



CHAPTER 16

Device Management: Roaming (Deprecated)



Warning

The roaming feature is deprecated and will be removed in future releases.

This chapter describes how to set up subnet roaming for wireless clients. Topics include:

- [Overview, page 16-1](#)
- [Before Starting, page 16-4](#)
- [Setting Up Simple Roaming, page 16-4](#)
- [Setting Up Advanced Roaming, page 16-6](#)
- [Monitoring Roaming Users, page 16-8](#)

Overview

With roaming enabled, users can physically move between Clean Access Server-connected subnets without interruption of network connectivity. Roaming is transparent to users—they can continue to browse the Internet or use a network application without losing work if using a web application or having to log in again.

A Clean Access Server supports roaming by identifying clients who have migrated from the range of an access point managed by another Clean Access Server. The new Server tunnels the traffic from those clients back to the original Server.

When the user roams from one access point to another, the physical connection established by the wireless client is uninterrupted. Also, the client keeps the same IP address, so VPN connections do not have to be rekeyed.

You can turn on roaming for Clean Access Servers selectively. That is, you can enable it for particular Servers and leave others disabled. Since a Clean Access Server can manage multiple subnets, you can also enable roaming by individual subnets.

Requirements

There are several requirements for the network to support roaming:

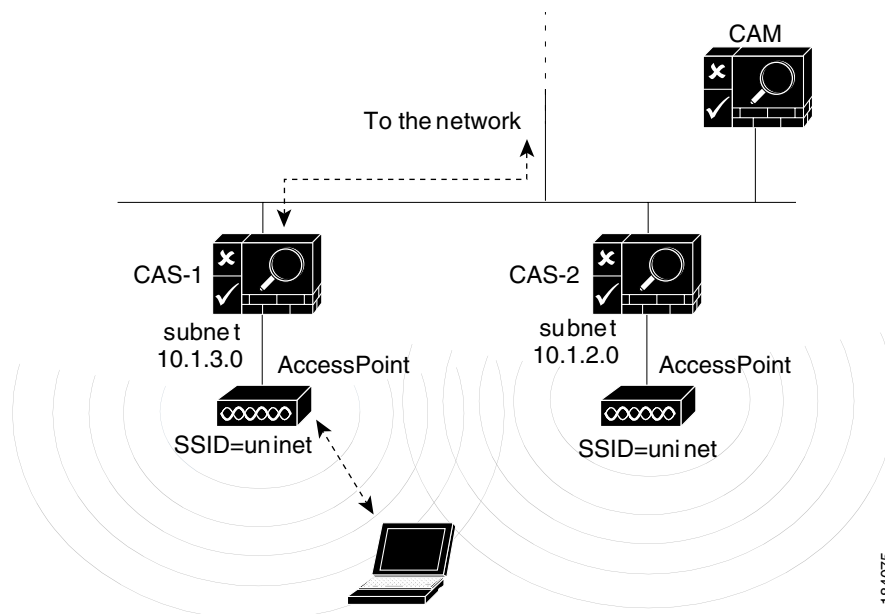
- The access points for which you want to enable roaming must all have the same SSID.
- The access point signals need to overlap. Gaps between the signals will cause the user connection to be lost.

- Each Clean Access Server that supports roaming needs to be on a different subnet.
- Clean Access Servers acting as virtual gateways only support roaming with other virtual gateway Servers. Roaming can occur between Clean Access Servers that are operating as real-IP gateways and NAT gateways, but not between these types and virtual gateways.

How Roaming Works

When users first access a roaming-enabled network, they associate with a particular access point and acquire an IP address. Also, authentication and security encryption parameters for the session are established.

Figure 16-1 Session Established



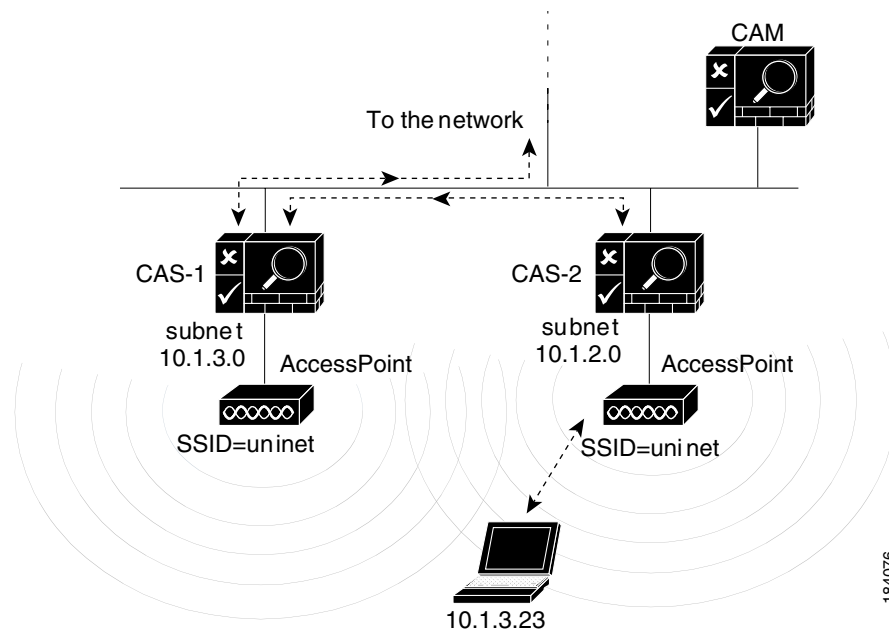
When the user moves to the range of the new access point, the IP address of the user device allows the second Clean Access Server to identify which Clean Access Server originated the session.

All traffic from the user is tunneled to the original Server, and traffic for the client is tunneled from the original Server to the current Server. From there, any filtering or other traffic handling measures or policies are enforced.

The traffic is then routed to the network as appropriate:

184075

Figure 16-2 Traffic Routing with Roaming

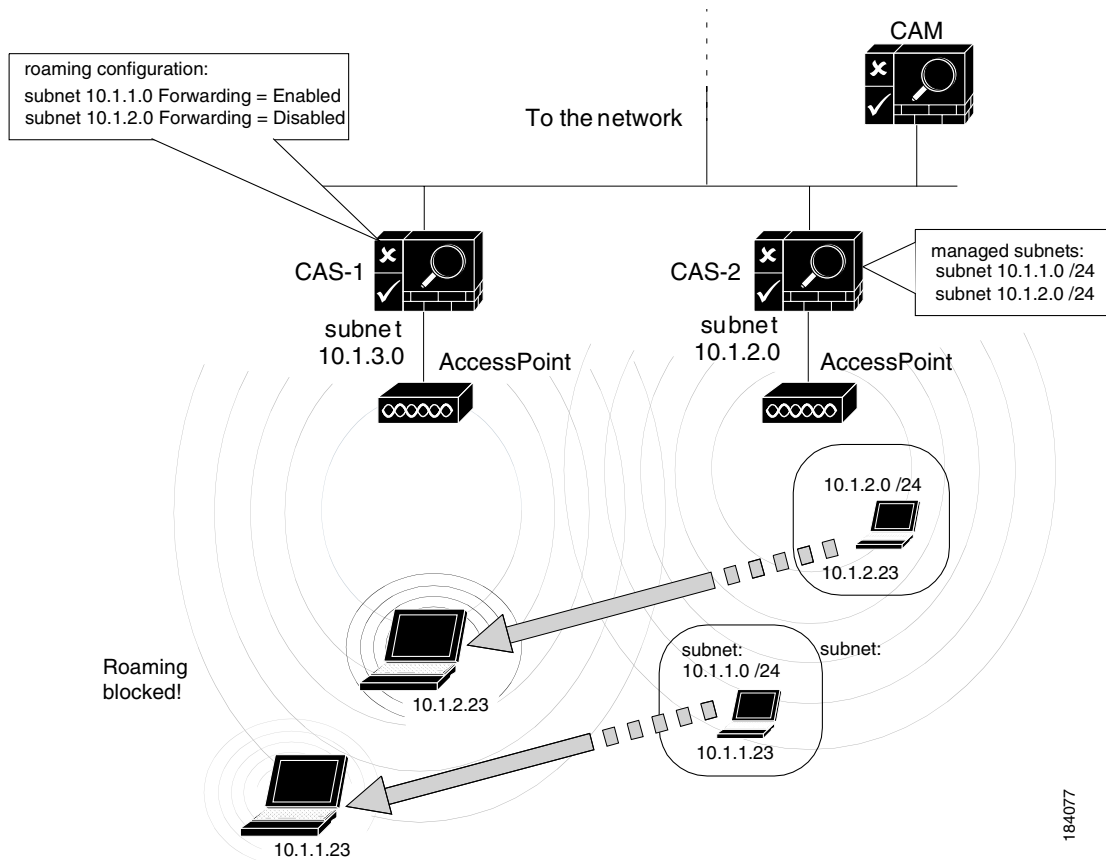


Roaming Modes

There are two roaming modes for the Clean Access Server:

- *Simple Roaming* mode – Lets you turn roaming off or on by Clean Access Server, regardless of the individual subnets that the CAS manages. Roaming applies to all subnets managed by the Clean Access Server. In most cases, simple roaming mode can be used.
- *Advanced Roaming* – Allows you to turn roaming off or on at the managed subnet level for a particular Clean Access Server. You only need to use this mode if a Server manages multiple subnets that have different roaming requirements. Clients who get an IP address in the address space of the supported subnet will be able to roam, while those that get an address from an unsupported subnet will not, as illustrated in [Figure 16-3](#).

Figure 16-3 Advanced Roaming



Before Starting

Before setting up roaming, you need to add the Clean Access Servers for which you want to support roaming to the Clean Access Manager's administrative domain. See [Add Clean Access Servers to the Managed Domain](#), page 3-2.

For advanced roaming, the managed subnets also need to be added to the Clean Access Server's configuration. To view or modify managed subnet settings, go to the following CAS configuration page: **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**. For more information, see the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(1\)](#).

Once you have configured managed Clean Access Servers and, optionally, managed subnets, use the procedures described in the following sections to set up roaming.

Setting Up Simple Roaming

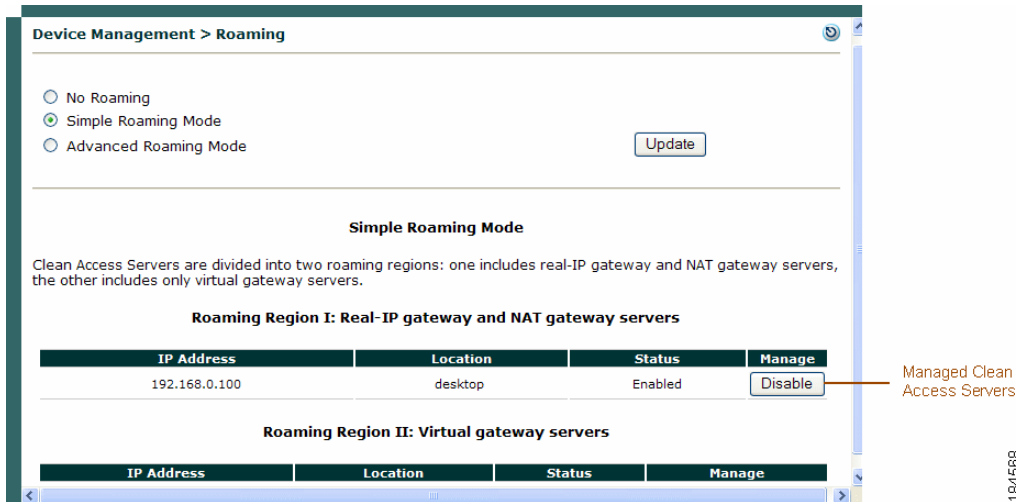
The simple roaming mode permits roaming for users per Clean Access Server. Users assigned addresses from a particular Clean Access Server will be able to roam to the Clean Access Server domains that you set up here as roaming-traffic forwarding servers.

To set up simple roaming:

1. In the Clean Access Manager admin console, click the **Roaming** link in the **Device Management** administration group:



2. Choose the **Simple Roaming Mode** button and click **Update**. The Clean Access Servers managed by the Clean Access Manager appear under the **Advanced Roaming Mode** heading:

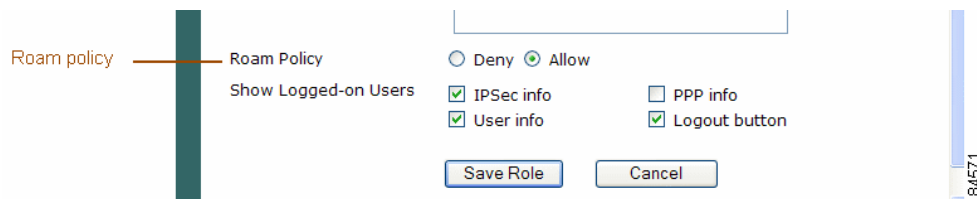


Roaming is possible only between Clean Access Servers within a roaming region, which appear at the bottom of the form. A roaming region is comprised of Servers running in roaming-compatible operating modes. Notice that roaming is not possible between Clean Access Servers of type real-IP/NAT and virtual gateway.

3. Click the **Enable** button for each Clean Access Server that you want to support roaming. Enabling roaming for a Server means that it will forward packets from users whose sessions originated in another Clean Access Server back to the original Clean Access Server. In other words, it is enabled as a roaming user destination.

The status indicator toggles between enabled and disabled.

4. Enable roaming as appropriate for particular roles. To enable roaming for a role:
 - a. Click the **User Roles** link.
 - b. In the **List of Roles** tab, click the **Edit** button for the role for which you want to enable roaming.
 - c. Choose **Allow** for the **Roam Policy** for the role.



d. Click **Save Role**.

You can turn off roaming at any time by choosing the **No Roaming** option in the roaming page and clicking **Update**. Confirm the operation when prompted.

Setting Up Advanced Roaming

The advanced roaming mode lets you enable/disable roaming for users by managed subnet. Users assigned addresses from particular subnets managed by a Clean Access Server will be able to roam to the Clean Access Server domains that you enable as roaming destinations, as described here.

1. Make sure that the subnets for which you want to permit roaming are configured in the **Managed Subnet** form of the originating Clean Access Server (that is, where the roaming users will be authenticated). To see the form, go to **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**:

Device Management > Clean Access Servers > 10.201.240.12

[Status](#)
[Network](#)
[Filter](#)
[Advanced](#)
[Authentication](#)
[Misc](#)

[Managed Subnet](#)
[VLAN Mapping](#)
[NAT](#)
[1:1 NAT](#)
[Static Routes](#)
[ARP](#)
[Proxy](#)

IP Address:

Subnet Mask:

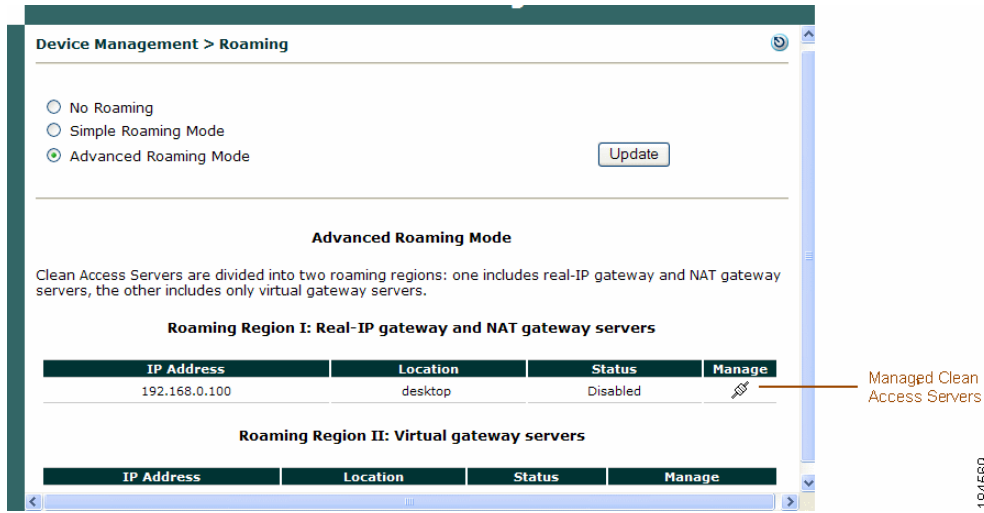
VLAN ID: (-1 for non-VLAN)

Description:

IP/Netmask	Description	VLAN	Delete
10.10.10.10 / 255.255.255.0	Main Subnet	-1	
192.168.2.1 / 255.255.255.0	CAS address for VLAN 31 managed subnet	31	X

Managed subnets

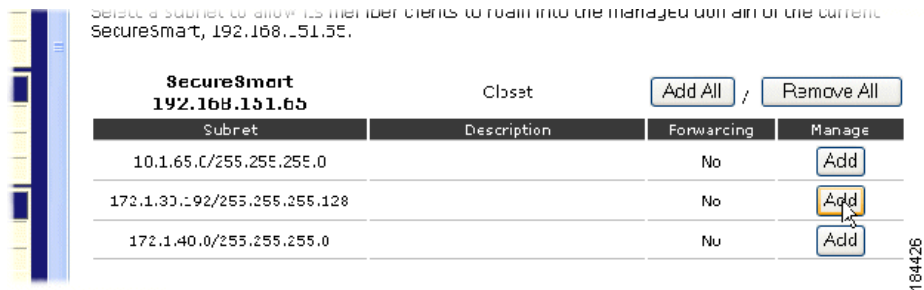
2. In the Clean Access Manager, click the **Roaming** link from the **Device Management** module.
3. Choose the **Advanced Roaming Mode** button and click **Update**. The Clean Access Servers managed by the Clean Access Manager appear under the **Advanced Roaming Mode** heading:



4. Click the **Manage** button for the Clean Access Server that you want to configure as a roaming destination.
5. Select the **Enable Roaming** option and then click **Update**:



6. For each subnet managed by another Clean Access Server that you want to enable as a roaming source, click the **Add** button:



Note

- Only subnets that have already been configured in the **Managed Subnet** form of the Clean Access Server management page appear in the list.
- Notice that the forwarding column changes to “Yes”

Select a subnet to allow its member clients to roam into the managed domain of the current SecureSmart, 192.168.151.65.

Subnet	Description	Forwarding	Manage
10.1.65.0/255.255.255.0		No	Add
172.1.30.192/255.255.255.128		Yes	Remove
172.1.40.0/255.255.255.0		No	Add

Enabled roaming source subnet

**Note**

- Clicking **Remove** disables roaming for clients in the source subnet.
- Clicking **Back** returns you to the **Device > Roaming** page.

7. Enable roaming as desired for particular roles. To enable roaming for a role:
 - a. Click the **User Roles** link.
 - b. In the **List of Roles** tab, click the **Edit** button for the role for which you want to enable roaming.
 - c. Choose **Allow** for the **Roam Policy** for the role.

Roam policy

Roam Policy

Show Logged-on Users

Deny
 Allow

IPsec info
 PPP info

User info
 Logout button

Save Role Cancel

- d. Click **Save Role**.

You can turn off roaming at any time by choosing the **No Roaming** option in the roaming page and clicking **Update**. Confirm the operation when prompted.

Monitoring Roaming Users

You can view which users are roaming from the **Monitoring > Online Users > View Online Users** page. The page also shows which Clean Access Server originated the roaming the user session and the Clean Access Server of the domain roamed into.

To view roaming users, click the **Online Users** link in the **Monitoring** administration group. An entry for a roaming user appears as follow:

User Name	User IP	User MAC	Provider	Role	SecureSmart	Foreign SecureSmart	Kick
rrair	10.1.60.191	C0:07:E9:15:03	NTDomain	almrighty	192.168.151.60		X
shotland	10.1.60.197	C0:6F:1D:1C:00	NTDomain	almrighty	192.168.151.60	192.168.151.65	X
jjohnsor	23.20.20.242	C0:02:2D:0E:00	NTDomain	almrighty	192.168.151.65		X

Roaming user

For a roaming user:

- The **CCA Server** column indicates the Clean Access Server through which the user originally logged in.

- The **Foreign CCA Server** column indicates the Clean Access Server through which the user is currently sending traffic (that is, the Clean Access Server “roamed into”). See [Display Settings, page 13-10](#) for further details on online user properties that can be monitored.

