

Automated Internet Sign On with Cisco Network Registrar

This white paper explains the system described in the Cisco Network Registrar customer profile “Automated Internet Sign On at Boston College” (www.cisco.com/go/cnr). The core enabling technology of this automated Internet sign-on system is Cisco Network Registrar (CNR), a modern, extensible, feature-rich, integrated DHCP and DNS server. The methodology, architecture, and CNR configuration required for this system is discussed in detail. Using this white paper as a guide, you can configure CNR as the core of an Internet activation system similar to that used at Boston College.

Problem Statement

All IP networks face a common set of problems. These are similar to those faced by Boston College prior to the development of its automated Internet sign-on system, such as the need to:

- Provide hands-off, user-driven configuration of computers with correct IP addresses and network settings
- Configure large numbers of computers in short amounts of time
- Acquire information about the computers being configured on the network
- Control access to IP network resources
- Collect information to assist troubleshooting network and security events

The Cisco Network Registrar Solution

You can use CNR as the core technology in an automated Internet sign-on system to address each of the problems noted previously. Using open protocols, such as the Dynamic Host Configuration Protocol (DHCP), the Domain Name System (DNS), and the HyperText Transfer Protocol (HTTP), and a commonly available client application (any Web browser), the CNR solution will:

- Allow hands-off configuration of computers through the use of DHCP
- Allow configuration of large numbers of computers in a short time by making the configuration user-driven; for example, Boston College activated and configured more than 3000 computers in a single weekend with this system
- Acquire the MAC and IP addresses of a given computer, the name of the person activating the computer, as well as any other information (such as the operating system or hardware type) requested at the point of activation
- Control access to the network by preventing unknown users from activating a computer
- Allow quick troubleshooting by building a data store that contains the MAC address of a computer, its IP address, and the name of the person who activated it

DHCP has gained widespread acceptance as the method of choice for IP device configuration. Most commercially available operating systems ship with a DHCP stack installed, making the protocol ubiquitous. DHCP is attractive because it allows computers to be automatically configured with the correct IP address, net mask, router address, and various other parameters necessary to function correctly on the network. For more information on the DHCP protocol, consult the URLs listed in Appendix A.

However, DHCP used in its standard mode has one major drawback. To function in a hands-off manner, the DHCP server is usually configured to answer any DHCP packet seen by the server. This means that all computers are given equal levels of access to the network, and that there is no information that links a computer and its IP address to a specific individual.

The CNR DHCP server provides a solution to this DHCP drawback. It uses client-class functionality in order to provide differentiated service based on the computers MAC address. The result is that:

- Inactivated computers are given a temporary address and are not allowed access to all services on the network
- Activated computers are given a full set of network configuration parameters, allowing full access to the local area network (LAN), and, if applicable, to the Internet

Before discussing details of the design, it is advantageous to understand this activation system from both the user's and the network administrator's perspective.

User's Perspective

The CNR solution provides the end user with a simple process to activate the computer and be allowed full access to the network. The process is as follows:

- Ensure the computer is configured for DHCP
- Plug the computer into an active Ethernet port
- Reboot the computer
- Open a Web browser and connect to the activation page
- Provide identification, such as a username
- Provide any additional information requested by the activation page
- Click Activate This Computer (a button on the activation page)
- Wait 30 seconds or reboot the computer

This process typically takes a user only about three minutes. When complete, the computer is activated for full service on the network.

Administrator's Perspective

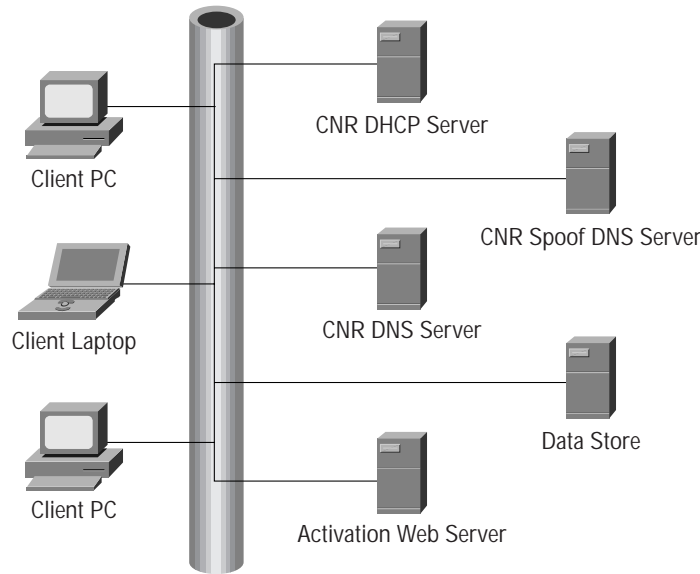
This system replaces many time-consuming and error-prone processes with a single, computerized process controlled by the activation system. Management of this activation system is extremely simple:

- Install and configure the CNR DHCP and DNS servers
- Install and configure a Web server
- Write and install the Common Gateway Interface (CGI) activation script
- Instruct users how to configure their computers to use DHCP
- Instruct users how to use the activation page
- Periodically check the status of the various CNR servers in the server complex, to ensure that they are functioning correctly
- Troubleshoot network and security events as necessary; because records are stored during the activation, a correlation exists between MAC and IP addresses and username, making the process much simpler than in the past

Architectural System Elements

The architecture of this system consists of five separate servers as shown in Figure 1.

Figure 1 Activation System Architecture



The operating system on which these servers are installed is a matter of customer preference. CNR runs on Windows NT Workstation and Server, Solaris, HP-UX, and AIX. Web server software (such as Microsoft IIS, Netscape FastTrack or Enterprise, or Apache) runs on a variety of operating systems.

The hardware selected for these servers is also largely a matter of customer preference. Hardware selection for CNR should follow the guidelines listed elsewhere in the product literature.

The processes that run on these servers are described in Table 1.

Table 1 Elements of the Activation System Architecture

Element	Description
Client PCs	End-user computers on the network
CNR DHCP Server	Answers DHCP packets for both inactivated and activated computers; can be co-hosted with CNR DNS server
CNR Spoof DNS Server	Answers DNS queries for inactivated computers and resolves all queries to the IP address of the activation Web server; can be cohosted with the activation Web server
CNR DNS Server	Answers DNS queries for activated computers; can be cohosted with CNR DHCP server
Data Store	Data store for the activation CGI to use for: <ul style="list-style-type: none"> • User credentials • Activation tracking (MAC † Username)
Activation Web Server	WWW server that serves the activation CGI; can be cohosted with CNR spoof DNS server

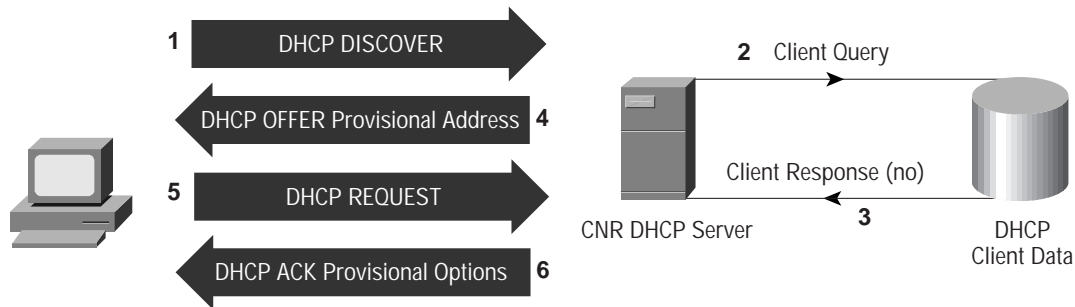
Process Flow

The processes in this activation system are presented here in Figures 2 through 5 as an end-to-end flow, broken into several discrete operations as follows:

- a) Initial client boot process
- b) Browser to activation server process
- c) CGI activation process
- d) Activated client boot process

Each operation is described in detail, with events listed and described in the order in which they occur.

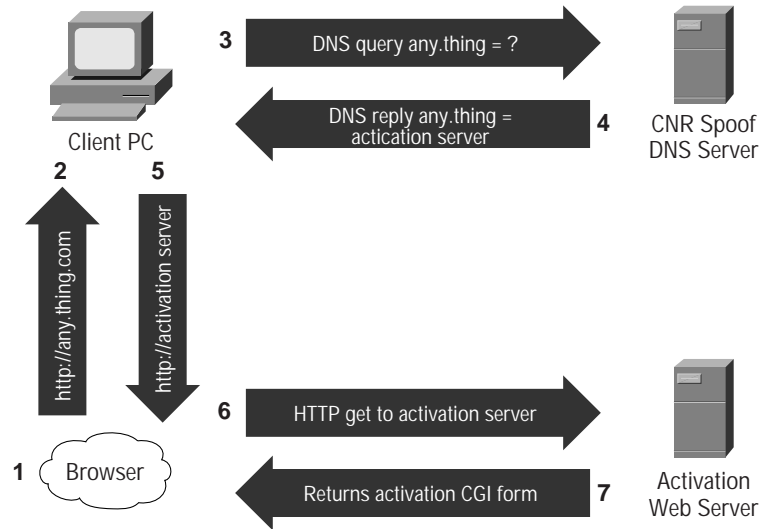
Figure 2 Initial Client Boot Process



1. The client boots onto the network and issues a DHCP DISCOVER. As specified in the RFC, the DISCOVER packet contains the client's MAC address. The DHCP server receives the DHCP DISCOVER. If the network is routed, the router receives the DHCP packet and forwards it to the configured IPHelper (BOOTP relay) address, which is the address of the DHCP server.
2. The DHCP server, configured for client-class processing, looks up the client's MAC address to see if there is a client associated with it.
3. Because this is an inactivated device, there is no client entry for the MAC address. Therefore, the DHCP server uses the default client rule set.
4. Using this default rule set, the DHCP server builds a DHCP OFFER packet and sends it to the client. The DHCP OFFER packet contains a provisional or temporary IP address, with DNS resolution handled by a spoof DNS server. The client receives the DHCP OFFER.
5. The client issues a DHCP REQUEST for a lease on the IP address in the OFFER.
6. The DHCP server performs steps 2 and 3 again (it does this for all inbound packets) and then builds the DHCP ACK packet, containing lease information and the default (inactivated) set of DHCP options.

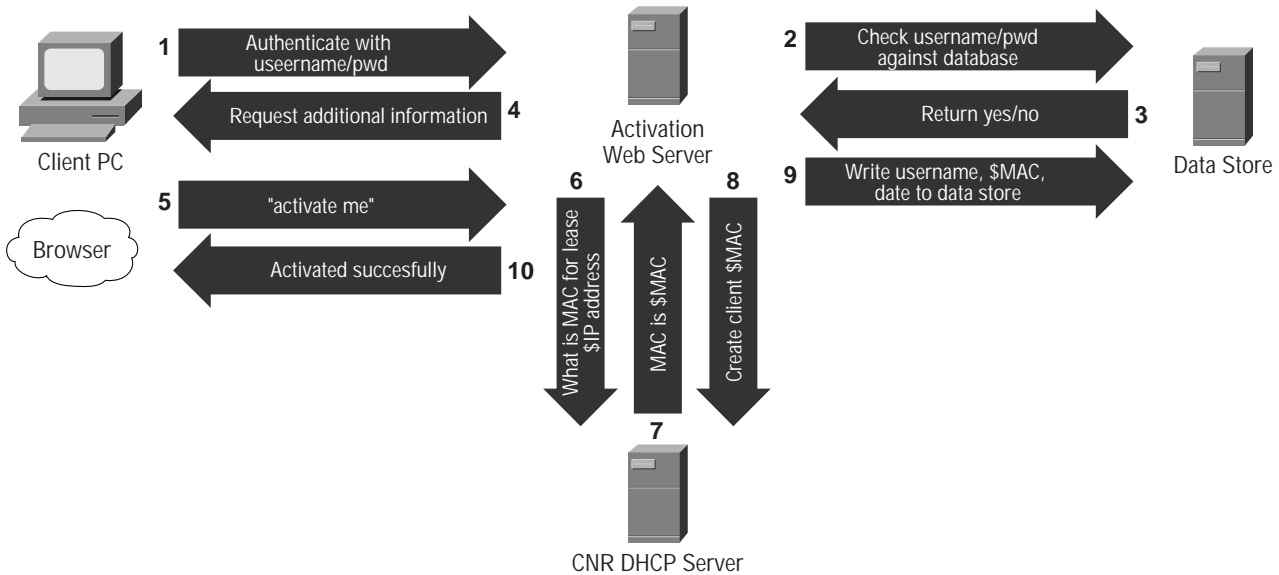
Note: Because the client did not receive the full set of DHCP options in the reply, not all functionality is present in this provisional state. Also, because the client was served a spoof DNS server address, hostname resolution is short-circuited, and all DNS queries from this inactivated computer are answered with the IP address of the activation Web server.

Figure 3 Browser to Activation Server Process



1. The user opens a Web browser.
2. The browser issues an HTTP request for its configured home page (can be any Web page).
3. The client DNS resolver attempts to resolve the hostname in this URL, sending a DNS query to the CNR spoofer DNS server.
4. The CNR spoofer DNS server resolves all hostnames to the IP address of the activation Web server.
5. The HTTP query now goes to the activation Web server instead of to the configured home page.
6. The browser sends its request to the activation Web server.
7. The activation Web server answers with the CGI activation form.

Figure 4 CGI Activation Process

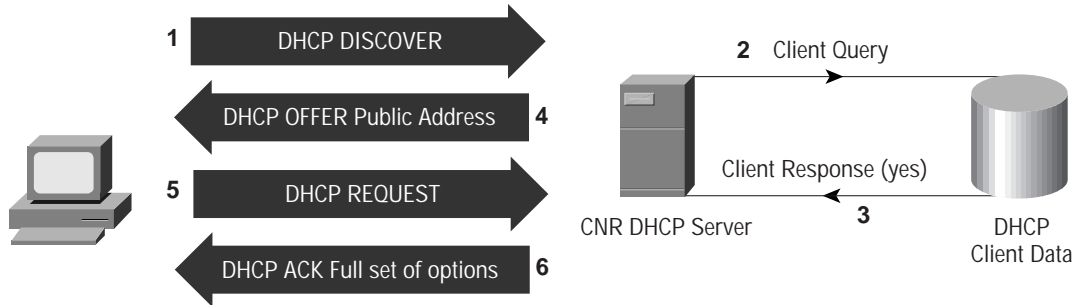


1. The user enters a username (and possibly some other credentials) and submits the CGI form.
2. The CGI form checks the username against a data store.
3. The data store returns a Yes or No verification (The answer Yes is assumed in example).

4. The CGI form sends the next screen of information, asking for additional information, such as computer type, location, department, and so on.
5. The user completes the required fields and submits the form.
6. The CGI determines the IP address of the client from HTTP meta-variables. It uses this IP address to query the CNR DHCP server, requesting the MAC associated with that IP address.
7. The CNR DHCP server returns the MAC address to the CGI script.
8. The CGI script issues a command to the CNR DHCP server, telling it to create a client entry for this MAC address.
9. The CGI script writes a record out to the data store with the username, the MAC address, the date, and any additional information that the CGI collected.
10. The CGI script sends the next screen of information, informing the user that the computer has been activated.

Note: The verification mechanism could be a secure username/password pair known to the user. The CGI uses this to authenticate the user. The decision of which data and data store to use will change with each implementation of this design, so this discussion does not focus on data modeling, access issues or authentication mechanisms.

Figure 5 Activated Client Boot Process



1. The client reboots and issues a DHCP DISCOVER. The CNR DHCP server receives the DHCP DISCOVER.
2. The CNR DHCP server, configured for client-class processing, looks up the MAC address to see if there is a client associated with it. Because this client is now activated, there is a MAC address associated with it.
3. The CNR DHCP server uses the rule set associated with this client to process the packet.
4. The CNR DHCP server builds and sends a DHCP OFFER packet to the client. This time, the OFFER contains a valid IP address, allowing access to all network resources. The client receives the DHCP OFFER.
5. The client issues a DHCP REQUEST for a lease on the IP Address in the OFFER.
6. The CNR DHCP server performs steps 2 and 3 again and then builds the DHCP ACK packet, containing lease information and the full set of DHCP options.

Cisco Network Registrar Configuration In Brief

To build the system explained in this white paper, you must slightly modify the CNR configuration from the out-of-the-box settings, enabling some of the server's advanced features. You can most easily and quickly accomplish this using the CNR graphical user interface (GUI).

For information on how to install CNR, consult the CNR Getting Started Guide.

For more information on how to use the GUI, consult the CNR GUI User's Guide.

You can find all of the other CNR production documentation at:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/>



The following sections explain how to modify the CNR configuration to build an Internet sign-on application. The overall process involves configuring both the DHCP and the DNS servers as outlined here.

DHCP

1. Configure two new DHCP policies.
2. Configure a test scope.
3. Enable client-class processing and create a client class for activated computers.
4. Create a default client for inactivated computers.
5. Reload the DHCP server.

DNS

1. Configure the DNS server as a standard DNS server.
2. Set up a spoof DNS server.

The remainder of this section explains these steps in detail.

Configuring the DHCP Server

You must configure the DHCP server to use client-class processing. The following example will work to test the proof of concept. Since this example only has one scope configured, you will have to expand it to support an enterprise network. However, the basic configuration details stay the same. Use the GUI to accomplish these tasks.

1a. Configure a new DHCP policy for inactivated clients

- Click the DHCP server icon.
- Click the Show Properties button.
- Click the Policies tab.
- Click New.
 - In the Name field, enter “inactivated.”
 - Accept Copy from: default
 - Click OK.

The Policies tab will now allow you to edit the inactivated policy.

- Set the Lease Time to 0 days, 0 hours, 1 minute.
- Set the Grace Period to 0 days, 0 hours, 5 minutes
- Click on the Edit Options button.
 - In the Basic option group, click domain-name-servers.
 - Click Add.
 - Enter the IP address of the spoof DNS server.

In a routed network it may be necessary to also configure the routers option, with the appropriate router interface address on a per-scope basis.

- Click OK, then click Yes to commit the changes to this policy.

1b. Configure a new DHCP policy for activated clients.

While still in the DHCP Policies tab:

- Click New again.
 - In the Name field, enter “activated.”
 - Select Copy from: default.
 - Click OK.

The Policies tab will now allow you to edit the activated policy.

- Set the Lease Time to 10 days, 0 hours, 0 minutes.
- Set the Grace Period to 1 day, 0 hours, 0 minutes.
- Click Edit Options.
 - In the Basic option group, click domain name servers.
 - Click Add.
 - Enter the IP addresses of the real DNS servers.

Also configure the DHCP option-value pairs necessary for computers to function correctly on this network. This will vary by network and also across different DHCP clients.

- Click OK, and then click Yes to commit the changes to this policy.
- Click Close.

These two policies will be used in steps 3 and 4.

2. Configure a test scope

In order to serve any addresses to test DHCP clients, you must first configure a test scope. Take care when configuring this scope, because as soon as there are addresses in a scope, the DHCP server begins to respond to any valid DHCP packets it sees on the wire. This portion of the testing should be done on a standalone Ethernet hub or a test VLAN, so that it will not impact real DHCP clients on the enterprise LAN.

- Click on the DHCP server icon.
- Click Add.
- In the Name field, provide a name for this scope (for example, Test_Scope).
- Select the default policy.
- Provide the Network Number of this scope (the network number of the subnet it will serve, for example 10.100.200.0).
- Provide the Net Mask of this scope (for example, the network mask of the subnet it will serve, such as 255.255.255.0).
- Provide a Start Address and End Address to define this scope's range of IP addresses (for example, 10.100.200.10, 10.100.200.250).
- Click OK.

There is now a test scope configured in the example case serving the network 10.100.200.0/24.

3. Enable client-class and configure client class for activated computers.

- Click the DHCP server icon.
- Click the Show Properties button.
- Click the Scope Selection Tags tab.
- Click in the Enable client class processing check box.
- Click the Client-Classes tab.
- Click Add.
 - In the Client-class field, enter the name “activated.”
 - In the Policy Name field, select “activated.”
- Click OK.

4. Create a Default client for inactivated computers.

- Click the Clients tab.
- Click Add.
 - In the MAC Address field, enter the word “default.”
 - In the Policy Name field, select “inactivated.”
- Click OK.

5. Reload the DHCP server.

- Close the Server Properties window by clicking OK.
- Click on the DHCP server icon.
- Click Control.
 - Select Reload.
- Click OK.
 - The Server Control Window will say “DHCP@hostname server restarted.” Close this window by clicking OK.

Configuring the DNS Servers

1. Real DNS server configuration

Configure the real DNS server (as opposed to the spoof DNS server) as a standard DNS server. For more information regarding how to configure DNS servers, consult the CNR Getting Started and User's guides.

2. Spoof DNS server configuration

The *spoof* DNS server ensures that all HTTP queries are sent to the activation server. To set up the spoof DNS server, you will need to know the hostname and IP address of the spoof DNS server itself and the IP address of the activation server.

The spoof DNS server must be set up on a separate server from the real DNS server.

- Delete any Forward or Reverse zones, but not the Loopback zone.
- Click on the DNS server icon, then click the Show Properties button.
- In the Properties window, click the Root Name Servers tab.
 - Delete all of the root name servers and their IP addresses. This prevents the spoof DNS server from forwarding requests to other DNS servers.
- In the Properties window, click the Options tab.
 - Deselect all the options in this window.
- In the Properties window, click the Advanced tab.
 - Deselect all the check-boxes in this window.
- Click OK.
- Click the DNS server icon again.
- Click Add.
- In the Name field, enter a single dot (.).
- Click OK. The Add Primary DNS Zone dialog box appears (in the SOA tab).
 - In the Contact Email Address field, enter the e-mail address of the administrator, replacing the @ sign with a dot (.), and adding a trailing dot at the end of the address; for example, “username@example.com” becomes “username.example.com.”
 - In the Primary Name Server field, enter the FQDN of the server on which the spoof DNS server resides, followed by a trailing dot (.); for example, “server10.example.com.”
- Click the Name Servers tab, and then click Add.
 - In the Name field, enter the FQDN of the server on which the spoof DNS server resides, followed by a trailing dot (.); for example “server10.example.com.”
 - Click OK.
- Click the Hosts tab, and then click Add.
 - In the Name field, enter the FQDN of the activation Web server without a trailing dot; for example, “pweb.example.com.”
 - In the Addresses column, enter the IP address of the activation Web server.
 - In the Aliases column, enter the following three aliases, each on a separate line:
 - “*”
 - “*.*”
 - “*.*.*”

- Click OK.
- Click Close.
- Reload the DNS server:
 - Click the DNS server icon again.
 - Click Control.
 - After the server reloads, the Server Control Results window will say “DNS@hostname has reloaded.” Close this window by clicking OK.
- Verify that the spoof DNS server is functioning using nslookup. The server should return the A record for the activation server, regardless of the hostname used for the query; for example, “do.ray.me” should return “pweb.example.com.”

The spoof DNS server is now fully functional.

DHCP Server CLI Callouts

This section explains the interaction between the CGI application and the CNR command line interface “nrcmd.”

The CGI application is not discussed in detail here because it will change at each implementation due to differences in the CGI development environments at various enterprises. However, regardless of the development environment, the callouts that the CGI script makes to the DHCP server are the same. These callouts use nrcmd, the Cisco Network Registrar command line interface (CLI). You can access the nrcmd CLI directly from the system on which the CGI resides, or you can reach it on a remote system using an rshell command. These are as follows:

Scenario 1: The CGI wants to know the MAC address associated with a given lease.

```
nrcmd -C <cluster name> -N <admin username> -P <password> lease <ip address> macaddr
```

Example:

```
nrcmd -C <cluster name> -N <admin username> -P <password> lease 123.34.67.8 macaddr
```

Returns:

```
1.6.00:08:b3:56:21
100 OK
```

Scenario 2: The CGI wants to create a DHCP client for a given MAC address.

```
nrcmd -C <cluster name> -N <admin username> -P <password> client <MAC address> create
  client-class-name=activated
```

Example:

```
nrcmd -C <cluster name> 0N <admin username> -P <password> client 1,6,00:08:b3:56:21 create
  client-class-name=activated
```

Returns:

```
100 OK
```

Scenario 3: The CGI wants to know the IP address leased to a given MAC address (used for troubleshooting).

```
nrcmd -C <cluster name> -N <admin username> -P <password> lease withMACaddr <MAC address>
```

Example:

```
nrcmd -C <cluster name> -N <admin username> -P <password> lease withMACaddr 1,6,00:80:08:B3:56:21
```

Returns:

```
123.45.67.8
100 OK
```

For more information on the CLI, consult the CNR CLI Reference Guide.

Appendix A: Additional Sources of Information

The following information about the CNR product is currently available, as of February 1999, as listed in Table 2.

Table 2 Network Registrar Product Information Available

Item	URL
CNR Software	ftp://www.cisco.com/cisco/netmgmt/network-registrar/
CNR Manuals	http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/nr/
DHCP and DNS RFCs	http://info.internet.isi.edu/in-notes/rfc/files



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

Americas
Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela