

# Introduction to the Cisco Broadband Operating System

---

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

---

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

---

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

This chapter includes the following sections:

- CBOS Features
- CBOS User Interfaces
- CBOS Help System

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

The list below defines the terminology used in this chapter.

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

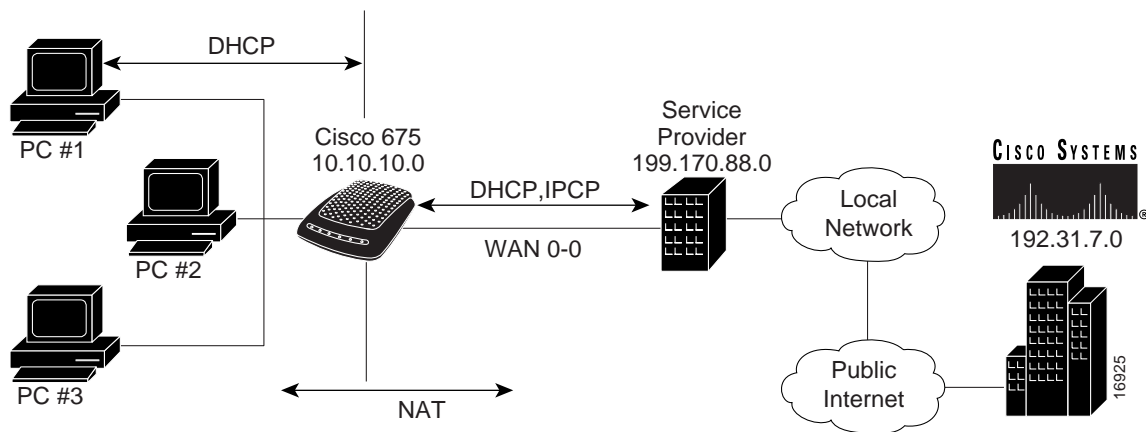
## 1.1 CBOS Features

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

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

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

**Figure 1-1 Configurationless Provisioning with DHCP and NAT**



## Benefits of Configurationless Provisioning

Configurationless provisioning provides:

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

---

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

---

### 1.1.1 Configurationless Provisioning Process

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

#### Understanding the DHCP Server and DHCP Client

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

- DHCP server
- DHCP client

## Using the Cisco 67x as a DHCP Server

When the Cisco 67x DHCP server operates in:

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

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

---

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

---

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

---

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

---

### Using the Cisco 67x as a DHCP Client

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

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

---

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

---

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

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

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

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

### Understanding NAT

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

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

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

---

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

---

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

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

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

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

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

### DHCP and NAT Together

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

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

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

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



---

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

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

---

## 1.1.2 Supported Applications

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

- Ping (packet Internet groper)

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

- RADIUS

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

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

- Livingston Enterprises RADIUS Version 2.01
- Sun Solaris Version 2.5
- Merit RADIUS (Sun binary)
- RADIUS NT (Microsoft)

#### Cisco 67x Implementation of the RADIUS Client:

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

- RIP (Routing Information Protocol)

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

- SYSLOG client

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

#### Implementing SYSLOG:

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

- Debug
- Info
- Warning
- Alarm
- Critical
- Crash

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

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

- Telnet server

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

- TFTP server

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

For security reasons, Cisco recommends that you disable the TFTP application, except when uploading or downloading a file. Typically, use TFTP to transfer new software from Cisco to your Cisco 67x, where the file name equals

`nsrouter.c67x.<version #>ima.hr`. You can also use TFTP to archive an image of your CBOS configuration file. This configuration file can be named anything you wish as long as you can view and edit the file with a standard text editor. Use the `.cfg` extension to make the configuration file easy to locate and to assure that it can be viewed and edited by a standard text editor. Archive an image of your configuration file before making changes to it so you can easily recover the old file if necessary. When uploading a configuration file to the 67x, you must name the configuration file `nsconfig.cfg` before uploading.

- Traceroute

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

- Web access

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

---

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

---

## 1.2 Using CBOS User Interfaces

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

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

## 1.3 Using the CBOS Help System

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

```
help [command-name]
```

or

```
? [command-name]
```

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

```
help show version
```

or

```
? show version
```