### Table of Contents

Preface .......................................................................................................................... 4  
Document Purpose ...................................................................................................... 4  
Document Audience ................................................................................................... 4  
Related Documentation .............................................................................................. 4  
Document History ....................................................................................................... 4  

Chapter 1 Overview .................................................................................................... 5  

Chapter 2 Switch Configuration .................................................................................. 6  
  Option 1 DHCP Snooping and Helper Address Configuration .................................... 6  
  Option 2 DHCP Snooping Configuration and Trusted Port ....................................... 7  

Chapter 3 DHCP Scopes .............................................................................................. 9  
  Reading DHCP Option 82 Information ...................................................................... 11  
  Adding DHCP Options ............................................................................................. 13  
  Configuring CNR for Option 43 ................................................................................. 15  
  Setting CNR to Ping an IP Address Before Assigning ............................................. 18  

Chapter 4 Creating Reports ......................................................................................... 19  
  Using nrcmd ............................................................................................................ 19
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 Documentation

- User Guide for Cisco Network Registrar, 7.1,

Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/23/10</td>
<td>First publication for Cisco StadiumVision Director Release 2.0.</td>
</tr>
</tbody>
</table>
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.
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

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.

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.
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 $ if DHCP Snooping is on
  address 10.60.2.1 255.255.255.0
  helper-address 10.50.1.254
  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

DHCP snooping is configured on following VLANs:
  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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/47</td>
<td>yes</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

Switch>show ip dhcp snooping binding

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IpAddress</th>
<th>Lease(sec)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0f:44:01:0e:95</td>
<td>172.16.102.6</td>
<td>429171</td>
<td>dhcp-snooping</td>
<td>10</td>
<td>GigabitEthernet0/33</td>
</tr>
<tr>
<td>00:0f:44:01:0e:49</td>
<td>172.16.102.4</td>
<td>427725</td>
<td>dhcp-snooping</td>
<td>10</td>
<td>GigabitEthernet0/1</td>
</tr>
<tr>
<td>00:0f:44:01:41:00</td>
<td>172.16.102.29</td>
<td>604686</td>
<td>dhcp-snooping</td>
<td>10</td>
<td>GigabitEthernet0/31</td>
</tr>
<tr>
<td>00:0f:44:01:0e:c6</td>
<td>172.16.102.10</td>
<td>493607</td>
<td>dhcp-snooping</td>
<td>10</td>
<td>GigabitEthernet0/7</td>
</tr>
<tr>
<td>00:0f:44:01:0e:97</td>
<td>172.16.102.3</td>
<td>426769</td>
<td>dhcp-snooping</td>
<td>10</td>
<td>GigabitEthernet0/35</td>
</tr>
<tr>
<td>00:0f:44:01:0e:9e</td>
<td>172.16.102.7</td>
<td>590252</td>
<td>dhcp-snooping</td>
<td>10</td>
<td>GigabitEthernet0/15</td>
</tr>
</tbody>
</table>

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.

3. To assign an IP address permanently to a device, select **DHCPv4 > Policies > default > Show A-Z View.**
4. Select Enable beside “permanent-leases.”

5. To verify the configuration, click on the IP address of interest to view the lease.
6. Scroll down to Advanced and expand that section to see the DHCP option 82 information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>gaddr</td>
<td>10.0.0.21</td>
</tr>
<tr>
<td>relay-agent-addr</td>
<td>60:04:00:26:01:10</td>
</tr>
<tr>
<td>relay-agent-device-class</td>
<td>60:04:00:26:01:10</td>
</tr>
<tr>
<td>relay-agent-option</td>
<td>circuit-id 100:04:00:03:01:10</td>
</tr>
<tr>
<td>relay-agent-device-class</td>
<td>60:04:00:26:01:10</td>
</tr>
<tr>
<td>relay-agent-relays-pool-name</td>
<td></td>
</tr>
<tr>
<td>relay-agent-relays-vendor-specifics</td>
<td></td>
</tr>
<tr>
<td>relay-agent-vendor-id</td>
<td>00:00:00:1b:65:67:a00</td>
</tr>
<tr>
<td>relay-agent-reserved-override</td>
<td></td>
</tr>
<tr>
<td>relay-agent-subnet-selection</td>
<td></td>
</tr>
<tr>
<td>relay-agent-vendor-class</td>
<td></td>
</tr>
<tr>
<td>relay-agent-nsp-id</td>
<td></td>
</tr>
<tr>
<td>vendor-update-config-name</td>
<td></td>
</tr>
<tr>
<td>dscp-name</td>
<td>Video</td>
</tr>
<tr>
<td>start-time-of-due</td>
<td>Thu Dec 3 16:22:13 2009</td>
</tr>
</tbody>
</table>

**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.
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.
4. Click Add/Edit Option Definitions.
5. Click Add Option Definition.
6. Specify the Option number, name and type and click **Add Option Definition**.

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

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

9. In the Value field, specify the IP address of CUCM.
Repeat these steps to add other options in the Default Profile that are applicable to all Scopes.

Other DHCP Options to add include:

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP-lease-time</td>
<td>1W</td>
</tr>
<tr>
<td>Domain-name-servers</td>
<td>CNR IP address or reachable customer DNS server IP address</td>
</tr>
<tr>
<td>Domain-name</td>
<td>Customer's Domain Name</td>
</tr>
</tbody>
</table>

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 (CNR Server)
   ip pim sparse-mode
   ```
3. In the Advanced Mode, Go to DHCPv4>Options then hit the Add Option Definition Set button
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.
5. Be sure to click, Modify Option Definition Set to save the option 43 settings.

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

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.
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.
Chapter 4  Creating Reports

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


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 usbin]$ pwd
/opt/nwreg2/local/usbin
[admin@localhost usbin]$ 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_leaselist_compress
  -rwxr-xr-x  1 root bin  402 Nov  3 22:46 cnr_rules
  -rwxr-xr-x  1 root bin  312 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  399 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.

```
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 00:05:00:1b: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]
```