanning-disabled
!
```

```

interface FastEthernet0/1
 ip address 14.66.1.2 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex auto
 speed 10
 no cdp enable
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Cable1/0
 ip address 14.66.1.2 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 no keepalive
 cable packet-cache
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 525000000
 no cable downstream rf-shutdown
 cable downstream rf-power 55
 cable upstream 0 frequency 17808000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000
 no cable upstream 0 shutdown
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.1.4.1 255.255.255.0
!
ip default-gateway 14.66.1.1
ip classless
no ip http server
!
no cdp run
bridge 1 protocol ieee
 bridge 1 route ip
alias exec scm show cable modem
!
line con 0
 exec-timeout 0 0
 privilege level 15
 length 0
line aux 0
line vty 0 4
 privilege level 15
 no login
line vty 5 15
 login
!
end

```

Verification Tips for Basic Configuration

This section provides information you can use to confirm that your configuration is working properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

1. Make sure that the commands are supported in the Cisco IOS Software Release by issuing a **show version** command.
2. Verify that the DOCSIS configuration file is in flash.

```
Ubr7111# dir

Directory of disk0:/

   1  -rw-          74   Feb 13 2001 16:14:26  silver.cm
   2  -rw-    10035464  Feb 14 2001 15:44:20  ubr7100-ik1s-mz.121-11b.EC.bin

47890432 bytes total (17936384 bytes free)
```

Note: The file silver.cm was built using the DOCSIS CPE Configurator tool. For the platinum.cm file that was built in the CMTS configuration, you do not need the statement **tftp server slot0:platinum.cm alias platinum.cm** because there is no .cm file; it resides within the configuration.

3. Verify that the cable modems are online by issuing the **show cable modem** command.

```
Ubr7111# show interface cable 1/0 modem 0
```

SID	Priv bits	Type	State	IP address	method	MAC address
75	00	host	unknown	172.16.29.2	static	00c0.4f97.61c5
75	00	modem	up	10.1.4.2	dhcp	0010.7bed.9b23
76	00	modem	up	10.1.4.3	dhcp	0002.fdfa.0a63
77	00	host	unknown	172.16.29.3	dhcp	00a0.243c.eff5
77	00	modem	up	10.1.4.5	dhcp	0010.7bed.9b45
78	00	modem	up	10.1.4.4	dhcp	0004.2752.ddd5
79	00	modem	up	10.1.4.6	dhcp	0002.1685.b5db
80	00	modem	up	10.1.4.7	dhcp	0001.64ff.e47d

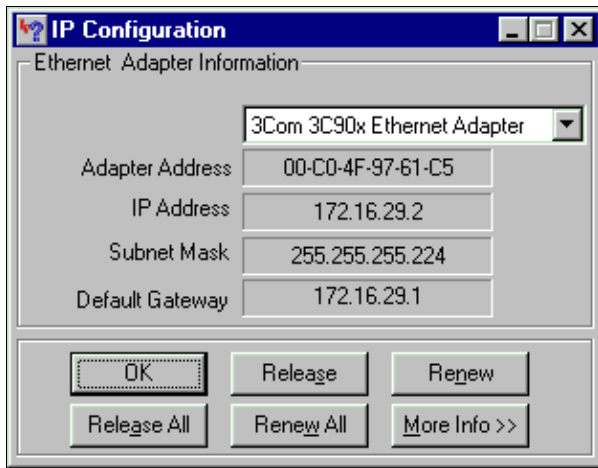
Notice that all of the cable modems are online. The ones connected to interface cable **1/0/U0** are in the network **10.1.4.0**. You can see from the configuration that their IP addresses are taken from the DHCP pool called **cm-platinum**.

Also notice that cable modems with MAC addresses **0010.7bed.9b23** and **0010.7bed.9b45** have a CPE behind them. Those cable modems come online with the default bridging configuration. Those PCs are configured with DHCP so that they can get their IP addresses from the network.

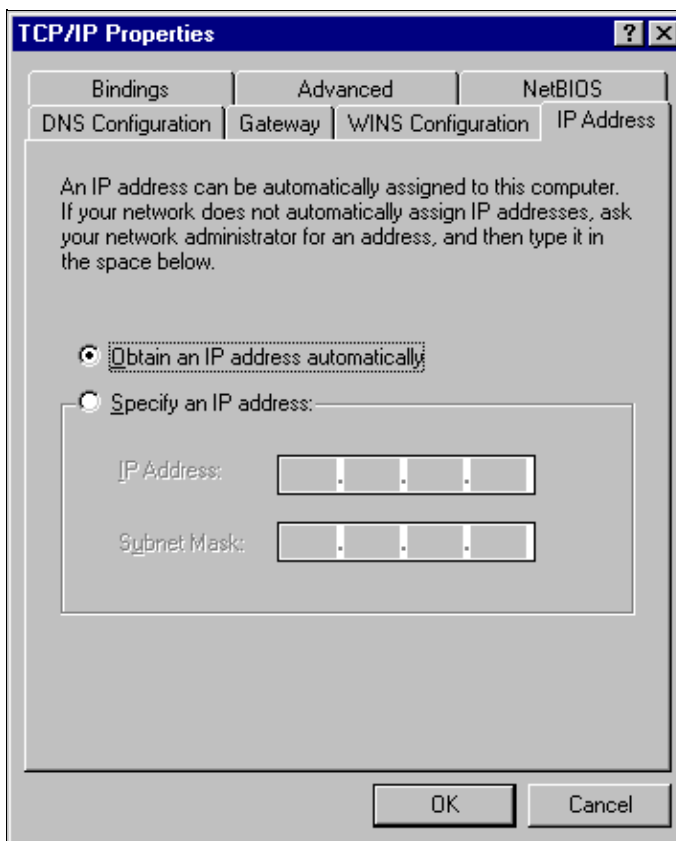
```
Ubr7111# show interface cable 1/0 modem 0
```

SID	Priv bits	Type	State	IP address	method	MAC address
75	00	host	unknown	172.16.29.2	static	00c0.4f97.61c5
75	00	modem	up	10.1.4.2	dhcp	0010.7bed.9b23
76	00	modem	up	10.1.4.3	dhcp	0002.fdfa.0a63
77	00	host	unknown	172.16.29.3	dhcp	00a0.243c.eff5
77	00	modem	up	10.1.4.5	dhcp	0010.7bed.9b45
78	00	modem	up	10.1.4.4	dhcp	0004.2752.ddd5
79	00	modem	up	10.1.4.6	dhcp	0002.1685.b5db
80	00	modem	up	10.1.4.7	dhcp	0001.64ff.e47d

This screen shot shows that those PCs get an IP address from the pools called **pcs-c4**.



You can also see from this PC that the TCP/IP settings are set to obtain IP address automatically.



Advanced All-in-one Configuration

This section provides a more sophisticated configuration example which involves the hierarchy functionality of DHCP pools. The way DHCP pool hierarchy works is that any DHCP pool with a network number that is a subset of another pool's network number inherits all of the characteristics of that other pool. This saves repetition in DHCP server configuration. If, however, the same specification is done with a different parameter, then the parameter is overwritten. This example shows a general pool with a boot file called platinum.cm and a subset of this pool with a boot file called disable.cm.

In addition to the DHCP pools created in the basic example, there are special requirements for two cable modems.

First, the cable modem **0010.7bed.9b45** is denied access; it is granted an IP address but it does not come online. Create this pool:

```
ip dhcp pool cm-0010.7bed.9b45
 host 10.1.4.65 255.255.255.0
 client-identifier 0100.107b.ed9b.45
 bootfile disable.cm
```

The most notable feature of this configuration example is the section where you specify special DHCP pools that correspond to individual cable modem MAC addresses. Such specification allows the DHCP server to send unique DHCP options to these modems. To specify a particular cable modem, the **client-identifier** parameter is used. The **client-identifier** must be set to **01**, followed by the MAC address of the device to which the entry corresponds. The **01** corresponds to the Ethernet for DHCP hardware type .

Note: When changing configuration files for a modem, you must do these steps to ensure that the cable modem gets the manually configured parameters:

1. Clear the IP DHCP binding table by issuing the **clear ip dhcp binding ip address** command.
2. Reset the cable modem in question by issuing the **clear cable modem mac address res** command.

Second, the cable modem **0010.7bed.9b23** also has a special requirement: it gets a different quality of service (QoS). Therefore, a different boot file is associated to the scope, as shown in this partial configuration:

```
ip dhcp pool cm-0010.7bed.9b23
 host 10.1.4.66 255.255.255.0
 client-identifier 0100.107b.ed9b.23
 bootfile silver.cm
!
```

When configuring DHCP pools for specific cable modems, it is always a good practice to give a relevant name. Also, because a specific IP address is assigned to the pool using the **host** command, you must issue the global command **ip dhcp exclude 10.1.4.60 10.1.4.70**. This command tells DHCP not to use addresses in this range.

Verification Tips for Advanced Configuration

The verification of this configuration focuses on the services that the cable modems are getting, especially **0010.7bed.9b45** and **0010.7bed.9b23**. You must be sure that they are getting both the addresses with which they were manually configured and the service.

The first thing to test is that **0010.7bed.9b45** comes online, but that service is denied. Issue the **show cable modem** command.

```
7246VXR# show cable modem
```

Interface	Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable4/0/U0	7	online	2813	0.00	7	0	10.1.4.7	0002.1685.b5db
Cable4/0/U0	8	online	2809	0.25	7	0	10.1.4.10	0002.fdfa.0a63
Cable4/0/U0	9	online	2288	-0.25	5	1	10.1.4.66	0010.7bed.9b23
Cable4/0/U0	10	online(d)	2287	0.50	6	0	10.1.4.65	0010.7bed.9b45
Cable4/0/U0	11	online	2809	-0.50	7	0	10.1.4.6	0001.64ff.e47d
Cable4/0/U0	12	online	2812	-0.50	7	0	10.1.4.9	0004.2752.ddd5

Notice these facts:

- Cable modem **0010.7bed.9b23** got IP address **10.4.1.66**, as specified in the **scope**

- **cm-0010.7bed.9b23**. There is a computer attached to it and it gets its IP address from pool **pcs-c4**.
- Cable modem **0010.7bed.9b23** has a different QoS.
- Cable modem **0010.7bed.9b45** got IP address **10.1.4.65**, as specified in the scope **cm-0010.7bed.9b45**. There *is* a computer attached to it; the CPE value, however, is **0** because that the service is denied.
- The Online State of **0010.7bed.9b45** is **online(d)**, which means that the cable modem comes online but access to the cable network is denied.

Consider this output from the **debug cable mac log verbose** command issued on the cable modem:

```

21:52:16: 78736.550 CMAC_LOG_RESET_RANGING_ABORTED
21:52:16: 78736.554 CMAC_LOG_STATE_CHANGE reset_interface_sta
21:52:16: 78736.558 CMAC_LOG_STATE_CHANGE reset_hardware_stat
21:52:17: 78737.024 CMAC_LOG_STATE_CHANGE wait_for_link_up_st
21:52:17: 78737.028 CMAC_LOG_DRIVER_INIT_IDB_RESET 0x082B9CA8
21:52:17: 78737.032 CMAC_LOG_LINK_DOWN
21:52:17: 78737.034 CMAC_LOG_LINK_UP
21:52:17: 78737.040 CMAC_LOG_STATE_CHANGE ds_channel_scanning
21:52:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed stat
21:52:18: 78738.386 CMAC_LOG_UCD_MSG_RCVD 1
21:52:19: 78739.698 CMAC_LOG_DS_64QAM_LOCK_ACQUIRED 747000000
21:52:19: 78739.702 CMAC_LOG_DS_CHANNEL_SCAN_COMPLETED
21:52:19: 78739.704 CMAC_LOG_STATE_CHANGE wait_ucd_state
21:52:20: 78740.368 CMAC_LOG_UCD_MSG_RCVD 1
21:52:22: 78742.396 CMAC_LOG_UCD_MSG_RCVD 1
21:52:22: 78742.398 CMAC_LOG_ALL_UCDS_FOUND
21:52:22: 78742.402 CMAC_LOG_STATE_CHANGE wait_map_state
21:52:22: 78742.406 CMAC_LOG_FOUND_US_CHANNEL 1
21:52:24: 78744.412 CMAC_LOG_UCD_MSG_RCVD 1
21:52:24: 78744.416 CMAC_LOG_UCD_NEW_US_FREQUENCY 39984000
21:52:24: 78744.420 CMAC_LOG_SLOT_SIZE_CHANGED 8
21:52:24: 78744.500 CMAC_LOG_UCD_UPDATED
21:52:24: 78744.564 CMAC_LOG_INITIAL_RANGING_MINISLOTS 41
21:52:24: 78744.566 CMAC_LOG_STATE_CHANGE ranging_1_state
21:52:24: 78744.570 CMAC_LOG_RANGING_OFFSET_SET_TO 9610
21:52:24: 78744.574 CMAC_LOG_POWER_LEVEL_IS 55.0 dBmV (command
21:52:24: 78744.578 CMAC_LOG_STARTING_RANGING
21:52:24: 78744.580 CMAC_LOG_RANGING_BACKOFF_SET 0
21:52:24: 78744.586 CMAC_LOG_RNG_REQ_QUEUED 0
21:52:24: 78744.622 CMAC_LOG_RNG_REQ_TRANSMITTED
21:52:24: 78744.626 CMAC_LOG_RNG_RSP_MSG_RCVD
21:52:24: 78744.628 CMAC_LOG_RNG_RSP_SID_ASSIGNED 10
21:52:24: 78744.632 CMAC_LOG_ADJUST_RANGING_OFFSET 2286
21:52:24: 78744.636 CMAC_LOG_RANGING_OFFSET_SET_TO 11896
21:52:24: 78744.638 CMAC_LOG_STATE_CHANGE ranging_2_state
21:52:24: 78744.644 CMAC_LOG_RNG_REQ_QUEUED 10
21:52:25: 78745.654 CMAC_LOG_RNG_REQ_TRANSMITTED
21:52:25: 78745.658 CMAC_LOG_RNG_RSP_MSG_RCVD
21:52:25: 78745.660 CMAC_LOG_RANGING_SUCCESS
21:52:25: 78745.680 CMAC_LOG_STATE_CHANGE dhcp_state
21:52:25: 78745.820 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS 10.1.4.65
21:52:25: 78745.824 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS 10.1.4.1
21:52:25: 78745.826 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS 10.1.4.1
21:52:25: 78745.830 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
21:52:25: 78745.834 CMAC_LOG_DHCP_TZ_OFFSET -28800
21:52:25: 78745.836 CMAC_LOG_DHCP_CONFIG_FILE_NAME disable.cm
21:52:25: 78745.840 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
21:52:25: 78745.846 CMAC_LOG_DHCP_COMPLETE
21:52:25: 78745.968 CMAC_LOG_STATE_CHANGE establish_tod_state
21:52:25: 78745.978 CMAC_LOG_TOD_REQUEST_SENT
21:52:26: 78746.010 CMAC_LOG_TOD_REPLY_RECEIVED 3192525217
21:52:26: 78746.018 CMAC_LOG_TOD_COMPLETE
21:52:26: 78746.020 CMAC_LOG_STATE_CHANGE security_associati

```

```

21:52:26: 78746.024 CMAC_LOG_SECURITY_BYPASSED
21:52:26: 78746.028 CMAC_LOG_STATE_CHANGE configuration_file
21:52:26: 78746.030 CMAC_LOG_LOADING_CONFIG_FILE disable.cm
21:52:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed state to up
21:52:27: 78747.064 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
21:52:27: 78747.066 CMAC_LOG_STATE_CHANGE registration_state
21:52:27: 78747.070 CMAC_LOG_REG_REQ_MSG_QUEUED
21:52:27: 78747.076 CMAC_LOG_REG_REQ_TRANSMITTED
21:52:27: 78747.080 CMAC_LOG_REG_RSP_MSG_RCVD
21:52:27: 78747.082 CMAC_LOG_COS_ASSIGNED_SID 1/10
21:52:27: 78747.088 CMAC_LOG_RNG_REQ_QUEUED 10
21:52:27: 78747.090 CMAC_LOG_NETWORK_ACCESS_DENIED
21:52:27: 78747.094 CMAC_LOG_REGISTRATION_OK
21:52:27: 78747.096 CMAC_LOG_STATE_CHANGE establish_privacy_state
21:52:27: 78747.100 CMAC_LOG_PRIVACY_NOT_CONFIGURED
21:52:27: 78747.102 CMAC_LOG_STATE_CHANGE maintenance_state
21:52:31: 78751.122 CMAC_LOG_RNG_REQ_TRANSMITTED
21:52:31: 78751.124 CMAC_LOG_RNG_RSP_MSG_RCVD
21:52:37: 78757.164 CMAC_LOG_RNG_REQ_TRANSMITTED
21:52:37: 78757.168 CMAC_LOG_RNG_RSP_MSG_RCVD
21:52:43: 78763.206 CMAC_LOG_RNG_REQ_TRANSMITTED
21:52:43: 78763.210 CMAC_LOG_RNG_RSP_MSG_RCVD
21:52:49: 78769.250 CMAC_LOG_RNG_REQ_TRANSMITTED
21:52:49: 78769.252 CMAC_LOG_RNG_RSP_MSG_RCVD

```

The output of this debug shows that the Network Access is DENIED.

```
Ubr7100# show cable modem detail
```

Interface	SID	MAC address	Max CPE	Concatenation	Rx SNR
Cable1/0/U0	7	0002.1685.b5db	10	yes	33.52
Cable1/0/U0	8	0002.fdfa.0a63	10	yes	33.24
Cable1/0/U0	9	0010.7bed.9b23	1	no	33.29
Cable1/0/U0	10	0010.7bed.9b45	1	no	33.23
Cable1/0/U0	11	0001.64ff.e47d	10	yes	33.20
Cable1/0/U0	12	0004.2752.ddd5	10	yes	33.44

Notice that the Max CPE for cable modems with special scopes is **1** and the rest are **10**. If you see the configuration of scope **platinum.cm**, it has 10 CPE specified; on the other hand, scope **disable.cm** has only 1 CPE specified. The pre-configured DOCSIS configuration file **silver.cm** has also only 1 CPE specified.

```
Ubr7111# show interface cable 1/0 modem 0
```

SID	Priv bits	Type	State	IP address	method	MAC address
7	00	modem	up	10.1.4.7	dhcp	0002.1685.b5db
8	00	modem	up	10.1.4.10	dhcp	0002.fdfa.0a63
9	00	host	unknown	172.16.29.2	static	00c0.4f97.61c5
9	00	modem	up	10.1.4.66	dhcp	0010.7bed.9b23
10	00	modem	up	10.1.4.65	dhcp	0010.7bed.9b45
11	00	modem	up	10.1.4.6	dhcp	0001.64ff.e47d
12	00	modem	up	10.1.4.9	dhcp	0004.2752.ddd5

To verify that the cable modems are getting the correct level of service, issue the **show cable qos profile** command.

```
Ubr7111# show cable qos profile
```

ID	Prio	Max upstream bandwidth	Guarantee upstream bandwidth	Max downstream bandwidth	Max tx burst	TOS mask	TOS value	Create by	B priv enab	IP prec. rate enab
1	0	0	0	0	0	0x0	0x0	cmts(r)	no	no
2	0	64000	0	1000000	0	0x0	0x0	cmts(r)	no	no
3	7	31200	31200	0	0	0x0	0x0	cmts	yes	no
4	7	87200	87200	0	0	0x0	0x0	cmts	yes	no

5	4	64000	0	512000	0	0x0	0x0	cm	no	no
6	0	1000	0	1600000	0	0x0	0x0	cm	no	no
7	0	128000	10000	10000000	1600	0x0	0x0	cm	no	no
8	0	0	0	0	0	0x0	0x0	mgmt	no	no
10	0	0	0	0	0	0x0	0x0	mgmt	no	no
12	0	0	100000000	0	0	0x0	0x0	mgmt	no	no

Notice that QoS ID 7 matches the configuration on platinum.cm:

```
cable config-file platinum.cm
service-class 1 max-upstream 128
service-class 1 guaranteed-upstream 10
service-class 1 max-downstream 10000
service-class 1 max-burst 1600
cpe max 10
timestamp
```

The same happens with the DOCSIS configuration of disable.cm:

```
Ubr7111# show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
10.1.4.6	0100.0164.ffe4.7d	Mar 08 2001 07:58 AM	Automatic
10.1.4.7	0100.0216.85b5.db	Mar 08 2001 07:58 AM	Automatic
10.1.4.9	0100.0427.52dd.d5	Mar 08 2001 07:58 AM	Automatic
10.1.4.10	0100.02fd.fa0a.63	Mar 08 2001 08:36 AM	Automatic
10.1.4.65	0100.107b.ed9b.45	Infinite	Manual
10.1.4.66	0100.107b.ed9b.23	Infinite	Manual

Related Information

- [Additional File Transfer Function Commands](#)
- [DOCSIS CPE Configurator](#)
- [Cisco IOS DHCP Server](#)
- [Cisco CMTS Configuration Commands](#)
- [Broadband Cable Technologies Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 08, 2006

Document ID: 29243
