Configuring DHCP

In the majority of deployments, a DHCP server already exists on the network, and the Clean Access Server needs to be configured in either DHCP Relay or DHCP Passthrough mode. DHCP Relay mode can be used when a CAS is a Real-IP Gateway, and DHCP Passthrough is used exclusively for a CAS in Virtual Gateway mode. For a lab/test environment, or if a DHCP server is not already set up, you can configure a Real-IP Gateway CAS to be the DHCP Server for your network. This chapter describes how to configure each of the DHCP modes of the Clean Access Server. Topics include:

- Overview, page 5-1
- Enable the DHCP Module, page 5-2
- Configuring IP Ranges (IP Address Pools), page 5-5
- Reserving IP Addresses, page 5-22
- User-Specified DHCP Options, page 5-23
- Global Action, page 5-30

Overview

DHCP (Dynamic Host Configuration Protocol) is a broadcast protocol for dynamically allocating IP addresses to computers on a network. When a client computer attempts to join a DHCP-enabled network, the client broadcasts an address request message. A DHCP server on the network responds to the request, and through the course of several exchanges, an IP address is negotiated for and delivered to the client.

In a DHCP-enabled network, the Clean Access Server can operate in one of several modes:

- **DHCP Passthrough**—This is the only mode that can be used when the CAS is configured as a Virtual Gateway. In DHCP Passthrough mode, a Virtual Gateway CAS propagates the DHCP broadcast messages across its interfaces without modification.
- **DHCP Relay**—In this mode, a Real-IP Gateway CAS forwards messages from clients to another DHCP server.
- **DHCP Server**—In this mode, a Real-IP Gateway CAS acts as the DHCP server and allocates client IP addresses for the managed (untrusted) network.

When a Real-IP Gateway CAS is enabled as a **DHCP Server**, it provides the services of a full-featured DHCP server. It can allocate addresses from a single IP pool or from multiple pools across many subnets. It can assign static IP addresses to particular client devices.

The **DHCP Server** configuration interface includes tools for auto-generating IP pools, making it easier to create many pools at once, and provides checking mechanisms to help detect configuration errors.
Auto-generating IP pools as a response to heightened virus activity can help to protect your network. By segmenting your network into many small subnets (such as /30 subnets), you can isolate clients from one another. Since clients cannot communicate directly across subnets, all traffic between them is routed through the Clean Access Server, limiting the ability of worms to propagate over peer-to-peer connections.

When you generate subnetted IP address pools, the Clean Access Server is automatically configured as the router for the subnet. An ARP entry for the subnet is automatically generated as well.

For static addresses, you can reserve a particular IP address for a particular device by MAC address.

### Table 5-1 Recommended DHCP limits

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP IP lease recommended limit of pool size</td>
<td>5000</td>
</tr>
<tr>
<td>Default/Min-Max lease time</td>
<td>0-2147483647 seconds</td>
</tr>
<tr>
<td>Recommended lease time</td>
<td>1800-7200 seconds</td>
</tr>
</tbody>
</table>

**Note** In case of pool size, a warning message is displayed if the limit exceeds.

### Enable the DHCP Module

You can enable DHCP Relay or DHCP Server mode on a Clean Access Server that is in Real-IP Gateway mode. When a CAS is a Virtual Gateway, it is always in DHCP Passthrough mode (see Figure 5-4).

### Configure DHCP Relay or DHCP Server Mode

1. From Device Management > CCA Servers > List of Servers, click the Manage button next to the Clean Access Server.
2. Click the DHCP link to open the DHCP form in the Network tab (Figure 5-1).

**Figure 5-1 Select DHCP Type (CAS in Real-IP Gateway Mode)**

3. From the DHCP Type dropdown menu, select one of the following options and click the **Select DHCP Type** button (note that this button label toggles to **Select DHCP Type and Reboot Clean Access Server** when in DHCP Server mode.) Options are as follows:
a. **None**—This is the default mode of the CAS, in which the CAS propagates DHCP broadcast messages across its interfaces without change. Leave the CAS in this default mode if a DHCP server already exists on the trusted network.

b. **DHCP Relay**—In this mode, the CAS forwards DHCP messages between clients and a specific external DHCP server. For DHCP Relay, you need to configure the DHCP server in the environment so that it hands out the Clean Access Server’s untrusted (eth1) address as the gateway IP address to managed clients. Selecting **DHCP Relay** mode displays an additional DHCP Relay configuration form (Figure 5-2). Type the IP address of the external DHCP server in the **Relay to DHCP server** field, and click the **Update** button.

c. **DHCP Server**—This sets the CAS to perform DHCP services for managed clients. Once the CAS is enabled as a **DHCP Server**, the DHCP Status, Subnet List, Reserved IPs, Auto-Generate, and Global Options subtabs are displayed (Figure 5-3). From there, you can add IP pools manually, auto-generate pools and subnets, or specify reserved IPs, as described in Configuring IP Ranges (IP Address Pools), page 5-5.
Chapter 5      Configuring DHCP

Enable the DHCP Module

Figure 5-3    DHCP Server Mode

Once **DHCP Server** is selected, to switch to a different DHCP Type for the Clean Access Server, you must reboot the CAS. To change the type, select **None** or **DHCP Relay** from the dropdown menu and click the button **Select DHCP Type and Reboot Clean Access Server**.

**DHCP Status Options**

When the CAS is enabled as a DHCP server, the **DHCP Status** tab includes the enable buttons shown in Figure 5-3.

Cisco NAC Appliance offers two DHCP enable/disable functions to ensure client IP addresses are renewed properly when the CAS is configured as the DHCP server for your network. These are User Logout on DHCP Lease Expiration and DHCP FORCERENEW, as described below.
Enable/Disable Logout on DHCP Lease Expiration

This toggle button is disabled by default. Clicking the Enable button causes the user to be logged out (either Agent or Web session logout) from the Cisco NAC Appliance when the client's DHCP lease expires.

Enable/Disable DHCP FORCERENEW

This toggle button is disabled by default. Clicking the Enable button instructs the DHCP server to execute a DHCP NAK command, which releases IP addresses assigned to a client by other DHCP servers. Following the NAK command, the DHCP client will be assigned a valid IP address as configured on the CAS.

Show/Hide DHCP Server Startup Message

When this button is clicked, the last DHCP server startup message is displayed. If the server does not start, an error message is shown here.

Show/Hide DHCP Configuration File

When this button is clicked, the DHCP configuration file is displayed. In some cases, the startup message displays an error for a particular line of the configuration. Clicking this button allows you to view the configuration file line-by-line.

For further information on the DHCP Status tab see Working with Subnets, page 5-15.
For additional information on DHCP configuration, see User-Specified DHCP Options, page 5-23.

A Virtual Gateway CAS is always in DHCP Passthrough mode (Figure 5-4).

Configuring IP Ranges (IP Address Pools)

To set up the Clean Access Server to provide DHCP services, you first configure the range of IP addresses to be allocated to clients (the IP address pool). In addition, you can specify network information to be handed to clients with the address, such as DNS addresses.

The CAS can allocate addresses from multiple pools and subnets. However, allocated addresses must fall within the ranges specified to be managed by the CAS. This can be either:

- The address space of its untrusted interface managed network (set in the Network> IP page)
- A managed subnet specified in the Managed Subnet form of the Advanced tab
If you try to create an address pool from a subnet that is not managed, an error message notifying you of the condition appears in the admin console and the pool is not created.

Auto-Generated versus Manually Created Subnets

You can automatically generate subnets in order to create many IP address pools at a time. Creating a large number of IP pools of relatively small size (from which only a few addresses can be assigned) can help protect your network. By isolating clients into small subnets, you limit the ability of peers to communicate directly with one another, and thereby prevent events such as worms from proliferating across peer connections.

Alternatively, you can manually create subnets if only a few IP address pools are required for your network.

Subnetting Rules

Whether creating IP pools automatically or manually in the admin console, the subnets you create must follow standard subnetting design rules. Only properly aligned, power-of-two subnet addresses are supported. For example, you cannot start a subnet range at address 10.1.1.57 with a subnet mask of 255.255.255.192, because the final octet of the netmask, 192, corresponds to a “size 64” subnet. There can only be four size-64 subnets, with subnet start address boundaries of .0, .64, .128, and .192. Since .57 is not a power-of-two, it cannot be used as the starting address for a subnet.

You must specify the starting address of the range for either manually-created or automatically-generated subnets. To manually create a pool you specify the end of the range, and to auto-generate a pool you specify the number of subnets to generate.

Addresses in the IP range are assigned as follows:

1. Network address—The first valid number entered for the range is used as the network address for the subnet (or the first subnet, if generating more than one subnet).
2. Router address—The second number is used as the router address (that is, the virtual gateway interface address for the subnet).
3. Host IP address—The third number is the first address that is leasable to clients.
4. Broadcast address—The final address in the range is the broadcast address.

By specifying an IP range of only four addresses, you can create a subnet for a single host.

Table 5-2 shows the number of leasable addresses for each subnet size and number of subnets possible per CIDR (Classless InterDomain Routing) prefix. Each CIDR prefix corresponds to a specific subnet mask. CIDR notation identifies the number of bits masked for the network portion of a 32-bit IP address in order to produce a specific number of host addresses. For example, a CIDR address of 10.5.50.6 /30 indicates that the first 30 bits of the address are used for the network portion, leaving the remaining 2 bits to be used for the host portion. Two bits of address yield four host addresses: three addresses are automatically allocated for the required network, gateway, and broadcast addresses for the subnet, and the remaining address can be leased. Therefore, a /30 network creates a subnet of one host.
Chapter 5 Configuring DHCP

Configuring IP Ranges (IP Address Pools)

Table 5-2  Addresses per Subnet Size

<table>
<thead>
<tr>
<th>CIDR Prefix</th>
<th>No. of possible subnets (Class C)</th>
<th>Total number of addresses</th>
<th>No. of leasable host addresses</th>
<th>Example valid start-of-range addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>/30</td>
<td>64</td>
<td>4</td>
<td>1</td>
<td>10.1.65.0 10.1.65.4 10.1.65.8 ...</td>
</tr>
<tr>
<td>/29</td>
<td>32</td>
<td>8</td>
<td>5</td>
<td>10.1.65.0 10.1.65.8 10.1.65.16 ...</td>
</tr>
<tr>
<td>/28</td>
<td>16</td>
<td>16</td>
<td>13</td>
<td>10.1.65.0 10.1.65.16 10.1.65.32 ...</td>
</tr>
<tr>
<td>/27</td>
<td>8</td>
<td>32</td>
<td>29</td>
<td>10.1.65.0 10.1.65.32 10.1.65.64 ...</td>
</tr>
<tr>
<td>/26</td>
<td>4</td>
<td>64</td>
<td>61</td>
<td>10.1.65.0 10.1.65.64 10.1.65.128 10.1.65.192</td>
</tr>
<tr>
<td>/25</td>
<td>2</td>
<td>128</td>
<td>125</td>
<td>10.1.65.0 10.1.65.128</td>
</tr>
<tr>
<td>/24</td>
<td>1</td>
<td>256</td>
<td>253</td>
<td>10.1.65.0</td>
</tr>
</tbody>
</table>

Table 5-3 shows the addressing for an automatically-generated IP range of four /30 subnets starting at address 10.1.100.12.

Table 5-3  Auto-Generated Subnets

<table>
<thead>
<tr>
<th>IP Range Entries</th>
<th>1st Subnet</th>
<th>2nd Subnet</th>
<th>3rd Subnet</th>
<th>4th Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network address</td>
<td>10.1.100.12</td>
<td>10.1.100.16</td>
<td>10.1.100.20</td>
<td>10.1.100.24</td>
</tr>
<tr>
<td>Router address</td>
<td>10.1.100.13</td>
<td>10.1.100.17</td>
<td>10.1.100.21</td>
<td>10.1.100.25</td>
</tr>
<tr>
<td>Client address range</td>
<td>10.1.100.14 - 10.1.100.14</td>
<td>10.1.100.18 - 10.1.100.18</td>
<td>10.1.100.22 - 10.1.100.22</td>
<td>10.1.100.26 - 10.1.100.26</td>
</tr>
<tr>
<td>Broadcast address</td>
<td>10.1.100.15</td>
<td>10.1.100.19</td>
<td>10.1.100.23</td>
<td>10.1.100.27</td>
</tr>
</tbody>
</table>
In general, the admin console enforces rules for properly configured subnets. If you attempt to use an invalid network address for the netmask, the message appears: “Subnet/Netmask pair do not match”. In this case, choose a new value for the address.

**Create IP Pools Manually**

To create an IP pool manually, you also need to define the subnet in which the pool resides. There are three ways to arrive at the subnet address and netmask values for a manually generated pool:

- Enter the subnet address directly, as an IP address and netmask.
- Have the admin console generate the smallest possible subnet based on the IP range you enter.
- Have the admin console calculate the values from the list of subnets currently managed by the Clean Access Server.

**To create an IP pool range:**

1. In the **DHCP** form, click the **Subnet List** tab, then the **New** link.

**Figure 5-5  New Subnet List Subtab Link**

```
<table>
<thead>
<tr>
<th>Device Management &gt; Clean Access Servers &gt; 10.201.5.120</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
</tr>
<tr>
<td>DHCP Status</td>
</tr>
<tr>
<td>List - New</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Range</th>
<th>Domain</th>
<th>VLAN ID</th>
<th>Subnet Range</th>
<th># IPs</th>
</tr>
</thead>
</table>
```

2. The new IP pool form appears.
3. Enter values for these fields:

- **IP Range** – The IP address pool to be assigned to clients. Provide a range of addresses not currently assigned in your environment.

- **Default Gateway** – The IP address of the default gateway passed to clients. This should be the untrusted interface address of the Clean Access Server.

- **Default/Max Lease Time (seconds)** – The amount of time the IP address is assigned to the client, if the client does not request a particular lease time, as well as the maximum amount of time for which a lease can be granted. If the client requests a lease for a time that is greater, the maximum lease time is used.

- **DNS Suffix** – The DNS suffix information to be passed to clients along with the address.

- **DNS Servers** – The address of one or more DNS servers in the client’s environment. Multiple addresses should be separated by commas.

- **WIN Servers** – The address of one or more WIN servers in the client’s environment. Multiple addresses should be separated by commas.

- **Restrict range to [VLAN ID] [RELAY IP]**

If choosing VLAN ID, type the VLAN ID in the text field. Clients not associated with the specified VLAN cannot receive addresses from this IP pool. A VLAN ID can be any number between 0 and 4095.
For IPs with VLAN restrictions, all IPs must be in a managed subnet, and you must create a managed subnet first before creating an IP range (DHCP pool). See Configuring Managed Subnets or Static Routes, page 4-25 for details.

If choosing RELAY IP, type the Relay IP in the text field. Clients not associated with the specified Relay IP cannot receive addresses from this IP pool.

For IPs with relay restrictions, all IPs should typically be in static routes, but can be in managed subnets if integrating the CAS with Aironet devices or other non-RFC 2131/2132 compliant devices. Note that these IP address pools must be in either a static route or a managed subnet, and IPs with relay restrictions should only be put in a managed subnet for these non-compliant devices. See Configuring Managed Subnets or Static Routes, page 4-25 for details.

4. From the Subnet/Netmask list, choose how you want the subnet address to be specified, from the following choices:

- **Calculate from existing managed subnets** – The admin console determines what to use for the subnet and netmask values based on the configuration in the Managed Subnet form (in the Advanced tab). It calculates the network address by applying the netmask to the gateway address for each managed subnet.

- **Calculate smallest subnet for IP range entered** – The admin console determines the subnet and netmask values based on the IP address range you entered.

- **Manually enter subnet and netmask** – To specify the desired network address and netmask manually. If selected, the Subnet and NetMask fields appear at the bottom of the form.

- **Inherit Scoped Global Options** – This field is only visible if DHCP options are enabled, and will be checked by default. If this field is disabled (unchecked), the scoped global options configured in the Global Options tab are not inherited. See User-Specified DHCP Options, page 5-23 for details.

5. Click Update when finished. If there are errors in the configuration, warning messages appear. Follow the instructions to correct the settings.

### Auto-Generating IP Pools and Subnets

By automatically generating subnets, you can quickly divide your network into small segments. Segmenting your network into small subnets can be an effective security measure in response to a worm attack, since a network comprised of many small subnets (with one host per subnet possible) limits the ability of clients to engage in peer-to-peer interaction.

**Caution**
The recommended maximum number of subnets per Clean Access Server is 1000. If the CAS machine has sufficient memory (>1G), up to 2500 subnets can be configured. Do not exceed the recommended limit if this will place an excessive burden on system resources, particularly server memory.
Add Managed Subnet

1. First, make sure that the IP pools you want to add are in the range of a managed subnet. If needed, add the managed subnet under Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet (for details, see Configure Managed Subnets for L2 Deployments, page 4-27).

Figure 5-7   Add Managed Subnet

![Add Managed Subnet](image)

**Note**

When adding a managed subnet, the IP Address field you configure should be the gateway address for the subnet—that is the address used by the CAS to route the subnet. The IP Address of the managed subnet should not be the network address (which the Clean Access Manager will calculate by applying the Subnet Mask to the gateway address).

Create Auto-Generated Subnet

1. Go to Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Auto-Generate. The Auto-Generate pane appears as follows:
2. In the **Start Generating at IP** field, type the first IP address of the range to be generated:

   - The first available valid address for the managed subnet range is used as the network address for the first subnet, the next number is used as the router address, and the next number after that becomes the first address that is leasable to clients.

3. In the **Number of Subnets to Generate** field, type the number of subnets to generate. As mentioned, the maximum recommended size is 1000. Exceeding this number can impose a burden on the server’s system resources.
4. From the **Generate Subnets of Size** dropdown list, select the size of each subnet. Subnet sizes are presented in CIDR format (such as /30). The dropdown menu also lists the corresponding number of available host addresses per subnet for each CIDR prefix. For each range, three addresses are automatically reserved and cannot be allocated to clients:

- The network address of the subnet
- The router address (for the Clean Access Server)
- The broadcast address

Therefore, a /30 size subnet has four addresses, but only one IP available for hosts.

5. Provide values for the remaining fields:

- **Default Lease Time (seconds)** – The amount of time the IP address is assigned to the client, if the client does not request a particular lease time.
- **Max Lease Time (seconds)** – The maximum amount of time a lease can be reserved. If the client requests a lease for a time that is greater, this max lease time is used.
- **DNS Suffix** – The DNS suffix information to be passed to clients along with the address lease.
- **DNS Server(s)** – The address of one or more DNS servers in the client’s environment. Multiple addresses should be separated by commas.
- **WIN Server(s)** – The address of one or more WIN servers in the client’s environment. Multiple addresses should be separated by commas.
- **Restrict this Subnet to a specific VLAN ID** – Clients not associated with the specified VLAN cannot receive addresses from this IP pool. A VLAN ID can be any number between 0 and 4095.
- **Inherit Scoped Global Options** – This field is only visible if DHCP options are enabled and is turned on by default. If this field is disabled, the scoped global options configured in the **Global Options** tab are not inherited. See **User-Specified DHCP Options, page 5-23** for details.

6. When finished, generate a preliminary list of subnets by clicking **Generate Subnet List**. If there are errors in the values provided, error messages appear at this time. If the subnet based on your address is not properly aligned, the interface suggests the closest legal starting IP address for your range.

If successful, a preliminary list of IP ranges appears, allowing you to review the results.

**Figure 5-9 Commit Subnet List**

7. Click **Commit Subnet List** to save the IP ranges.

8. The auto-generated subnets appear as a single subnet range under **Subnet List > List**. The “# of Subnets” and “# of IPs” columns allow you to view how large the auto-generated range is in terms how many subnets have been created as well as the number of IP addresses for the range.
9. The newly-generated list also appears in summary form under **DHCP Status** tab (listing VLAN ID and number of dynamic, available, and static IP addresses).

**Figure 5-11 DHCP Status**

**Figure 5-12 ARP Entries Generated for DHCP**

**Note**

ARP entries are automatically created in the Clean Access Server configuration for the generated subnets (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > ARP**), as shown in Figure 5-12. Deleting generated subnets also removes the corresponding ARP entries.
Working with Subnets

View Users by MAC Address/VLAN

1. After committing an auto-generated list, the Network > DHCP > DHCP Status page appears and lists the newly-generated subnet. If the auto-generated subnet is restricted to a VLAN ID, the subnet is listed by that VLAN ID; otherwise, the VLAN column is blank if no VLAN is specified.

![Figure 5-13 DHCP Status — VLANs](image)

2. By clicking the View MACs icon for the VLAN, you can see the MAC address, IP and type of client, as shown in Figure 5-14.

![Figure 5-14 View MAC Address](image)

- For DHCP clients, the Type column lists “Dynamic” and the lease assignment and expiration times are shown.
- For reserved IP clients, the Type column lists “Static” and the lease time columns display N/A.

View or Delete Subnets from the Subnet List

1. You can view the list of subnets created or modify individual subnets from Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Subnet List > List.
2. To view the subnets for a particular VLAN only, select the VLAN from the scroll menu next to the View button and click View.

3. To remove an individual subnet, click the Delete icon next to it.

4. To remove all auto-generated subnets, click the Delete all Generated Subnets button. This action deletes only auto-generated subnets; all manually entered subnets are retained.

**Edit a Subnet**

1. To edit a subnet, click the Edit button next to it in the Subnet List to bring up the Edit Subnet List form. Figure 5-16 shows the Edit form for an auto-generated subnet. (The Edit form for a manually-generated subnet is similar to Figure 5-6 on page 5-9.)
2. You can modify the lease time, DNS/WIN server information and VLAN ID restriction. Click **Update** to save the changes. To change the IP range, default gateway or subnet mask, the subnet must be deleted from **Subnet List > List** form and re-added with the modified parameters.

3. For auto-generated subnets, you can disable a particular subnet by clicking the **Disabled** checkbox next to it. This allows you to disable the IPs associated with a particular generated subnet so that the IPs are not leased out. This can be particular useful if you have one or two servers in the middle of a subnet range.
Typically, when a Clean Access Server is configured as a DHCP server it is in Layer 2 mode. The CAS acts as a DHCP server for the Layer 2 VLANs which are trunked to it. In Layer 2 mode, you configure a DHCP scope for that VLAN on the CAS and then configure a managed subnet for that VLAN so that the CAS can communicate to clients in that VLAN.

However, Layer 3 clients are one or multiple hops away from the CAS and therefore work differently. L3 clients are not adjacent to the CAS and DHCP discover broadcast from these clients will never reach the CAS (DHCP server). Therefore, a DHCP scope for these clients cannot be created based on VLAN. Figure 5-17 illustrates an example scenario.

In this example:
- CAM is on VLAN 900
- CAS trusted interface is on VLAN 10 and untrusted interface is on VLAN 100.
- Client machines in VLAN 700 are multiple hops away from the CAS
- CAS is required to act as a DHCP server for these clients

As previously mentioned, DHCP discover broadcast from these L3 clients are not able to cross the VLAN 700 boundary. Therefore, an “IP helper address” needs to be configured under the router interface acting as the gateway for VLAN 700, for example:

```
Interface vlan 700
Ip address 10.60.60.1 255.255.255.0
Ip helper-address x.x.x.x
```

Where x.x.x.x is the untrusted side (eth1) IP address of the CAS (e.g. 10.20.20.1).

On the CAS, the following needs to be configured:
- A DHCP scope for clients in VLAN 700 with an “IP RELAY” of 10.60.60.1
- A route for 10.60.60.0/24 (VLAN 700) pointing towards the untrusted side
Figure 5-18 shows the IP information of the CAS configured as a Real-IP Gateway:

- Trusted (eth0) interface IP address is 10.2.2.1
- Trusted Default Gateway is 10.2.2.2
- Untrusted (eth1) interface IP address is 10.20.20.1
- Untrusted Default Gateway is 10.20.20.3

**Figure 5-18 CAS IP Configuration**

The CAS has already been enabled as a **DHCP Server** (as described in **Enable the DHCP Module**, page 5-2). Figure 5-19 shows the New Subnet list form configured under **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Subnet List > New** with:

- A client IP range of 10.60.60.100-10.60.60.200
- Default gateway of 10.60.60.1
- **Restrict range to RELAY IP** is chosen with 10.60.60.1 entered as the IP relay.
- Subnet of 10.60.60.0 and subnet mask of 255.255.255.0 manually entered
- Click **Update** to create the new DHCP scope.
Figure 5-19  Restrict Subnet List to Relay IP

<table>
<thead>
<tr>
<th>Status</th>
<th>Network</th>
<th>Filter</th>
<th>Advanced</th>
<th>Authentication</th>
<th>Misc</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DHCP</td>
<td>DNS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DHCP Status</th>
<th>Subnet List</th>
<th>Reserved IPs</th>
<th>Auto-Generate</th>
<th>Global Options</th>
<th>Global Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List</td>
<td>- New</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- IP Range: 192.168.10.100 - 192.168.10.200
- Default Gateway: 192.168.10.1
- Default/Max Lease Time (seconds): 7200 / 7200
- DNS Suffix: 
- DNS Servers: 172.16.16.183
- WINS Servers: 
- Restrict range to RELAY\IP
- Subnet/Netmask: Manually enter subnet and netmask
- Subnet: 10.201.201.0
- Netmask: 255.255.255.0

Figure 5-20 shows the Static Routes form configured under Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Static Routes with:

- Destination Subnet Address of **10.60.60.0** and Subnet Mask of 255.255.255.0 (the subnet/netmask configured in Figure 5-19).
- **Untrusted[eth1]** chosen as the Link.
- Gateway of **10.20.20.3**, which is the CAS eth1 default gateway shown in Figure 5-18
- Click Add Route to add this static route to the CAS.
### Create Static Route

<table>
<thead>
<tr>
<th>Status</th>
<th>Network</th>
<th>Filter</th>
<th>Advanced</th>
<th>Authentication</th>
<th>Misc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Subnet</td>
<td>VLAN Mapping</td>
<td>NAT</td>
<td>1:1 NAT</td>
<td>Static Routes</td>
<td>ARP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dest. Subnet Address/Mask</th>
<th>Gateway (optional)</th>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.69.0 / 255.255.255.0</td>
<td>10.20.20.3</td>
<td>Untrusted</td>
<td>[x]</td>
</tr>
</tbody>
</table>

Figure 5-20: Create Static Route
Reserving IP Addresses

By reserving an IP address, you can keep a permanent association between a particular IP address and device. A reserved device is identified by MAC address. Therefore, before starting, you need to know the MAC address of the device for which you want to reserve an IP address. The configuration for a reserved IP does not include a maximum or default lease time. The address is always available for the device and in effect has an unlimited lease time. Table 5-4 lists several rules that apply to reserved IP addresses.

Table 5-4 Reserved IP Address Rules

<table>
<thead>
<tr>
<th>A reserved address cannot be...</th>
<th>A reserved address must be...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Within the address range of an IP pool.</td>
<td>• Within the address range of the Clean Access Server’s managed network (as configured in Device Management &gt; CCA Servers &gt; Manage [CAS_IP] &gt; Network &gt; IP), or</td>
</tr>
<tr>
<td>• A network or broadcast address.</td>
<td>• Within the address range of the CAS’s managed subnets (as configured in Device Management &gt; CCA Servers &gt; Manage [CAS_IP] &gt; Advanced &gt; Managed Subnet).</td>
</tr>
<tr>
<td>• Currently set as a default gateway for an existing IP address range.</td>
<td></td>
</tr>
</tbody>
</table>

Add a Reserved IP Address


Figure 5-21 Reserved IPs—New
Chapter 5 Configuring DHCP

User-Specified DHCP Options

2. In the MAC Address field, type the MAC address for the device for which you want to reserve an IP address, in hexadecimal MAC address format (e.g., 00:16:21:11:4D:67).

3. In the IP Address to allocate field, type the IP address that you want to reserve.

4. Enter an optional Description.

5. Provide values for the remaining fields:
   - DNS Suffix – The DNS suffix information to be passed to clients along with the address lease.
   - DNS Servers – The address of one or more DNS servers in the client’s network. Multiple addresses should be separated by commas.
   - WIN Servers – The address of one or more WIN servers in the client’s network. Multiple addresses should be separated by commas.
   - Restrict this IP to VLAN ID – If the client is associated with a particular VLAN, click this checkbox to specify the VLAN identifier in the VLAN ID field.

6. When finished, click Update.

The reserved IP now appears in under Subnet List > List. From there, it can be modified by clicking the Edit button or removed by clicking Delete.

User-Specified DHCP Options

The Global Options tab (Figure 5-22) allows advanced users to modify the DHCP configuration directly. DHCP options can be specified as follows:

- Root global options appear at the root level or top of the DHCP configuration file and apply to all DHCP subnet declarations. Root global options are inherited by everything in the file.

- Scoped global options are added to each subnet definition, but you can enable whether or not a subnet inherits the option. When DHCP options are enabled, an “Inherit Scoped Global Option” enable appears on the forms used to add or edit manually-created or automatically-generated subnets. Note that the “Inherit Scoped Global Option” checkbox appears only while customized DHCP options are enabled and only for subnets created after the options are enabled.

- Local options apply only to the subnet for which they are entered. Local DHCP options can be added to an individual subnet using the Subnet List > Edit form described in Add Local Scoped DHCP Option, page 5-28.

You can create DHCP option rules based on class restrictions to restrict access to DHCP subnets. You can create rules for:

- All clients on a specific VLAN
- Clients coming from a specific relay IP

You can create new options by selecting the options type or by creating a custom option to create an option that is not on the list, or of a different type.

Caution

The DHCP configuration file should not be modified under most circumstances.

A server directive instructs the DHCP server to behave differently, while a DHCP option refers to a specific piece of data to be returned by the DHCP server. For example, the “allow-bootp” server directive (disabled by default) instructs the DHCP server to allow older BOOTP clients to connect. See Table 5-5 “DHCP Server Directives” for additional details.
Most server directives can only be added as root global options. This is because their actions direct the behavior of the entire server and cannot be limited in scope or effect on a per-subnet basis.

Enable User-Specified DHCP Options

1. Go to the **Network > DHCP > Global Options** tab and click the **Enable** button (Figure 5-22).

2. With **Global Options** enabled on the CAS (Figure 5-23), choose one of the following option types to configure:
   - Root Global Option
   - Scoped Global Option
   - Class Option

   Once an option is added, it is displayed on this main page under the corresponding list name.
When specifying DHCP Global Options (Root, Scoped or Class), you may select a particular DHCP option by entering its number in the Option # input box on the New/Edit form.

If the desired option number is not known, or if specifying a server directive which changes server behavior but has no corresponding DHCP option number, then select the name of the option or directive from the dropdown menu next to the Set Option Type button. In either case, click the Set Option Type button after the desired DHCP option type has been selected.

DHCP option numbers are specified in RFC 2132.

**Add Root Global DHCP Option**

3. Click the New Option link at the top right-hand corner of the Root Global Option List to open the Root Global DHCP Options form (Figure 5-24). This form allows you to enter text directly into the DHCP configuration file at the root level.

**Figure 5-24  DHCP Global Options - New Root Global (Custom Option)**

4. Either type the Option #, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click Set Option Type.

5. If instead configuring a Custom Option, type the option number in the ID field, choose a data Type from the dropdown menu, and click Create Custom Option.

**Add Scoped Global DHCP Option**

6. From the Global Options main page (Figure 5-23), click the New Option link at the top right-hand corner of the Scoped Global Option List to open the Scoped Global DHCP Options form (Figure 5-24). This form allows you to enter text directly into the DHCP configuration file at the subnet scope level.
Chapter 5  Configuring DHCP

5-26

User-Specified DHCP Options

Figure 5-25  DHCP Global Options - New Scoped Global

7. Either type the Option #, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click Set Option Type.

8. If configuring a Custom Option, type the ID of the option, choose a data Type from the dropdown menu, and click Create Custom Option.

Add New Class Option

9. From the Global Options main page (Figure 5-23), choose one of the following Class Types from the dropdown menu to the right of the Class Options list:

   - All VLAN-Restricted Subnets—To apply the option to all subnets in the Subnet List (autogenerated or manually-created) that are restricted to a VLAN ID.
   - All Relay IP-Restricted Subnets—To apply the option to all subnets in the Subnet List (manually-created) that are restricted to a Relay IP.
   - No VLAN tagged—To apply the option to all subnets in the Subnet List that have no VLAN specified.
   - VLAN ID <n>—To apply the option to a specific subnet for VLAN ID (<n>) in the Subnet List.

10. Click the New Class Option button at the top right-hand corner of the Class Options List to open the New Class Option form (Figure 5-25).
11. Either type the Option #, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click Set Option Type.

12. If configuring a Custom Option, type the ID of the option, choose a Type from the dropdown menu, and click Create Custom Option.

Restore Options to Default
13. To restore factory defaults, click the Restore Options To Default button at the top-right side of the Global Options > List page (Figure 5-27).

Disable DHCP Options
To disable admin-specified DHCP options, click the Disable button at the top-left side of the Global Options > List page (Figure 5-23 on page 5-24).
Add Local Scoped DHCP Option

1. Make sure DHCP options are enabled as described in Enable User-Specified DHCP Options, page 5-24.

2. Go to Network > Subnet List > List and click the Edit button next to the subnet for which you want to add an option.

3. The Edit form appears.

4. Click the Add New Option Link at the bottom of the form. The New Local Option form appears:
Figure 5-29  Add New Local Option

Table 5-5  DHCP Server Directives

<table>
<thead>
<tr>
<th>Server Directive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow bootp</td>
<td>Allows booting by BOOTP devices. Disabled by default. Some older printers still in use require BOOTP. The BOOTP protocol does not specify a time limit for the lease assignment, although other server directives can invalidate BOOTP leases.</td>
</tr>
<tr>
<td>always-broadcast</td>
<td>Normal DHCP operation calls for the DHCP DISCOVER and OFFER packets to be broadcast if the DHCP client is unsure of where the DHCP server is located. In typical operation, the DHCP REQUEST and ACK, and all subsequent REQUESTS and ACKs between a known client and a known DHCP server are unicast. The “always-broadcast” server directive instructs the DHCP server to always respond to all DHCP packets with a broadcast packet.</td>
</tr>
<tr>
<td>always-reply-rfc1048</td>
<td>Some DHCP clients violate RFC 1048 when sending DHCP packets. The DHCP server responds by default to these clients with packets that also violate RFC 1048. A very small set of clients send a DHCP packet which violates RFC 1048, but do not accept as valid a return packet which violates RFC 1048. This server directive instructs the server to always respond with RFC-1048 compliant packets no matter what is received.</td>
</tr>
<tr>
<td>deny bootp</td>
<td>This is the default behavior of the server. This server directive instructs the server to reject BOOTP requests.</td>
</tr>
<tr>
<td>dynamic-bootp-lease-length</td>
<td>Instructs the server to invalidate and make available for re-assignment IP leases assigned to BOOTP clients. Note that this does not guarantee that the BOOTP client will stop using the IP address. This server directive can be specified as a scoped global or local option.</td>
</tr>
</tbody>
</table>
Chapter 5      Configuring DHCP

Global Action

The Global Action tab allows you to change fields on all DHCP elements of a particular CAS. For example, if you have 300 managed subnets and IP pools and you need to change the DNS server in all of them, you can achieve this using the Global Action form.

1. Go to the Network > DHCP > Global Action (Figure 5-30).

<table>
<thead>
<tr>
<th>Server Directive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>Instructs the DHCP server to fill out the filename portion of the DHCP packet. This is not an option, as it does not appear in the DHCP options list. This server directive can be specified as a scoped global or local option.</td>
</tr>
<tr>
<td>get-lease-hostname</td>
<td>Instructs the server to look up the domain name corresponding to the IP address of each address in the lease pool and use that address for the DHCP hostname.</td>
</tr>
<tr>
<td>next-server</td>
<td>Instructs the server to fill out the next-server field in all DHCP responses. This is typically used by devices which need additional configuration information, such as IP phones. This server directive can be specified as a scoped global or local option.</td>
</tr>
<tr>
<td>one-lease-per-client</td>
<td>Instructs the server to invalidate the first lease assigned to a DHCP client that has requested more than one. By default this is disabled, as some network devices require two or three addresses.</td>
</tr>
<tr>
<td>ping-check</td>
<td>Instructs the server to ping an IP address prior to assigning it. This is disabled by default, and has a significant negative impact on DHCP server performance.</td>
</tr>
<tr>
<td>server-identifier</td>
<td>Instructs the server to change its identifier. By default, the IP address of the untrusted network interface is used.</td>
</tr>
<tr>
<td>server-name</td>
<td>Instructs the server to change its name. By default, the hostname of the CAS is used. This server directive can be specified as a scoped global or local option.</td>
</tr>
<tr>
<td>use-lease-addr-for-default-route</td>
<td>Instructs the server to send a default route (gateway) equal to the assigned IP for all responses.</td>
</tr>
</tbody>
</table>
2. In the **Action will target:** dropdown, choose one of the following options:
   - **Everything** (all of the options below combined)
   - All Manual Subnets
   - All IP Reservations
   - All Auto-Generated Subnets
   - All by VLAN ID

3. Click the checkbox for each applicable parameter, then type the value in the associated textbox.
   - **VLAN ID** (when **All by VLAN ID** is chosen)
   - Default Lease Time (seconds)
   - Maximum Lease Time (seconds)
   - DNS Suffix
   - DNS Servers (separate multiple addresses with a comma)
   - WINS Servers (separate multiple addresses with a comma)

4. Click **Update**.

5. Click **Perform Action** in the confirmation page that appears (Figure 5-31).
**Figure 5-31 Example Global Action**

Device Management > Clean Access Servers > 10.201.5.120

<table>
<thead>
<tr>
<th>Status</th>
<th>Network</th>
<th>Filter</th>
<th>Advanced</th>
<th>Authentication</th>
<th>Misc</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>DHCP</td>
<td>DNS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DHCP Status** | **Subnet List** | **Reserved IPs** | **Auto-Generate** | **Global Options** | **Global Action**

**Change:**
Default Lease Time to 300 seconds

**Change applies to:**

### Subnet List

<table>
<thead>
<tr>
<th>IP Range</th>
<th>Subnet Range</th>
<th>Domain</th>
<th>VLAN ID</th>
<th># Subnets</th>
<th># IPs</th>
</tr>
</thead>
</table>

### IP Reservations

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Description</th>
<th>MAC Address</th>
<th>Reserved IP Address</th>
<th>VLAN ID</th>
</tr>
</thead>
</table>

25-05-2013