StadiumVision

Cisco StadiumVision
Cisco Network Registrar Implementation Guide

All Releases

March 2010

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Table of Contents

Preface

Document Purpose

This document describes the details around using Cisco Network Registrar (CNR) in the Cisco StadiumVision Deployment.

Document Audience

This document is written for installers, designers, and system engineers.

Related Docmentation

- User Guide for Cisco Network Registrar, 7.1, http://www.cisco.com/en/US/docs/net_mgmt/network_registrar/7.1/user/guide/cnr71book.html

Document History

Table 1. Revision History

Date	Descripton
03/23/10	First publication for Cisco StadiumVision Director Release 2.0.

Chapter 1 Overview

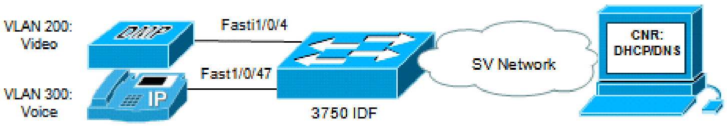
The Cisco Network Registrar (CNR) provides a feature-rich DHCP and DNS server that can be used in the Cisco StadiumVision network.

The CNR provides:

- A central DHCP server for distributing IP addresses.
- A database for tracking device IP address, associated switch and connected port.
- A report containing device scope, IP address, switch ID, and port information that can be married with the wiring schedules provided by the installation partner.
- Added security by filtering IP address assignment based on MAC address (future).
- Automatic DNS name assignment and populating the embedded DNS server with the device DNS name so devices may be connected to and managed by name (future).
- IP address per switch port assignment (future).

Figure 1 provides a conceptual view of how CNR fits into the Cisco StadiumVision network.

Figure 1. Cisco StadiumVision Network Plus CNR



In this illustration, only a Voice and Video VLANs are shown for simplicity. CNR may also be used to provide IP addressing for other VLANs within the venue.

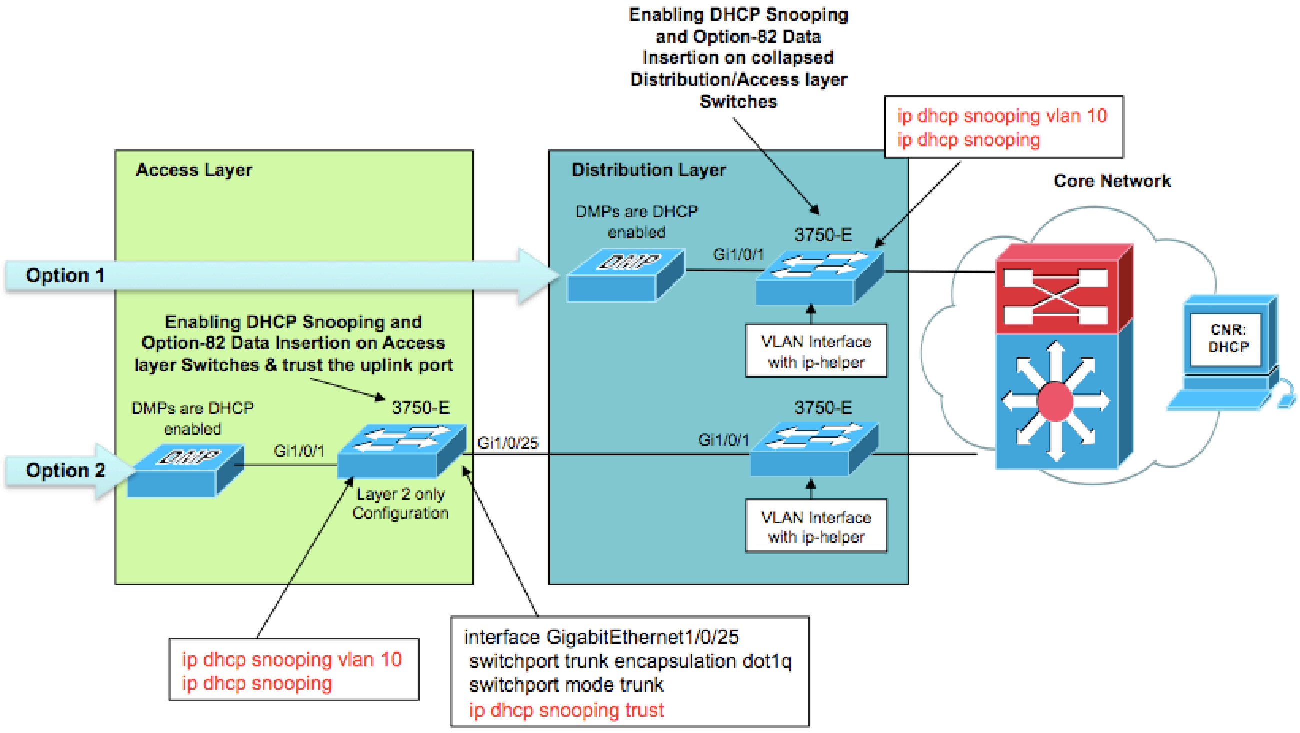
Chapter 2 Switch Configuration

Two common network designs are currently employed at the venues:

- A two-layer design, where the Access and Distribution layers are collapsed together and connected to the Core (shown as Option 1 in Figure 2).
- A three-layer design, where a separate Access layer of switches is used for aggregating endpoints (shown as Option 2 in Figure 2).

These two designs require a slightly different configuration of the switches to enable CNR as the DHCP server for the Cisco StadiumVision network.

Figure 2. Two-Layer (Option 1) verses Three-Layer (Option 2) Network Design


Enabling DHCP Snooping and Option-82 Data Insertion on collapsed Distribution/Access layer Switches
Access Layer
Distribution Layer
Core Network
Option 1
Option 2
DMPs are DHCP enabled
3750-E
Gi1/0/1
DMP
VLAN Interface with ip-helper
CNR: DHCP
Enabling DHCP Snooping and Option-82 Data Insertion on Access layer Switches & trust the uplink port
DMPs are DHCP enabled
3750-E
Gi1/0/1
Gi1/0/25
3750-E
Gi1/0/1
Layer 2 only Configuration
VLAN Interface with ip-helper

```
ip dhcp snooping vlan 10
ip dhcp snooping
```

```
ip dhcp snooping vlan 10
ip dhcp snooping
```

```
interface GigabitEthernet1/0/25
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
```

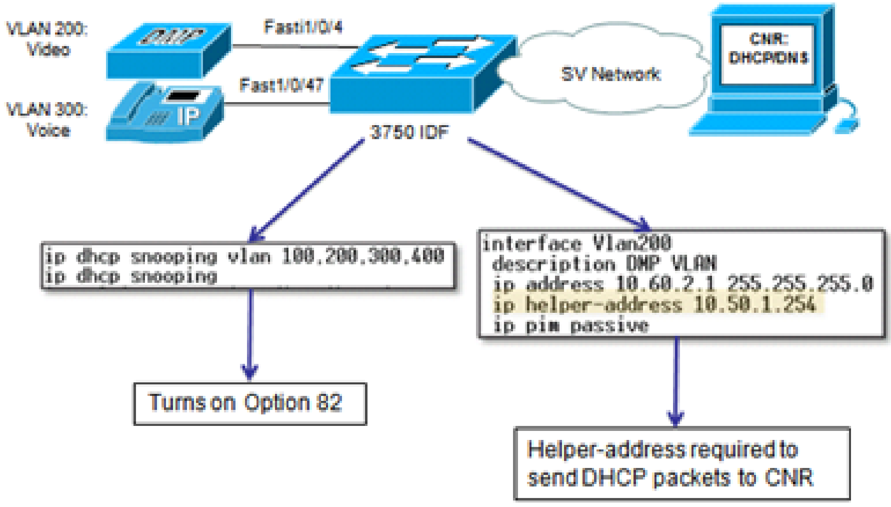
Option 1 DHCP Snooping and Helper Address Configuration

In the two-layer network design (represented by Option 1), the Cisco Catalyst 3750-E switch that is directly connected to the endpoint devices (e.g., DMPs, IP Phones), is configured for DHCP snooping at a global level and for each of the applicable VLANs.

Also, the VLAN interface is configured with an “ip helper-address” of the CNR server to direct DHCP packets to the CNR over the Cisco Connected Stadium network.

Figure 3 provides an illustration of this configuration.

Figure 3. Switch Configuration for DHCP Option 82 and Helper Address



```
ip dhcp snooping vlan 100,200,300,400
ip dhcp snooping
```

Turns on Option 82

```
interface Vlan200
 description DMP VLAN
 ip address 10.60.2.1 255.255.255.0
 ip helper-address 10.50.1.254
 ip pim passive
```

Helper-address required to send DHCP packets to CNR

The “ip dhcp snooping vlan …” global configuration command must be configured for the VLANs where DHCP snooping is desired. This command currently supports the option to specify one VLAN, a group of comma-separated VLANs, or a VLAN range.

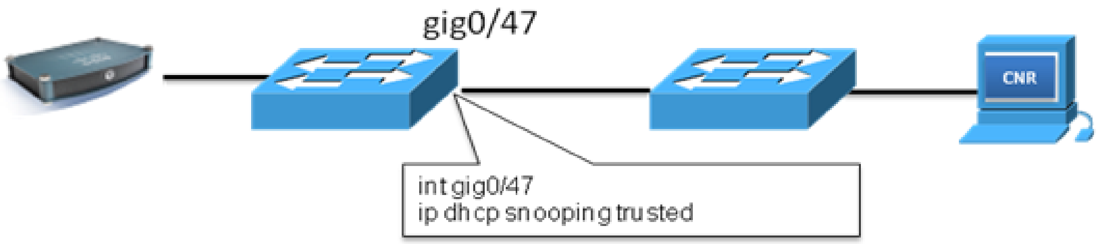
For DHCP snooping to be active on a switch, both configuration commands must be entered. If the general “ip dhcp snooping” is removed from the configuration, any configured “ip dhcp snooping vlan” commands will remain in the switch configuration, but DHCP snooping will not function on the switch.

Option 2 DHCP Snooping Configuration and Trusted Port

In the three-layer network design (represented as Option 2), the Cisco Catalyst 3750-E switch that is directly connected to endpoint devices (e.g. DMPs, IP Phones) is globally configured for DHCP snooping (similar to the configuration shown in Figure 3).

In addition, the uplink port must be configured to trust the DHCP traffic that traverses it. Figure 4 provides an illustration of this configuration.

Figure 4. Switch Configuration for the Uplink as a DHCP Trusted Port



```
int gig0/47
ip dhcp snooping trusted
```

In the three-layer design, only the distribution switch contains the “ip helper-address” configuration for the VLAN interface to forward the DHCP requests to CNR.

If DHCP snooping is enabled on both the Distribution and Access Layer switches, DHCP snooping on the Distribution switch will drop DHCP packets that have the option-82 information appended to the DHCP data. To allow the DHCP packets to be forwarded or relayed by the Distribution switch to CNR via the ip-helper address command, the VLAN interface must be configured to trust the Option 82 information, as illustrated in the following example.

```
interface Vlan200
  description DMP VLAN
  ip dhcp relay information trusted ß only required if DHCP Snooping is on
both the Distribution and Access Switches
  ip address 10.60.2.1 255.255.255.0
  ip helper-address 10.50.1.254
  ip pim passive
```

Below is an example of properly configured DHCP snooping with one trusted uplink:

```
Switch>show ip dhcp snooping
Switch DHCP snooping is enabled     ß result of “ip dhcp snooping”
DHCP snooping is configured on following VLANs:
10                                  ß result of “ip dhcp snooping vlan 10”
DHCP snooping is configured on the following Interfaces:

Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     -----------
GigabitEthernet0/47          yes         unlimited  ß result of “ip dhcp snooping trusted”


Switch>show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------
00:0F:44:01:0E:95   172.16.102.6     429171      dhcp-snooping   10    GigabitEthernet0/33
00:0F:44:01:0E:49   172.16.102.4     427725      dhcp-snooping   10    GigabitEthernet0/1
00:0F:44:01:41:00   172.16.102.29    604686      dhcp-snooping   10    GigabitEthernet0/31
00:0F:44:01:0E:C6   172.16.102.10    493607      dhcp-snooping   10    GigabitEthernet0/7
00:0F:44:01:0E:97   172.16.102.3     426769      dhcp-snooping   10    GigabitEthernet0/35
00:0F:44:01:0E:9E   172.16.102.7     590252      dhcp-snooping   10    GigabitEthernet0/15
Total number of bindings: 6
```

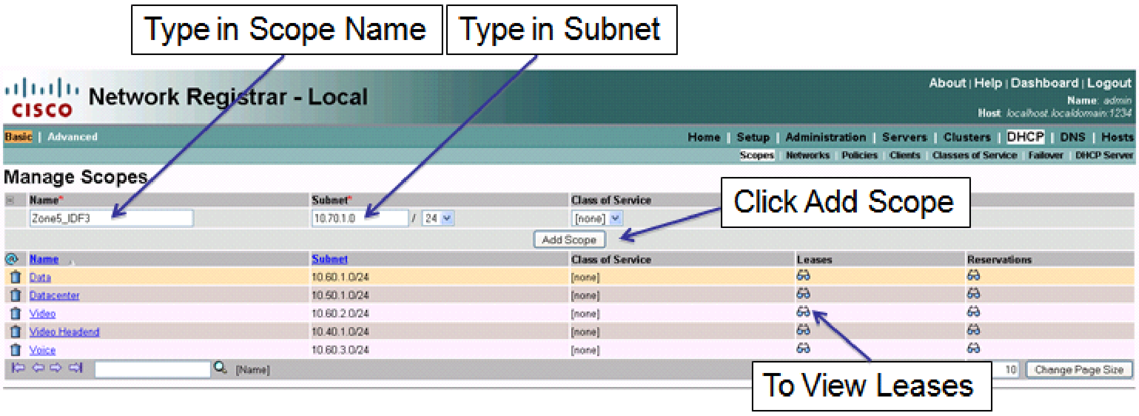
Chapter 3 DHCP Scopes

This chapter describes the basic DHCP configuration for a Cisco StadiumVision CNR deployment.

- From the IP address plan for the venue, DHCP IP scopes are created to assign IP addresses to the devices as they are connected to the Cisco StadiumVision network.
- User-friendly names should be used to make it simple to identify (by the Scope name) where the device is located.
- Wiring schedule nomenclature should be used to provide consistency between the reports generated from the CNR database and the wiring schedule.

To configure DHCP Scopes:

1. Select on **DHCP > Scopes** to add IP address scopes to CNR.
2. After devices have received an IP address lease, click on the eye glasses under Leases column to view the lease.



Type in Scope Name

Type in Subnet

Click Add Scope

To View Leases

Manage Scopes

Name*: Zone5_IDF3

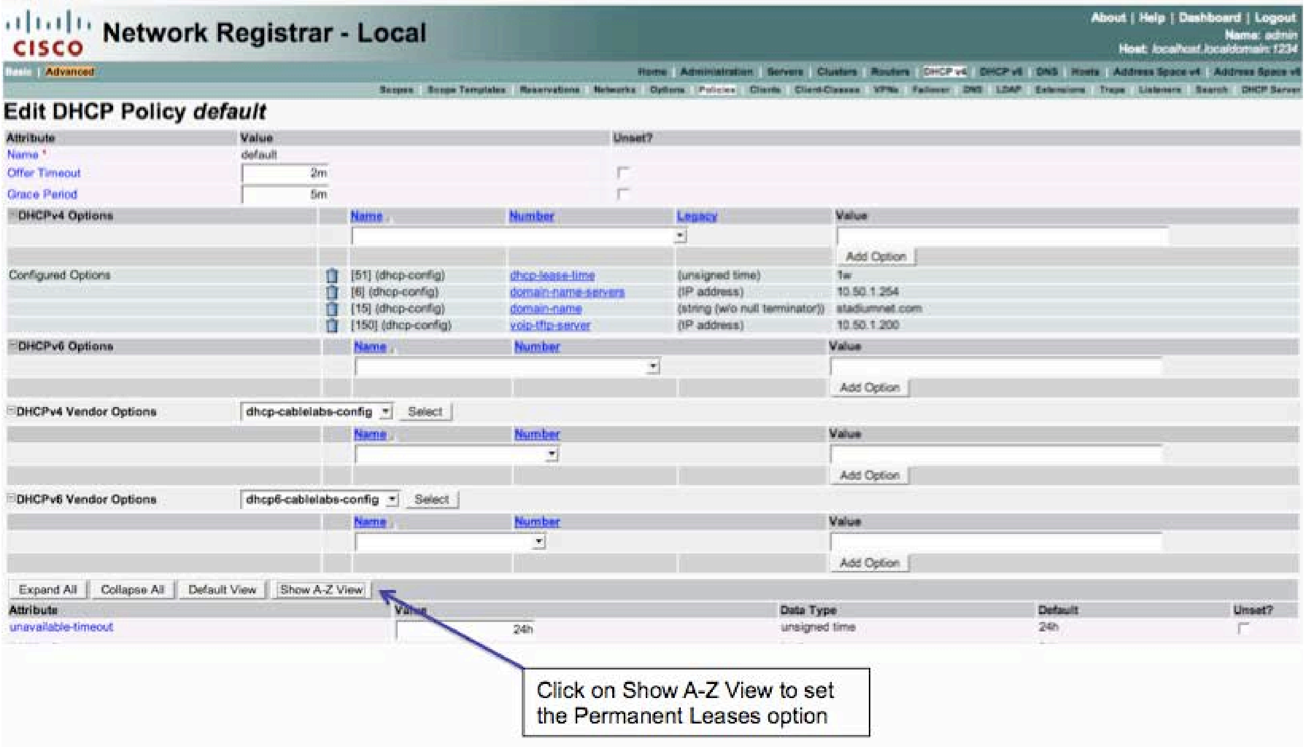
Subnet*: 10.70.1.0 / 24

Class of Service: [none]

Name	Subnet	Class of Service	Leases	Reservations
Data	10.60.1.0/24	[none]	👓	👓
Datacenter	10.50.1.0/24	[none]	👓	👓
Video	10.60.2.0/24	[none]	👓	👓
Video Headend	10.40.1.0/24	[none]	👓	👓
Voice	10.60.3.0/24	[none]	👓	👓

cisco
Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Setup | Administration | Servers | Clusters | DHCP | DNS | Hosts
Scopes | Networks | Policies | Clients | Classes of Service | Failover | DHCP Server
Add Scope
[Name]
10
Change Page Size

3. To assign an IP address permanently to a device, select **DHCPv4 > Policies > default > Show A-Z View**.


Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | DNS | Hosts | Address Space v4 | Address Space v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | Extensions | Traps | Listeners | Search | DHCP Server
Add Option
Select
Expand All
Collapse All
Default View
Show A-Z View

Edit DHCP Policy *default*

Attribute	Value	Unset?
Name *	default	
Offer Timeout	2m	□
Grace Period	5m	□

DHCPv4 Options	Name	Number	Legacy	Value
Configured Options	[51] (dhcp-config)	dhcp-lease-time	(unsigned time)	1w
	[6] (dhcp-config)	domain-name-servers	(IP address)	10.50.1.254
	[15] (dhcp-config)	domain-name	(string (w/o null terminator))	stadiumnet.com
	[150] (dhcp-config)	voip-tftp-server	(IP address)	10.50.1.200

DHCPv6 Options — Name, Number, Value

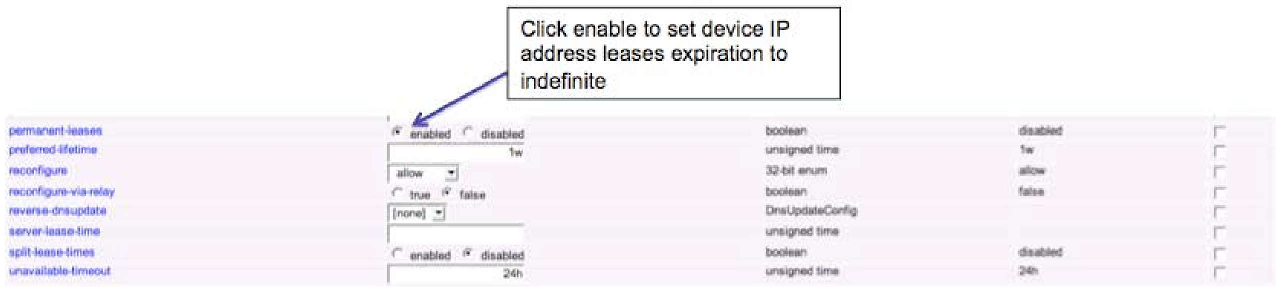
DHCPv4 Vendor Options: dhcp-cablelabs-config — Name, Number, Value

DHCPv6 Vendor Options: dhcp6-cablelabs-config — Name, Number, Value

Attribute	Value	Data Type	Default	Unset?
unavailable-timeout	24h	unsigned time	24h	□

Click on Show A-Z View to set the Permanent Leases option

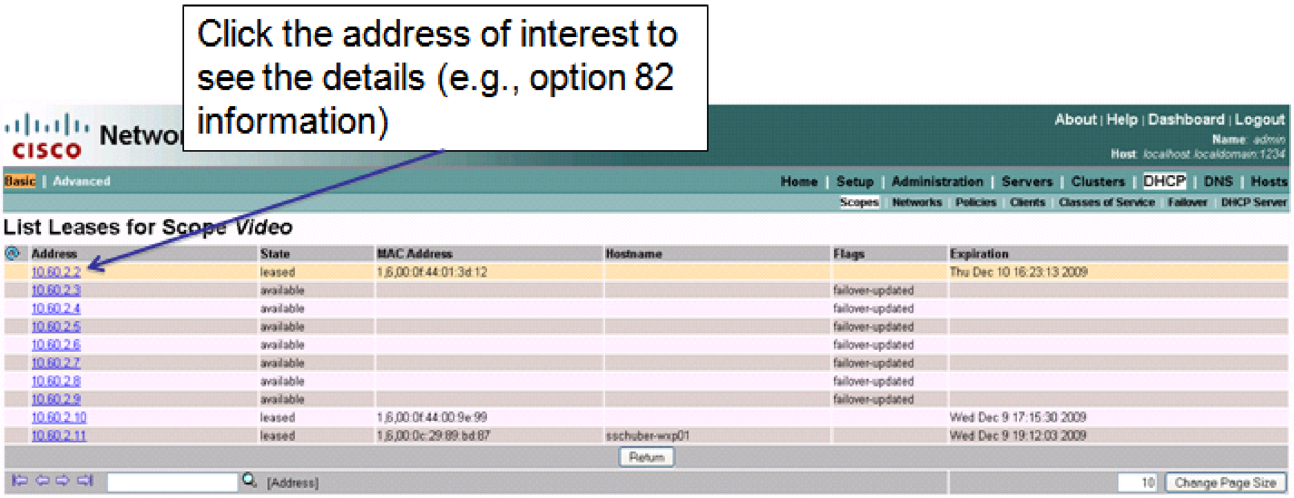
4. Select **Enable** beside “permanent-leases.”



Click enable to set device IP address leases expiration to indefinite

permanent-leases	● enabled ○ disabled	boolean	disabled	□
preferred-lifetime	1w	unsigned time	1w	□
reconfigure	allow	32-bit enum	allow	□
reconfigure-via-relay	○ true ● false	boolean	false	□
reverse-dnsupdate	[none]	DnsUpdateConfig		□
server-lease-time		unsigned time		□
split-lease-times	○ enabled ● disabled	boolean	disabled	□
unavailable-timeout	24h	unsigned time	24h	□

5. To verify the configuration, click on the IP address of interest to view the lease.

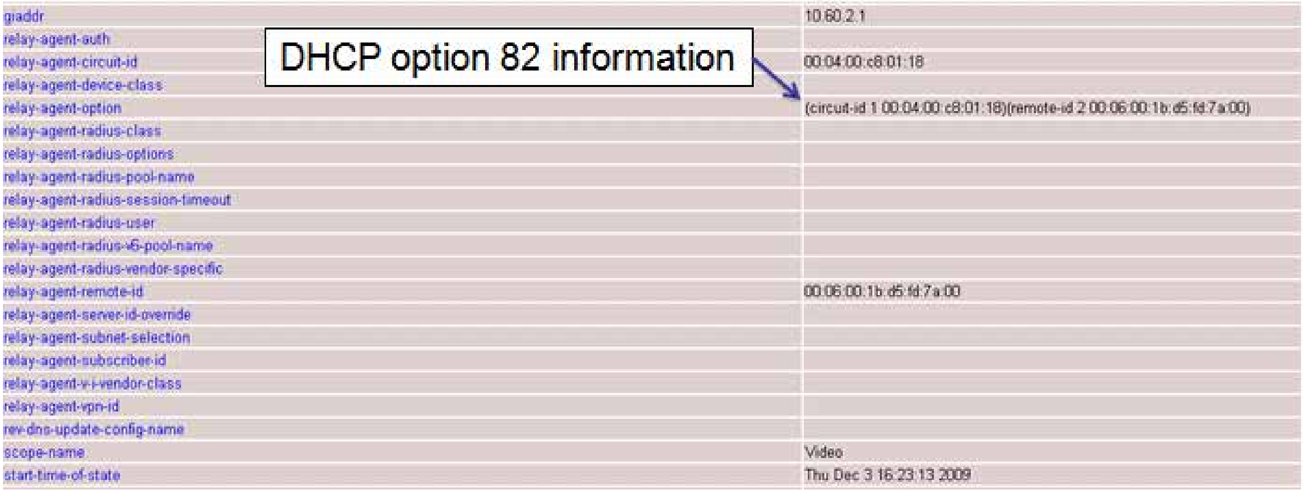

Netwo
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Setup | Administration | Servers | Clusters | DHCP | DNS | Hosts
Scopes | Networks | Policies | Clients | Classes of Service | Failover | DHCP Server
Return
[Address]
10
Change Page Size

Click the address of interest to see the details (e.g., option 82 information)

List Leases for Scope *Video*

Address	State	MAC Address	Hostname	Flags	Expiration
10.60.2.2	leased	1,6,00:0f:44:01:3d:12			Thu Dec 10 16:23:13 2009
10.60.2.3	available			failover-updated	
10.60.2.4	available			failover-updated	
10.60.2.5	available			failover-updated	
10.60.2.6	available			failover-updated	
10.60.2.7	available			failover-updated	
10.60.2.8	available			failover-updated	
10.60.2.9	available			failover-updated	
10.60.2.10	leased	1,6,00:0f:44:00:9e:99			Wed Dec 9 17:15:30 2009
10.60.2.11	leased	1,6,00:0c:29:89:bd:87	sschuber-wxp01		Wed Dec 9 19:12:03 2009

6. Scroll down to Advanced and expand that section to see the DHCP option 82 information.



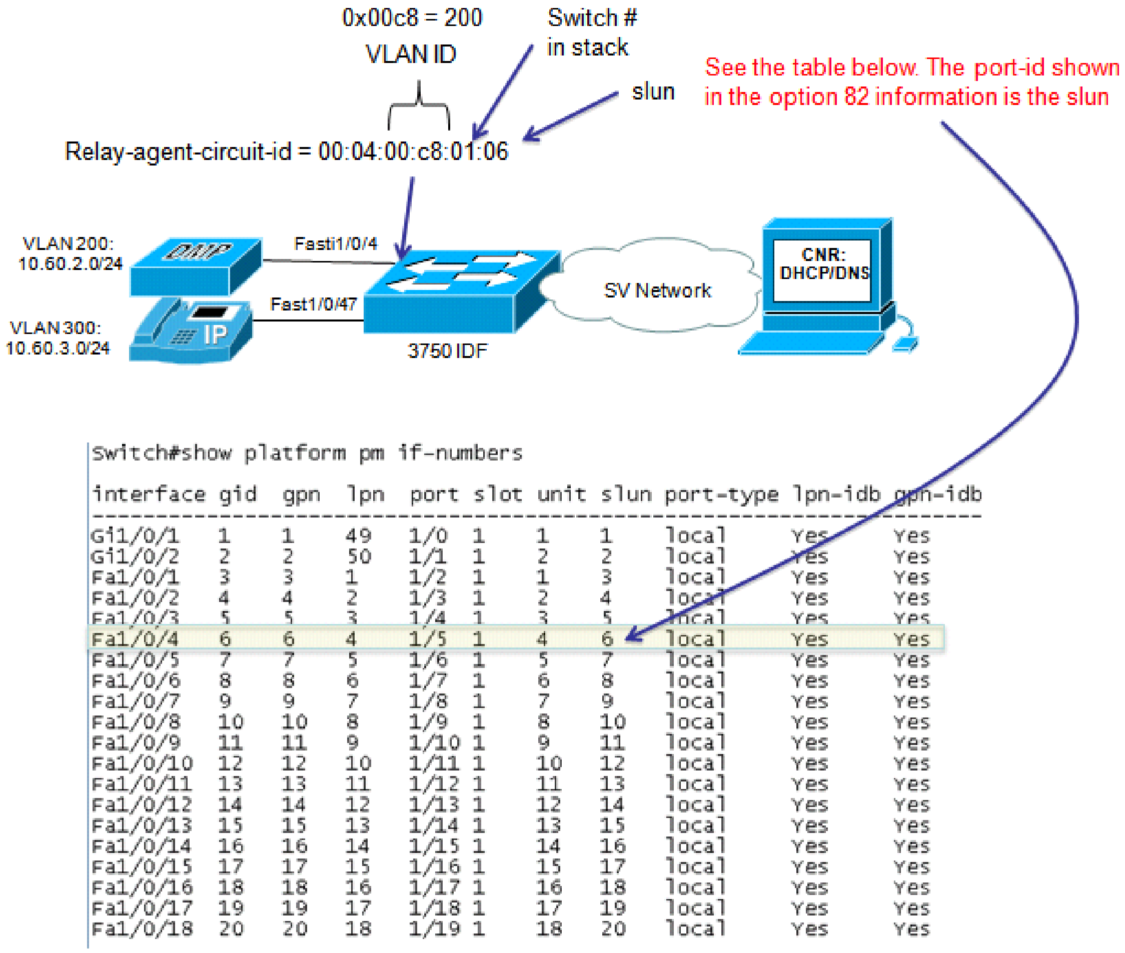
DHCP option 82 information

giaddr	10.60.2.1
relay-agent-auth	
relay-agent-circuit-id	00:04:00:c8:01:18
relay-agent-device-class	
relay-agent-option	(circuit-id 1 00:04:00:c8:01:18)(remote-id 2 00:06:00:1b:d5:fd:7a:00)
relay-agent-radius-class	
relay-agent-radius-options	
relay-agent-radius-pool-name	
relay-agent-radius-session-timeout	
relay-agent-radius-user	
relay-agent-radius-v6-pool-name	
relay-agent-radius-vendor-specific	
relay-agent-remote-id	00:06:00:1b:d5:fd:7a:00
relay-agent-server-id-override	
relay-agent-subnet-selection	
relay-agent-subscriber-id	
relay-agent-v-i-vendor-class	
relay-agent-vpn-id	
rev-dns-update-config-name	
scope-name	Video
start-time-of-state	Thu Dec 3 16:23:13 2009

Reading DHCP Option 82 Information

This section describes how to read the DHCP option 82 information provided back to CNR by the switch. The information is reported in Hexadecimal and must be converted to decimal to be read correctly.

Figure 5. Reading Option 82 Information



```
Switch#show platform pm if-numbers
interface gid  gpn  lpn  port slot unit slun port-type lpn-idb gpn-idb
----------------------------------------------------------------------
Gi1/0/1   1    1    49   1/0  1    1    1    local     Yes     Yes
Gi1/0/2   2    2    50   1/1  1    2    2    local     Yes     Yes
Fa1/0/1   3    3    1    1/2  1    1    3    local     Yes     Yes
Fa1/0/2   4    4    2    1/3  1    2    4    local     Yes     Yes
Fa1/0/3   5    5    3    1/4  1    3    5    local     Yes     Yes
Fa1/0/4   6    6    4    1/5  1    4    6    local     Yes     Yes
Fa1/0/5   7    7    5    1/6  1    5    7    local     Yes     Yes
Fa1/0/6   8    8    6    1/7  1    6    8    local     Yes     Yes
Fa1/0/7   9    9    7    1/8  1    7    9    local     Yes     Yes
Fa1/0/8   10   10   8    1/9  1    8    10   local     Yes     Yes
Fa1/0/9   11   11   9    1/10 1    9    11   local     Yes     Yes
Fa1/0/10  12   12   10   1/11 1    10   12   local     Yes     Yes
Fa1/0/11  13   13   11   1/12 1    11   13   local     Yes     Yes
Fa1/0/12  14   14   12   1/13 1    12   14   local     Yes     Yes
Fa1/0/13  15   15   13   1/14 1    13   15   local     Yes     Yes
Fa1/0/14  16   16   14   1/15 1    14   16   local     Yes     Yes
Fa1/0/15  17   17   15   1/16 1    15   17   local     Yes     Yes
Fa1/0/16  18   18   16   1/17 1    16   18   local     Yes     Yes
Fa1/0/17  19   19   17   1/18 1    17   19   local     Yes     Yes
Fa1/0/18  20   20   18   1/19 1    18   20   local     Yes     Yes
```

The port-id that is reported to CNR is actually the “slun” number. This number can be found using the *show platform pm if-numbers* command on the switch. These numbers do not always correlate to the physically labeled port numbers, as shown above.

If GbE interfaces are present on the switch, then these ports are listed first followed by the Fast Ethernet interfaces.

Remember the numbers are reported in Hexadecimal and must be converted to decimal.

Adding DHCP Options

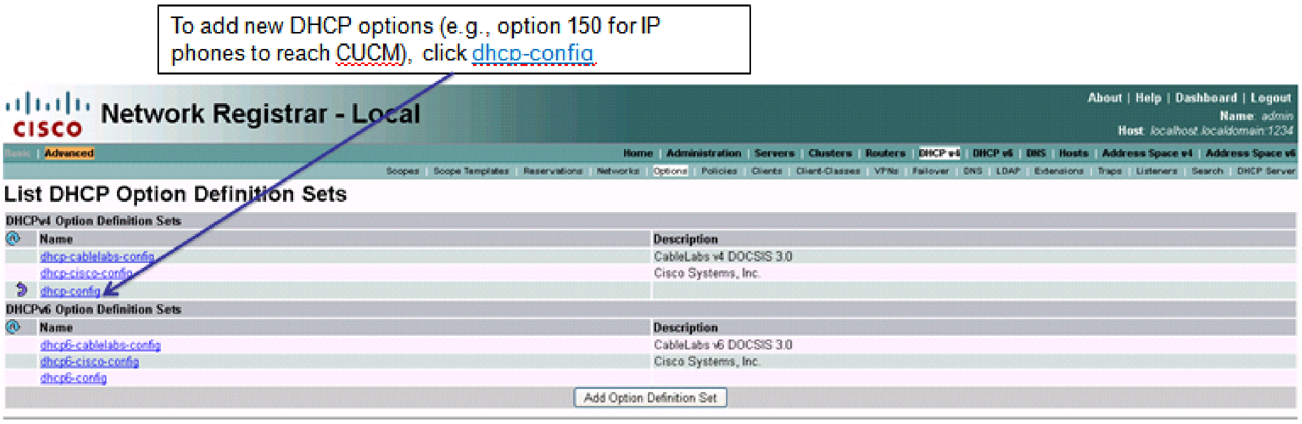
Cisco IP phones request DHCP option 150 or 66 for reaching the Cisco Unified Call Manager (CUCM) server.

Notes:

- DHCP option 150 is used when specifying the CUCM as an IP address. Option 66, if used, should be set to FQDN.
- The Option Definition Sets are all part of the Default profile that is used by all Scopes. If there are devices that use the same DHCP option but with differing values, then a new Option Definition Set must be created to include the new option and the scope used for that specific device set should use the newly-created profile containing the new Option Definition Set.

To add these options in CNR:

1. Click **Advanced** on the left side of the menu while in the DHCP menus.
2. Click **Options**.
3. Click **dhcp-config** to add the new option.



To add new DHCP options (e.g., option 150 for IP phones to reach CUCM), click dhcp-config

List DHCP Option Definition Sets

DHCPv4 Option Definition Sets

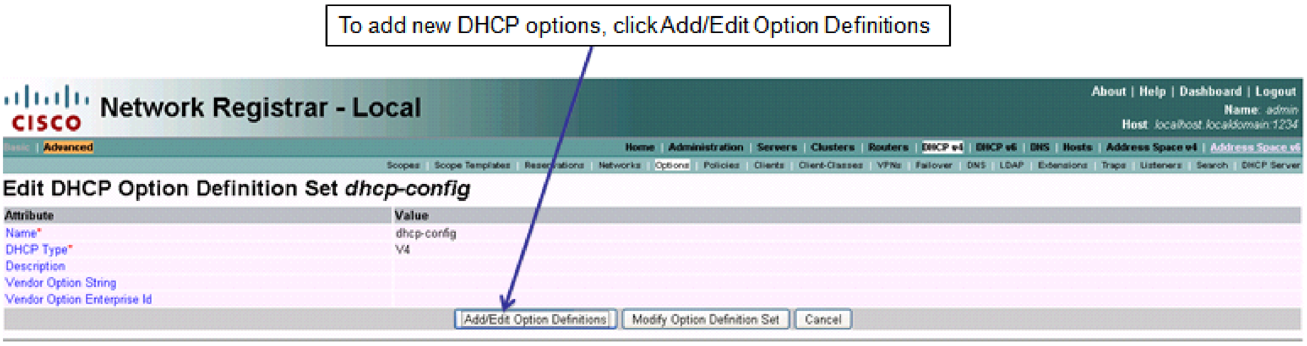
Name	Description
dhcp-cablelabs-config	CableLabs v4 DOCSIS 3.0
dhcp-cisco-config	Cisco Systems, Inc.
dhcp-config	

DHCPv6 Option Definition Sets

Name	Description
dhcp6-cablelabs-config	CableLabs v6 DOCSIS 3.0
dhcp6-cisco-config	Cisco Systems, Inc.
dhcp6-config	

Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | DNS | Hosts | Address Space v4 | Address Space v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | Extensions | Traps | Listeners | Search | DHCP Server
Add Option Definition Set

4. Click **Add/Edit Option Definitions**.



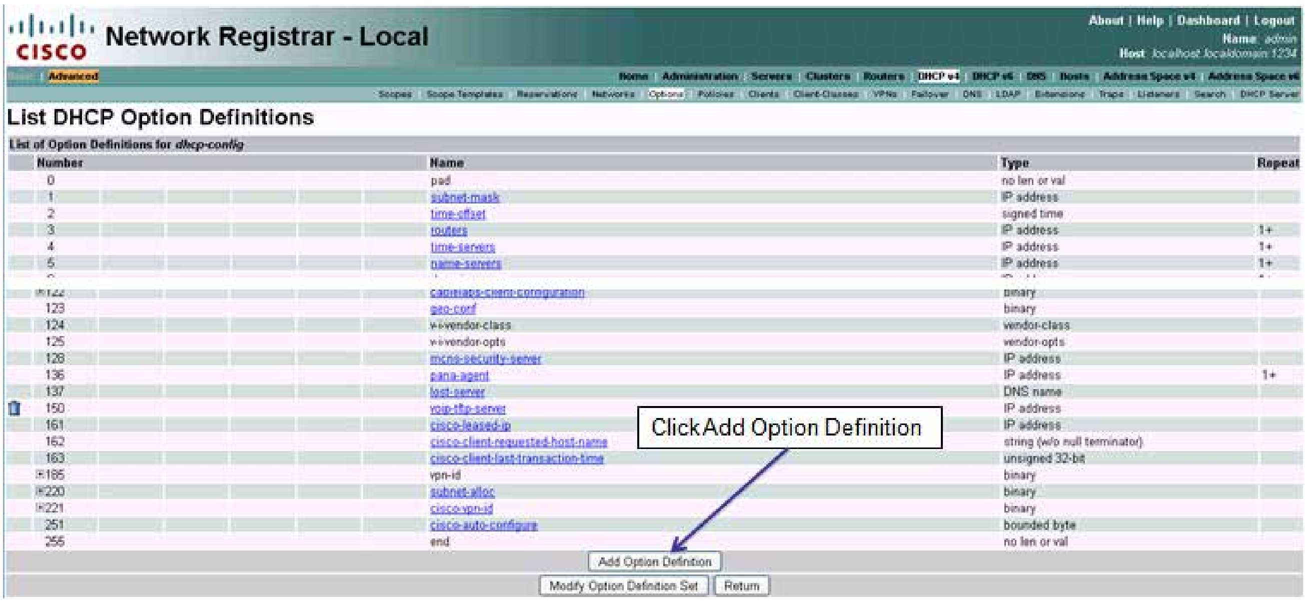
To add new DHCP options, click Add/Edit Option Definitions

Edit DHCP Option Definition Set *dhcp-config*

Attribute	Value
Name*	dhcp-config
DHCP Type*	V4
Description	
Vendor Option String	
Vendor Option Enterprise Id	

Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | DNS | Hosts | Address Space v4 | Address Space v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | Extensions | Traps | Listeners | Search | DHCP Server
Add/Edit Option Definitions
Modify Option Definition Set
Cancel

5. Click **Add Option Definition**.


Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | DNS | Hosts | Address Space v4 | Address Space v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | Extensions | Traps | Listeners | Search | DHCP Server

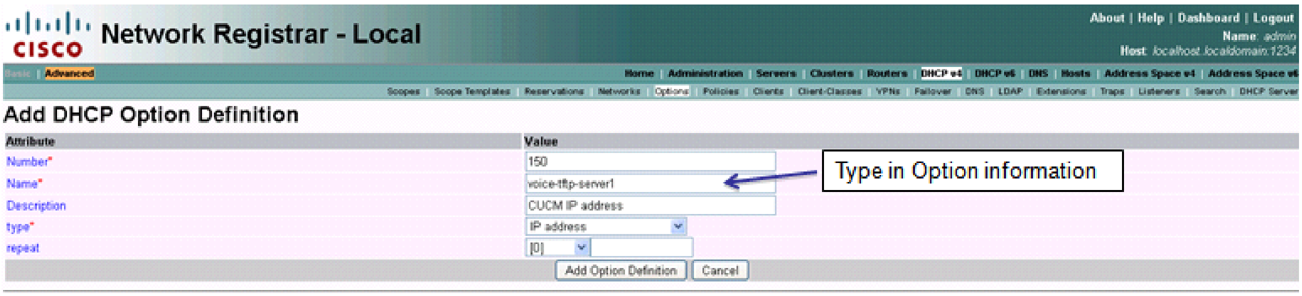
List DHCP Option Definitions

List of Option Definitions for *dhcp-config*

Number	Name	Type	Repeat
0	pad	no len or val	
1	subnet-mask	IP address	
2	time-offset	signed time	
3	routers	IP address	1+
4	time-servers	IP address	1+
5	name-servers	IP address	1+
⊞122	cablelabs-client-configuration	binary	
123	geo-conf	binary	
124	v-i-vendor-class	vendor-class	
125	v-i-vendor-opts	vendor-opts	
128	mcns-security-server	IP address	
136	pana-agent	IP address	1+
137	lost-server	DNS name	
150	voip-tftp-server	IP address	
161	cisco-leased-ip	IP address	
162	cisco-client-requested-host-name	string (w/o null terminator)	
163	cisco-client-last-transaction-time	unsigned 32-bit	
⊞185	vpn-id	binary	
⊞220	subnet-alloc	binary	
⊞221	cisco-vpn-id	binary	
251	cisco-auto-configure	bounded byte	
255	end	no len or val	

Click Add Option Definition

6. Specify the Option number, name and type and click **Add Option Definition**.


Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | DNS | Hosts | Address Space v4 | Address Space v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | Extensions | Traps | Listeners | Search | DHCP Server

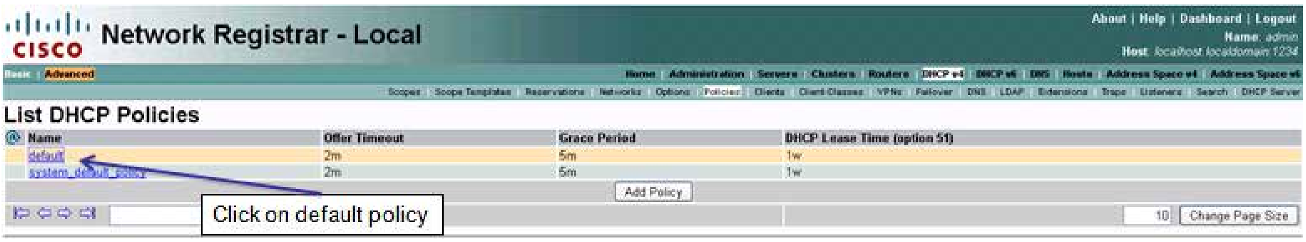
Add DHCP Option Definition

Attribute	Value
Number*	150
Name*	voice-tftp-server1
Description	CUCM IP address
type*	IP address
repeat	[0]

Add Option Definition
Cancel

Type in Option information

7. In the Policy list, click on the default policy.


Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | DNS | Hosts | Address Space v4 | Address Space v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | Extensions | Traps | Listeners | Search | DHCP Server

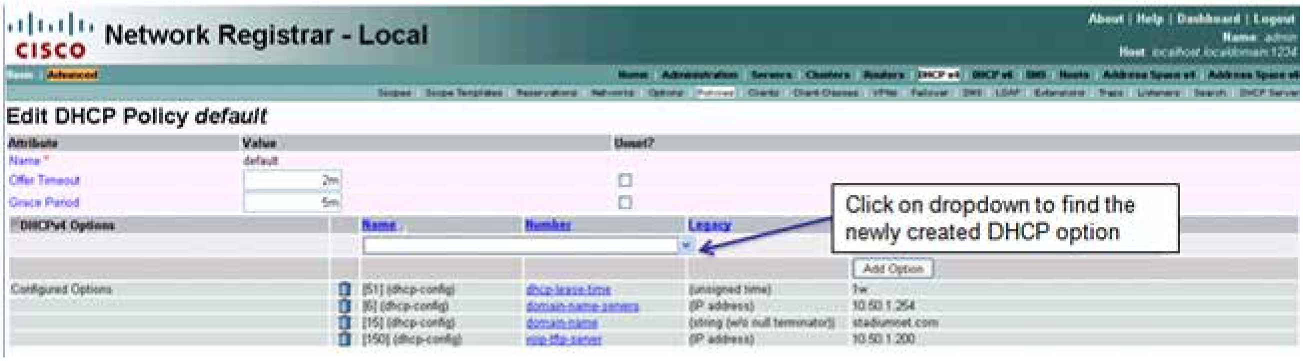
List DHCP Policies

Name	Offer Timeout	Grace Period	DHCP Lease Time (option 51)
default	2m	5m	1w
system_default_policy	2m	5m	1w

Add Policy
10
Change Page Size

Click on default policy

8. Under DHCPv4 Options, click on the drop-down list to locate the newly-created DHCP option.


Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | DNS | Hosts | Address Space v4 | Address Space v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | Extensions | Traps | Listeners | Search | DHCP Server

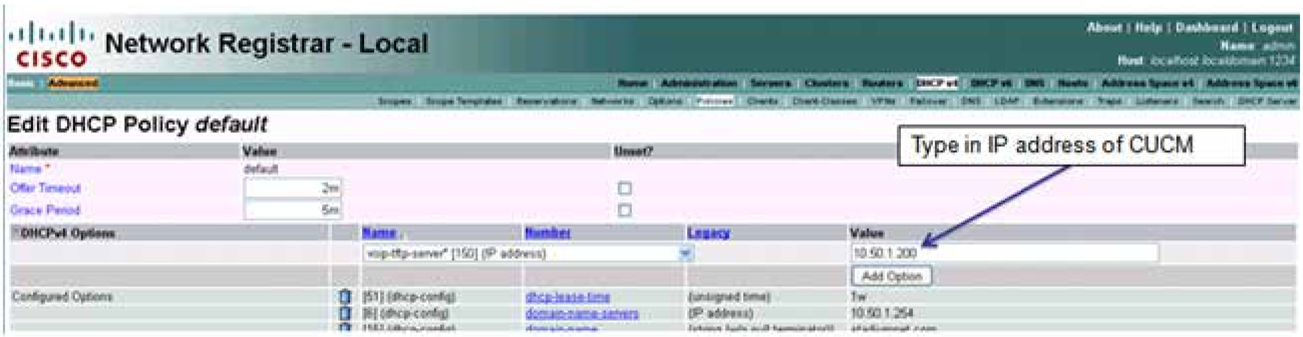
Edit DHCP Policy *default*

Attribute	Value	Unset?
Name *	default	
Offer Timeout	2m	□
Grace Period	5m	□

DHCPv4 Options	Name	Number	Legacy	
Configured Options	[51] (dhcp-config)	dhcp-lease-time	(unsigned time)	1w
	[6] (dhcp-config)	domain-name-servers	(IP address)	10.50.1.254
	[15] (dhcp-config)	domain-name	(string (w/o null terminator))	stadiumnet.com
	[150] (dhcp-config)	voip-tftp-server	(IP address)	10.50.1.200

Click on dropdown to find the newly created DHCP option

9. In the Value field, specify the IP address of CUCM.



Name admin
Host localhost localdomain 1234

Edit DHCP Policy *default*

Attribute	Value	Unset?
Name *	default	
Offer Timeout	2m	□
Grace Period	5m	□

DHCPv4 Options		Name	Number	Legacy	Value
		voip-tftp-server* [150] (IP address)			10.50.1.200
Configured Options		[51] (dhcp-config)	dhcp-lease-time	(unsigned time)	1w
		[6] (dhcp-config)	domain-name-servers	(IP address)	10.50.1.254
		[15] (dhcp-config)	domain-name	(string (w/o null terminator))	[illegible].com

Repeat these steps to add other options in the Default Profile that are applicable to all Scopes.

Other DHCP Options to add include:

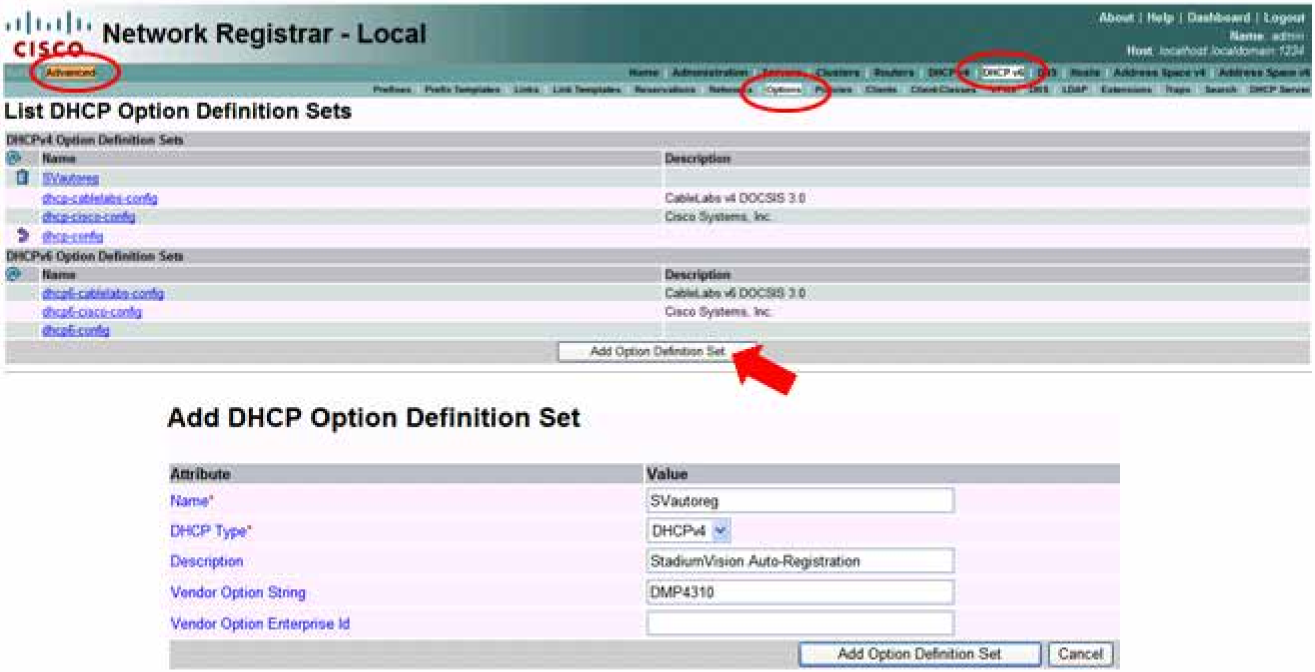
Option	Value
DHCP-lease-time	1W
Domain-name-servers	CNR IP address or reachable customer DNS server IP address
Domain-name	Customer's Domain Name

Configuring CNR for Option 43

1. Enter configuration mode at the Cisco IOS CLI.
2. Configure ip help-address on the Video VLAN to point the CNR DHCP server where this configuration will be done. If the DHCP server is configured on the same VLAN where the DMPs are connected then this step is not required.

```
interface Vlan200
    ip address 10.50.1.1 255.255.255.0
    ip helper-address 10.129.130.1 ß(CNR Server)
    ip pim sparse-mode
```

3. In the Advanced Mode, Go to DHCPv4>Options then hit the Add Option Definition Set button


Network Registrar - Local
About | Help | Dashboard | Logout
Advanced
Options
DHCP v6
Add Option Definition Set
Add Option Definition Set
Cancel

List DHCP Option Definition Sets

DHCPv4 Option Definition Sets

Name	Description
SVautoreg	
dhcp-cablelabs-config	CableLabs v4 DOCSIS 3.0
dhcp-cisco-config	Cisco Systems, Inc.
dhcp-config	

DHCPv6 Option Definition Sets

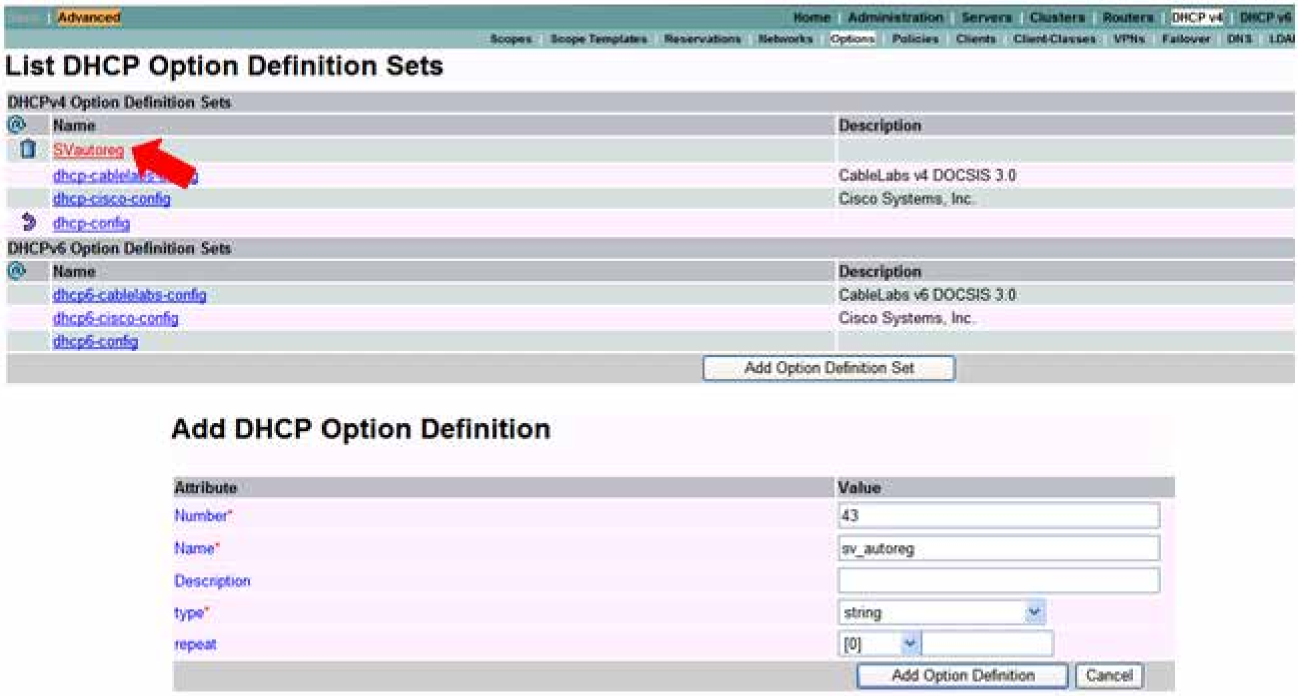
Name	Description
dhcp6-cablelabs-config	CableLabs v6 DOCSIS 3.0
dhcp6-cisco-config	Cisco Systems, Inc.
dhcp6-config	

Add DHCP Option Definition Set

Attribute	Value
Name*	SVautoreg
DHCP Type*	DHCPv4
Description	StadiumVision Auto-Registration
Vendor Option String	DMP4310
Vendor Option Enterprise Id	

Create an Option definition by giving it a Name (e.g., SVautoreg) and choose DHCP Type DHCPv4. The Description is optional but you will have to specify a Vendor Option String. Use “DMP4310” as the string. This string is what is sent to the DHCP server when the DMP sends its DHCP Discover message requesting network setting information (e.g., IP Address, Gateway, etc.)

4. Click the DHCP Option Definition Set you created and then Add DHCP Option. Set the number to 43 and give it a name (e.g., sv_autoreg). Define this option to use a string as its value.


Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP
Add Option Definition Set
Add Option Definition
Cancel

List DHCP Option Definition Sets

DHCPv4 Option Definition Sets

Name	Description
SVautoreg	
dhcp-cablelabs-config	CableLabs v4 DOCSIS 3.0
dhcp-cisco-config	Cisco Systems, Inc.
dhcp-config	

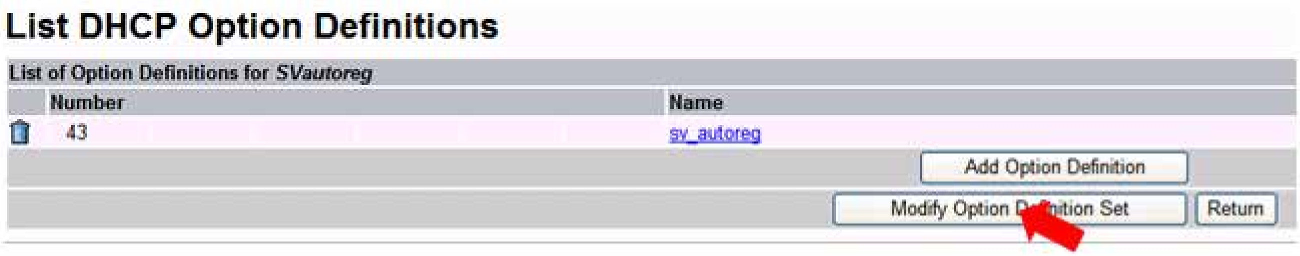
DHCPv6 Option Definition Sets

Name	Description
dhcp6-cablelabs-config	CableLabs v6 DOCSIS 3.0
dhcp6-cisco-config	Cisco Systems, Inc.
dhcp6-config	

Add DHCP Option Definition

Attribute	Value
Number*	43
Name*	sv_autoreg
Description	
type*	string
repeat	[0]

5. Be sure to click, Modify Option Definition Set to save the option 43 settings.

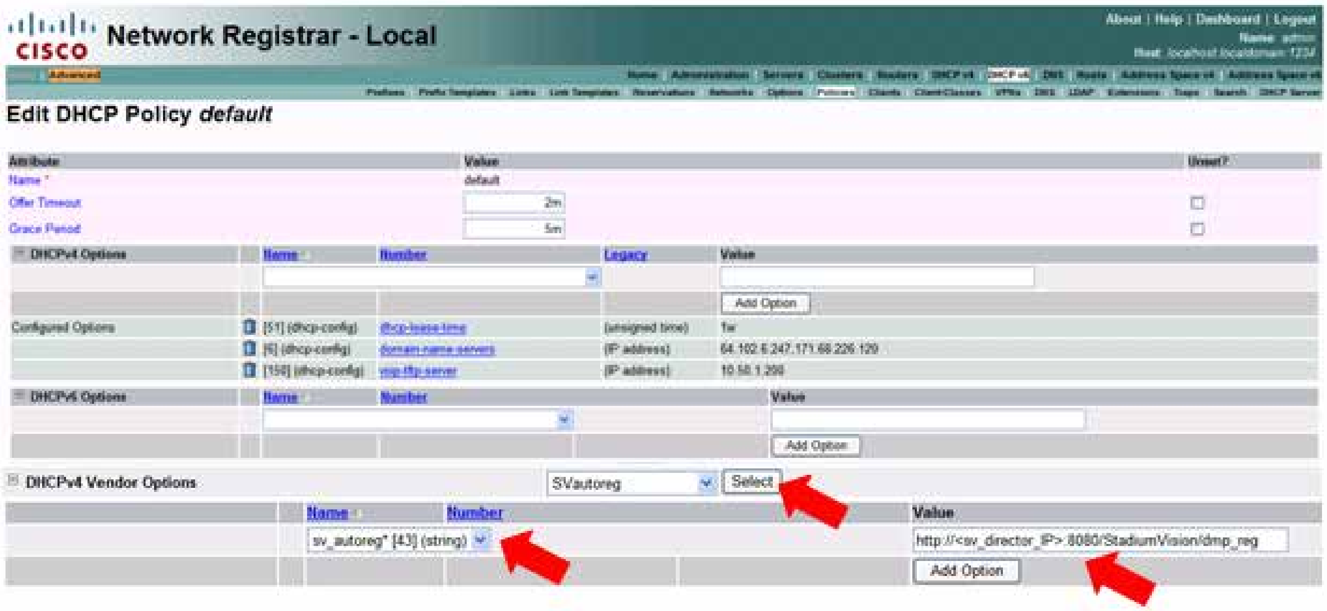


List DHCP Option Definitions

List of Option Definitions for *SVautoreg*

Number	Name
43	sv_autoreg

6. Now, add this option to the default policy by going to DHCPv4>Policies and click default. Go to the DHCPv4 Options drop-down menu and choose the Option (e.g., SVautoreg). Select the option 43, (e.g., sv_autoreg) to set the string. This string should be the following: http://<sv_director_IP>:8080/StadiumVision/dmp_reg



Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Advanced

Edit DHCP Policy *default*

Attribute	Value	Unset?
Name *	default	
Offer Timeout	2m	□
Grace Period	5m	□

DHCPv4 Options

	Name	Number	Legacy	Value
Configured Options	[51] (dhcp-config)	dhcp-lease-time	(unsigned time)	1w
	[6] (dhcp-config)	domain-name-servers	(IP address)	64.102.6.247,171.68.226.120
	[150] (dhcp-config)	voip-tftp-server	(IP address)	10.50.1.200

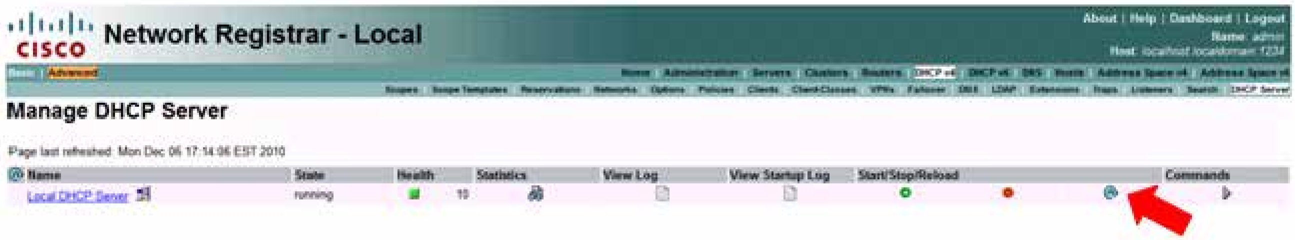
DHCPv6 Options

DHCPv4 Vendor Options: SVautoreg

Name	Number	Value
sv_autoreg* [43] (string)		http://<sv_director_IP>:8080/StadiumVision/dmp_reg

Make sure to hit the Modify Policy button at the bottom of the page for the configuration to be saved.

7. Once this configuration is completed and saved. The DHCP Server must be restarted. Click on DHCP Server and click the restart icon.



Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: localhost.localdomain:1234
Basic | Advanced

Manage DHCP Server

Page last refreshed: Mon Dec 06 17:14:06 EST 2010

Name	State	Health		Statistics	View Log	View Startup Log	Start/Stop/Reload			Commands
Local DHCP Server	running	●	10				●	●	●	▷

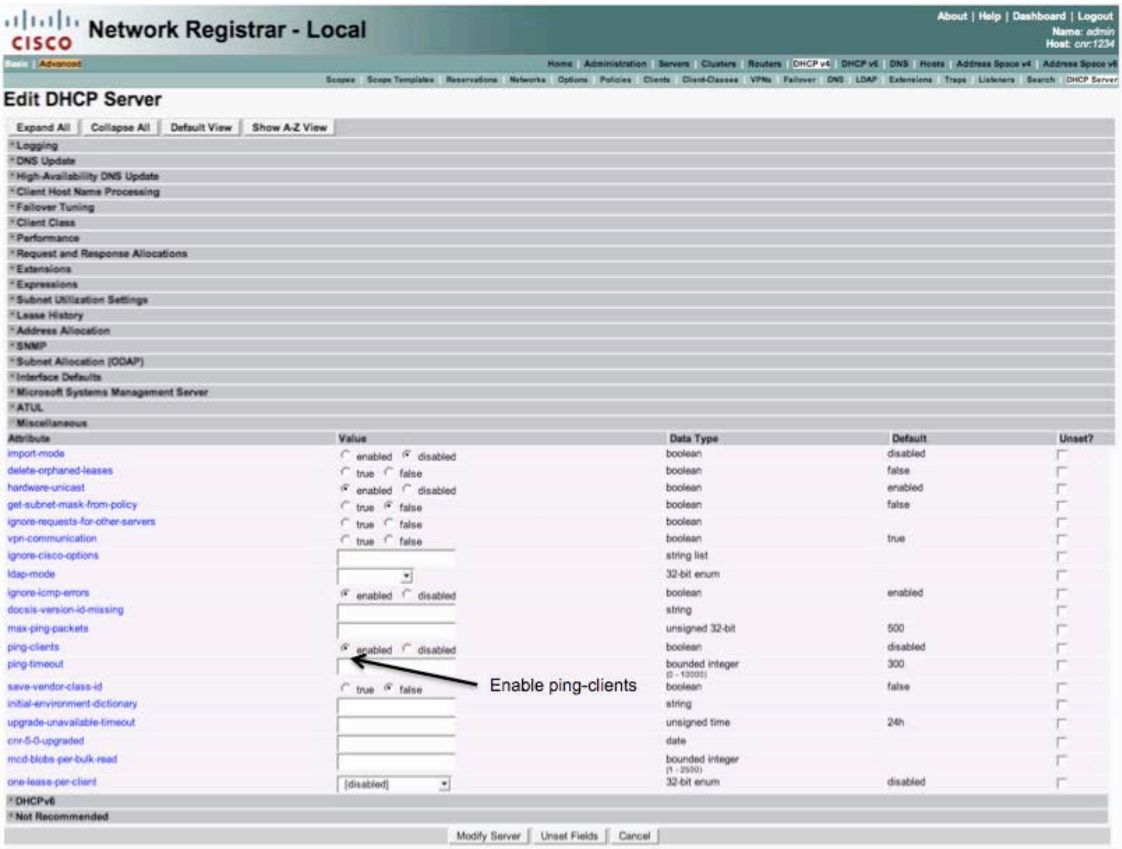
Setting CNR to Ping an IP Address Before Assigning

To avoid duplicate address assignment, CNR can be configured to ping an IP address before assigning it to the client. This is important in a Cisco StadiumVision deployment because the prepping script for the DMPs disable DHCP.

If a client responds to the ping, the DHCP server marks that address as unavailable and offers a different address. This test works only for powered-up clients; it is possible for clients to have a lease and be powered down.

Figure 6 illustrates how this feature is configured.

Figure 6. Enabling Ping



Network Registrar - Local
About | Help | Dashboard | Logout
Name: admin
Host: cnr:1234
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | DNS | Hosts | Address Space v4 | Address Space v6
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | Extensions | Traps | Listeners | Search | DHCP Server
Expand All
Collapse All
Default View
Show A-Z View

Edit DHCP Server

- Logging
- DNS Update
- High-Availability DNS Update
- Client Host Name Processing
- Failover Tuning
- Client Class
- Performance
- Request and Response Allocations
- Extensions
- Expressions
- Subnet Utilization Settings
- Lease History
- Address Allocation
- SNMP
- Subnet Allocation (ODAP)
- Interface Defaults
- Microsoft Systems Management Server
- ATUL
- Miscellaneous

Attribute	Value	Data Type	Default	Unset?
import-mode	○ enabled ● disabled	boolean	disabled	□
delete-orphaned-leases	○ true ○ false	boolean	false	□
hardware-unicast	● enabled ○ disabled	boolean	enabled	□
get-subnet-mask-from-policy	○ true ● false	boolean	false	□
ignore-requests-for-other-servers	○ true ○ false	boolean		□
vpn-communication	○ true ○ false	boolean	true	□
ignore-cisco-options		string list		□
ldap-mode		32-bit enum		□
ignore-icmp-errors	● enabled ○ disabled	boolean	enabled	□
docsis-version-id-missing		string		□
max-ping-packets		unsigned 32-bit	500	□
ping-clients	● enabled ○ disabled	boolean	disabled	□
ping-timeout		bounded integer (0 - 10000)	300	□
save-vendor-class-id	○ true ● false	boolean	false	□
initial-environment-dictionary		string		□
upgrade-unavailable-timeout		unsigned time	24h	□
cnr-5-0-upgraded		date		□
mcd-blobs-per-bulk-read		bounded integer (1 - 2500)		□
one-lease-per-client	[disabled]	32-bit enum	disabled	□

- DHCPv6
- Not Recommended

Enable ping-clients

Chapter 4 Creating Reports

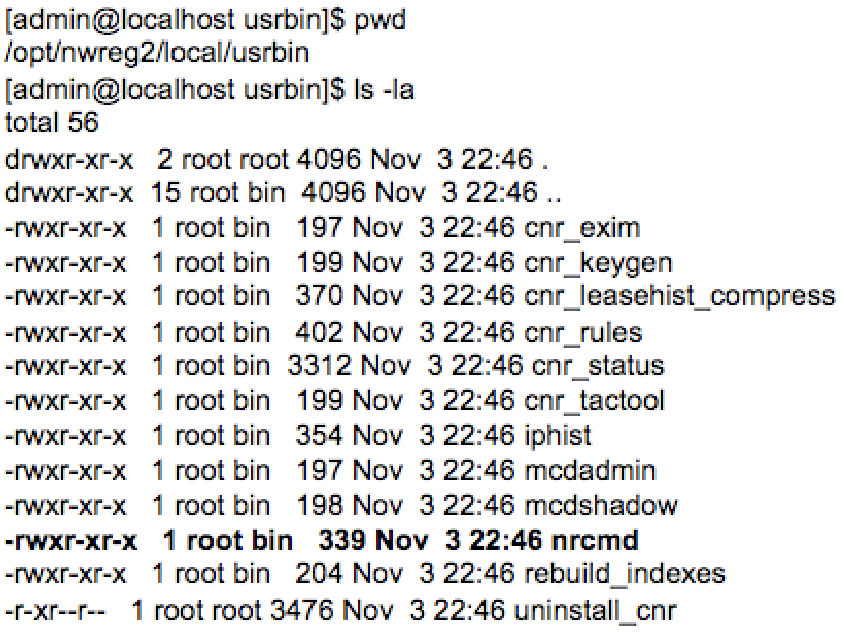
Lease reports can be retrieved two ways; via the CLI and via a sample Java client included with CNR.

For information about the sample Java client, see the CNR User’s Guide. http://www.cisco.com/en/US/docs/net_mgmt/network_registrar/7.1/user/guide/cnr71book.html

Using nrcmd

CNR has a CLI that can be invoked via the nrcmd application. Figure 6 illustrates the location of nrcmd.

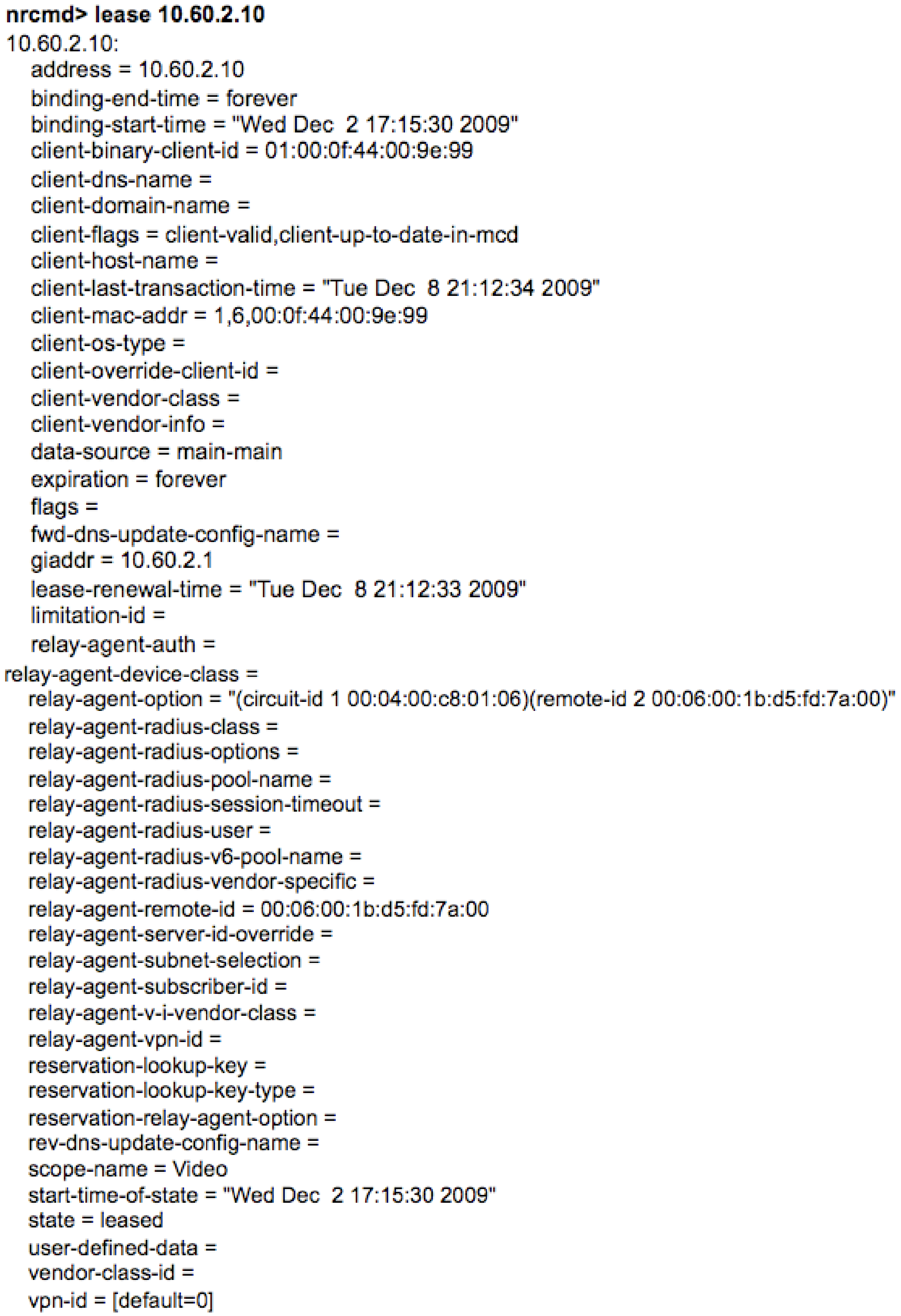
Figure 7. Using nrcmd



```
[admin@localhost usrbin]$ pwd
/opt/nwreg2/local/usrbin
[admin@localhost usrbin]$ ls -la
total 56
drwxr-xr-x   2 root root 4096 Nov  3 22:46 .
drwxr-xr-x  15 root bin  4096 Nov  3 22:46 ..
-rwxr-xr-x   1 root bin   197 Nov  3 22:46 cnr_exim
-rwxr-xr-x   1 root bin   199 Nov  3 22:46 cnr_keygen
-rwxr-xr-x   1 root bin   370 Nov  3 22:46 cnr_leasehist_compress
-rwxr-xr-x   1 root bin   402 Nov  3 22:46 cnr_rules
-rwxr-xr-x   1 root bin  3312 Nov  3 22:46 cnr_status
-rwxr-xr-x   1 root bin   199 Nov  3 22:46 cnr_tactool
-rwxr-xr-x   1 root bin   354 Nov  3 22:46 iphist
-rwxr-xr-x   1 root bin   197 Nov  3 22:46 mcdadmin
-rwxr-xr-x   1 root bin   198 Nov  3 22:46 mcdshadow
-rwxr-xr-x   1 root bin   339 Nov  3 22:46 nrcmd
-rwxr-xr-x   1 root bin   204 Nov  3 22:46 rebuild_indexes
-r-xr--r--   1 root root 3476 Nov  3 22:46 uninstall_cnr
```

Figure 8 Illustrates the information returned using the nrcmd lease command.

Figure 8. Displaying Lease Information



```
nrcmd> lease 10.60.2.10
10.60.2.10:
   address = 10.60.2.10
   binding-end-time = forever
   binding-start-time = "Wed Dec  2 17:15:30 2009"
   client-binary-client-id = 01:00:0f:44:00:9e:99
   client-dns-name =
   client-domain-name =
   client-flags = client-valid,client-up-to-date-in-mcd
   client-host-name =
   client-last-transaction-time = "Tue Dec  8 21:12:34 2009"
   client-mac-addr = 1,6,00:0f:44:00:9e:99
   client-os-type =
   client-override-client-id =
   client-vendor-class =
   client-vendor-info =
   data-source = main-main
   expiration = forever
   flags =
   fwd-dns-update-config-name =
   giaddr = 10.60.2.1
   lease-renewal-time = "Tue Dec  8 21:12:33 2009"
   limitation-id =
   relay-agent-auth =
relay-agent-device-class =
   relay-agent-option = "(circuit-id 1 00:04:00:c8:01:06)(remote-id 2 00:06:00:1b:d5:fd:7a:00)"
   relay-agent-radius-class =
   relay-agent-radius-options =
   relay-agent-radius-pool-name =
   relay-agent-radius-session-timeout =
   relay-agent-radius-user =
   relay-agent-radius-v6-pool-name =
   relay-agent-radius-vendor-specific =
   relay-agent-remote-id = 00:06:00:1b:d5:fd:7a:00
   relay-agent-server-id-override =
   relay-agent-subnet-selection =
   relay-agent-subscriber-id =
   relay-agent-v-i-vendor-class =
   relay-agent-vpn-id =
   reservation-lookup-key =
   reservation-lookup-key-type =
   reservation-relay-agent-option =
   rev-dns-update-config-name =
   scope-name = Video
   start-time-of-state = "Wed Dec  2 17:15:30 2009"
   state = leased
   user-defined-data =
   vendor-class-id =
   vpn-id = [default=0]
```