C H A P T E R **2**

Planning Your Deployment

This chapter discusses planning considerations for deploying the software. Topics include:

- Overview, page 2-1
- Clean Access Server Operating Modes, page 2-1
- Central Versus Edge Deployment, page 2-4

Overview

Before installing the Clean Access Server (CAS), you should consider how the Clean Access Server will fit into your existing network:

- Choose the operating mode for the Clean Access Server—The operating mode determines the services the Clean Access Server will provide. For example, the CAS can operate as a bridge between the untrusted and trusted network, or it can operate as a gateway for the untrusted network.
- Deploy the Clean Access Server centrally or at the edge of your network.

This chapter describes operating modes and deployment options for the Clean Access Server. It also provides an overview of how the deployment options affect configuration of the Clean Access Server as well as any external elements in your network, such as routers.

Clean Access Server Operating Modes

The Clean Access Server can operate in one of the following in-band (IB) or out-of-band (OOB) modes:

- **IB Virtual Gateway** (L2 transparent bridge mode)—Operates as a bridge between the untrusted network and an existing gateway, while providing posture assessment, filtering and other services.
- **IB Real-IP Gateway**—Operates as the default gateway for the untrusted network.
- **IB NAT Gateway (for testing only)**—Operates as an IP router/default gateway and performs NAT (Network Address Translation) services for the untrusted network.
- **OOB Virtual Gateway** (L2 transparent bridge mode)—Operates as a Virtual Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).
- **OOB Real-IP Gateway**—Operates as a Real-IP Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).

- **OOB NAT Gateway (for testing only)**—Operates as a NAT Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).

> ✎
>
> **Note** NAT Gateway mode is primarily intended to facilitate testing, as it requires the least amount of network configuration and is easy to initially set up. However, because NAT Gateway is limited in the number of connections it can handle, NAT Gateway mode (in-band or out-of-band) is NOT supported for production deployment. Cisco NAC Appliance uses ports 20000-65535 (45536 connections) for NAT Gateway mode.

The Clean Access Manager can control both in-band and out-of-band CASs in its domain. However, the Clean Access Server itself must be *either* in-band or out-of-band.

For more information on OOB configuration in the CAM, see the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.6(1).* The following sections further describe each CAS operating mode.

Real-IP Gateway

In the Real-IP Gateway configuration, the Clean Access Server operates as the default gateway for untrusted network (managed) clients. All traffic between the untrusted and trusted network passes through the Clean Access Server, which applies the IP filtering rules, access policies, and any other traffic handling mechanisms you configure.

Figure 2-1   Real-IP Gateway Configuration
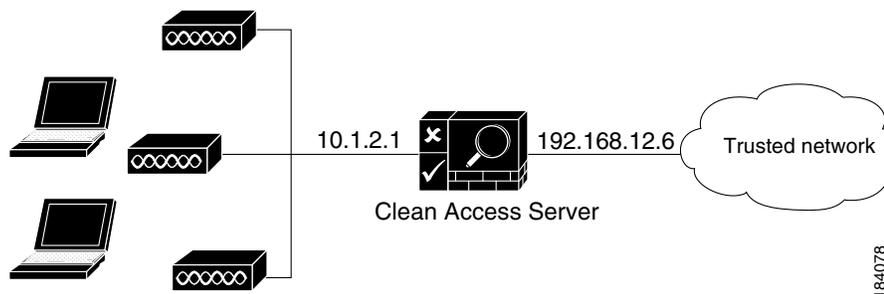
When using the Clean Access Server as a Real-IP Gateway, you need to specify the IP addresses of its two interfaces: one for the trusted side and one for the untrusted side. The two addresses should be on different subnets. The Clean Access Server can manage one or more subnets, with its untrusted interface acting as a gateway for the managed subnets. For details on setting up managed subnets, see Configuring Managed Subnets or Static Routes, page 5-26.

The Clean Access Server does not advertise routes. Instead, static routes must be added to the next hop router indicating that traffic to the managed subnets must be relayed to the Clean Access Server's trusted interface.

> ✎
>
> **Note** In Real-IP Gateway mode, the CAS can send traffic out of the trusted port in one VLAN only. You cannot configure the switch port connecting to the trusted port of the CAS as a trunk port.

Additionally, when the Clean Access Server is in Real-IP Gateway mode, it can act as a DHCP server or relay. With DHCP server functionality enabled, the CAS provides the appropriate gateway information to the clients, that is, the appropriate gateway IP held by the CAS for the particular managed subnet. If the CAS is working as a DHCP relay, then the DHCP server must be configured to provide the managed clients with the appropriate gateway information (that is, the appropriate gateway IP held by the CAS for the particular managed subnet). For further details, refer to Configuring Managed Subnets or Static Routes, page 5-26 and Chapter 6, "Configuring DHCP".
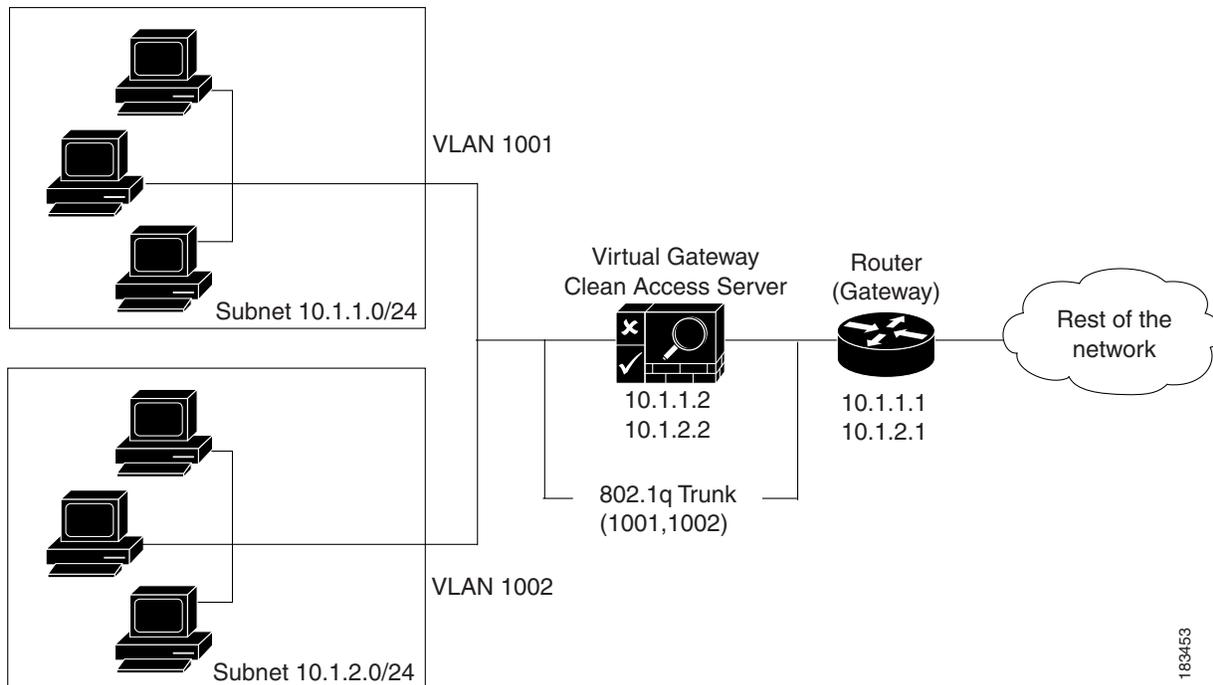
Virtual Gateway

In Virtual Gateway deployment, the Clean Access Server operates as a standard Ethernet bridge, but with the added functionality provided by the IP filter and IPSec module. This configuration is typically used when the untrusted network already has a gateway and you do not wish to alter the existing configuration.

For example, if there are two untrusted subnets, 10.1.1.0/24 and 10.1.2.0/24, with gateways 10.1.1.1 and 10.1.2.1, respectively, the CAS in Virtual Gateway mode is deployed between the untrusted subnets and their gateways (Figure 2-2). The untrusted subnets are configured as "Managed Subnets" in the CAS. Note especially that:

- The CAS needs to have an IP address on each managed subnet.
- Traffic from clients **must** pass through the CAS before hitting the gateway.

Figure 2-2   Virtual Gateway Configuration

When the CAS is a Virtual Gateway:

- The CAS and CAM **must** be on different subnets.
- eth0 and eth1 of the Clean Access Server can have the same IP address.
- All end devices in the bridged subnet must be on the untrusted side of the CAS.

- The CAS should be configured for DHCP forwarding.

- Make sure to configure managed subnets for the CAS. For the example in Figure 2-2, you would configure two managed subnets:
    - 10.1.1.2 / 255.255.255.0 1001
    - 10.1.2.2 / 255.255.255.0 1002

When the CAS is an Out-of-Band Virtual Gateway, the following also applies:

- The CAS and CAM must be on different VLANs.

- The CAS should be on a different VLAN than the user or Access VLANs.

Note
- For Virtual Gateway (In-Band or OOB), Cisco recommends connecting the untrusted interface (eth1) of the CAS to the switch only **after** the CAS has been added to the CAM via the web console.

- For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See Configure VLAN Mapping, page 5-37.

NAT Gateway

In the NAT Gateway configuration, the Clean Access Server functions similarly to the Real-IP Gateway configuration, but adds Network Address Translation (NAT) services. With NAT, clients are assigned IP addresses dynamically from a private address pool. The Clean Access Server performs the translation between the private and public addresses as traffic is routed between the untrusted (managed) and external network. The Clean Access Server supports standard, dynamic NAT and 1:1 NAT. In 1:1 NAT, there is a one-to-one correlation between public and private addresses. With 1:1 NAT, you can map port numbers as well as IP addresses for translation.

Note
NAT Gateway mode is primarily intended to facilitate testing, as it requires the least amount of network configuration and is easy to initially set up. However, because it is limited in the number of connections it can handle, NAT Gateway mode (in-band or out-of-band) is not supported for production deployment. See CAM/CAS Connectivity Across a Firewall, page 4-25 for details.

Central Versus Edge Deployment

The Clean Access Server can be deployed either centrally or at the edge of your network. A central deployment reduces the number of Clean Access Servers you need to deploy, facilitating management and scalability. In a central deployment, the Clean Access Server can be configured to perform either routing or bridging for the untrusted network.

Cisco NAC Appliance allows you to achieve multi-hop L3 deployment if you want to move the CAS several hops away from users.

Routed Central Deployment (L2)

In a routed central deployment, the Clean Access Server is configured to act as the Real-IP Gateway for each of the subnets that you wish to manage.
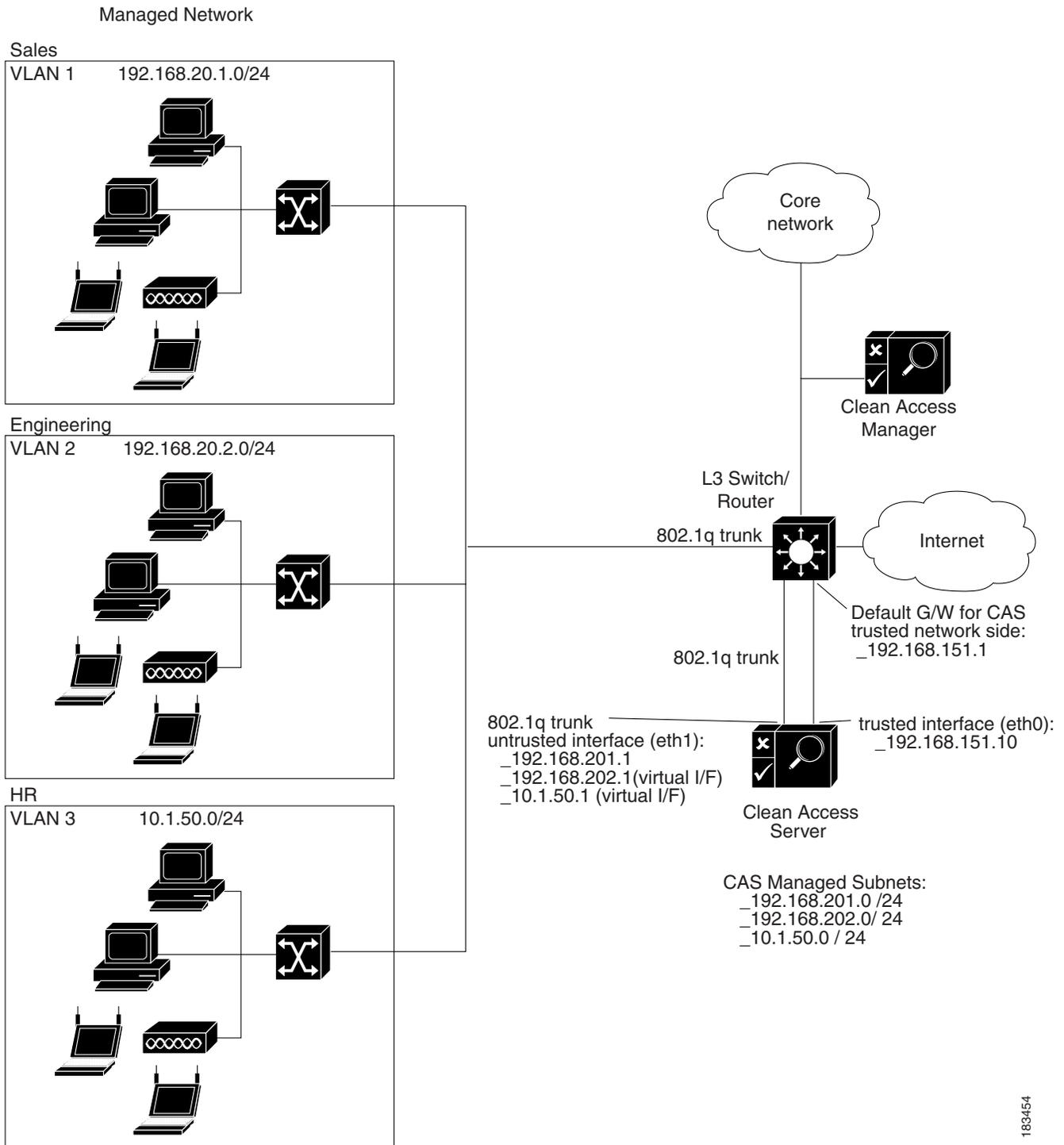
Deployment Steps

The specific steps to deploy a centrally routed Clean Access Server in a typical network include:

1. Turn off routing on your existing Layer 3 switch or router for the subnets that you wish to manage through the CAS.

2. Configure the untrusted interface of the CAS to be the gateway for the managed subnets.

3. Configure the default gateway of the CAS's trusted interface to be the L3 switch or the router.

4. Add static routes on the L3 switch or router to route traffic for the managed subnets to the CAS's trusted interface.

5. If using your own DHCP server, modify its configuration so that the default gateway address that the DHCP server passes to clients with the lease is the address of the CAS's untrusted interface.

In a VLAN-enabled environment, multiple VLANs are trunked through a single Clean Access Server. Aggregating multiple VLANs—organized by location, wiring, or shared needs of users—through a single CAS (by VLAN trunking) can help to simplify your deployment. Figure 2-3 shows a centrally-routed deployment:

Figure 2-3   Routed Central Deployment in a VLAN-Enabled Network

Managed Network

Sales
VLAN 1   192.168.20.1.0/24

Engineering
VLAN 2   192.168.20.2.0/24

HR
VLAN 3   10.1.50.0/24

Core network

Clean Access Manager

L3 Switch/ Router
802.1q trunk

Internet

Default G/W for CAS trusted network side:
_192.168.151.1

802.1q trunk

802.1q trunk
untrusted interface (eth1):
_192.168.201.1
_192.168.202.1(virtual I/F)
_10.1.50.1 (virtual I/F)

trusted interface (eth0):
_192.168.151.10

Clean Access Server

CAS Managed Subnets:
_192.168.201.0 /24
_192.168.202.0/ 24
_10.1.50.0 / 24

183454

Multi-Hop L3 Deployment

You can choose to deploy the CAS either closer to the edge of the network or several hops away from the network. With centralized L3 deployment, the CAS(es) may be placed several hops away from users. Multi-hop L3 deployment allows:

- Easier deployment. The CAS(es) are deployed between routers, spanning VLANs is not necessary and fewer CASs are needed.
- Not every packet has to go through the CAS. User traffic only needs to traverse the CAS for trusted network access.

However, note that Cisco NAC Appliance policies are enforced at the CAS only. Traffic which does not reach the CAS is not subject to policy enforcement.

Deployment Steps

The specific steps to deploy a centrally routed Clean Access Server in a typical network include:

1. Enable L3 on the CAS by going to **Device Management > CCA Servers > Manage [CAS_IP] > Network** and clicking the checkbox for **Enable L3 support for Clean Access Agent**.

2. Managed subnets should be configured for user subnets that are Layer 2 adjacent to the CAS. For user subnets that are one or more hops away from the CAS, static routes should be configured. Hence if enabling L3 support on the CAS, for the L3 users configure their subnets under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Static Routes** and NOT under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnets**.

3. Set the **Discovery Host** field under **Device Management > Clean Access > Clean Access Agent > Installation**.

4. If enabling the L3 multi-hop feature for VPN concentrator integration, perform all the configuration described in Chapter 7, "Integrating with Cisco VPN Concentrators."

Bridged Central Deployment

In a central deployment with the Clean Access Server configured as a bridge (Virtual Gateway), VLAN trunks are used to aggregate the traffic from the managed subnets to the CAS before being forwarded to their respective gateways on the L3 switch or router.

To ensure that no path exists from the clients to the gateway, Cisco recommends deploying a switch that aggregates all VLANs to the untrusted interface of the CAS, while the trusted interface of the CAS is directly connected to the L3 switch or the router, as shown in Figure 2-4. Note that the Clean Access Server interfaces will be connected to trunked ports and should provide VLAN passthrough.

Figure 2-4   *Bridged Central Deployment in a VLAN-Enabled Network*

West dormitories
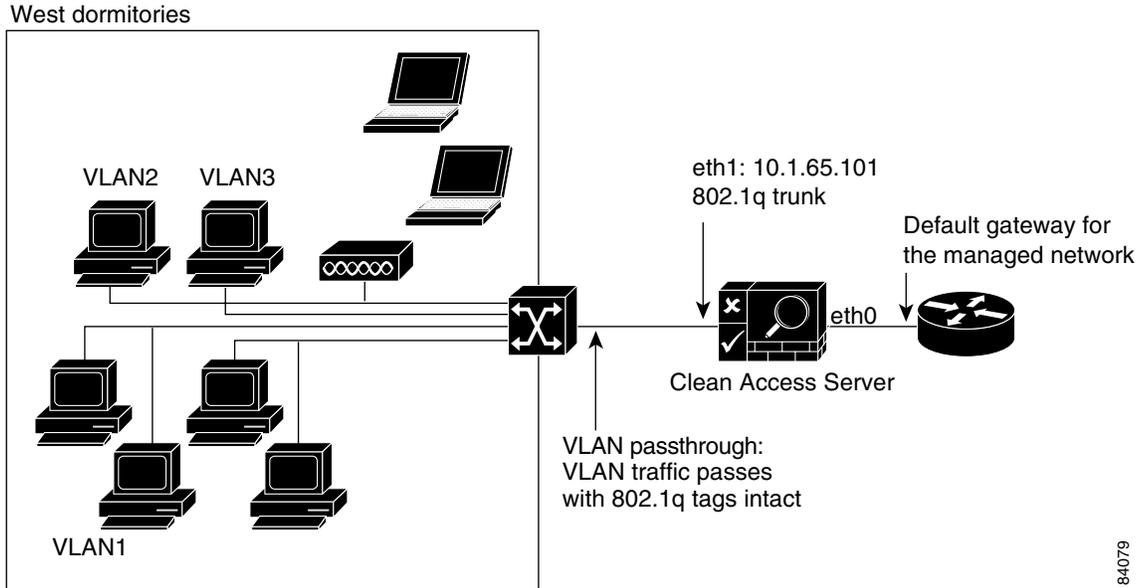
Edge Deployment

While central deployment has advantages in terms of reducing the number of required Clean Access Servers, a central deployment is not always possible. For example, if using gigabit throughput to your network's edge, an edge deployment is required. In edge deployment, the Clean Access Server is placed between each managed subnet and router in the network, as illustrated in Figure 2-5. This allows the Clean Access Server to continue to capture MAC addresses for the devices to be managed. In edge deployment, the CAS can act as either a Virtual Gateway or a Real-IP Gateway.

Figure 2-5   Edge Deployment
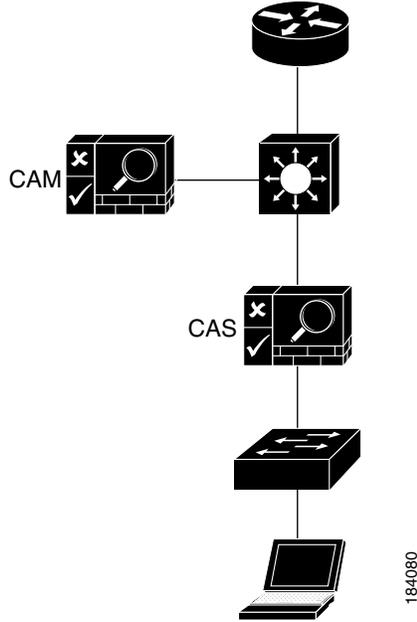
CAS Operating Mode Summary

Table 2-1 summarizes the features and advantages for each operating mode.

Table 2-1   CAS Operating Mode Summary

CAS Type	Features	Advantages
Virtual Gateway	• CAS acts like a bridge for the managed network • CAS acts as a DHCP passthrough.	• CAS acts in an unobtrusive manner. • Good if you do not want to modify the existing network. • There is no need to define static routes on the main router.
Real-IP Gateway	• CAS acts as a gateway for the managed subnet. • CAS is designated as a static route for the managed subnet. • CAS can perform DHCP services, or act as a DHCP relay.	• Good for situations in which a new subnet can be used for the managed network. • Clients are assigned real IP addresses. • Takes advantage of the CAS's advanced DHCP services.
NAT Gateway	• CAS performs NAT (Network Address Translation) or PAT (Port Address Translation) services, so that clients can use private addresses • Performs DHCP address allocation for managed clients. • All traffic originating from managed clients appears on the trusted side as originating from the Clean Access Server.	• Allows the use of a private address range for managed clients. • Setup is easy: does not involve setting up routes or creating subnets. • Only requires two IP addresses.

Table 2-1   *CAS Operating Mode Summary*

CAS Type	Features	Advantages
OOB Virtual Gateway	• CAS acts like a bridge for the managed network only during the authentication, posture assessment and remediation process. • CAS acts as a DHCP passthrough for Authentication VLAN.	• Once successfully logged on, user traffic bypasses the CAS and traverses the switch ports directly. • User can be logged out via role-based session timer or link-down SNMP traps. • Can be deployed in Edge or Core (central) switches. • No need to bounce client ports. • Recommended configuration if sharing ports between IP phones and PCs.
OOB Real-IP Gateway	• CAS acts as an inline L3 router for the managed network only during the authentication, posture assessment and remediation process. • CAS can perform DHCP services, or act as a DHCP relay. • User obtains DHCP address from Authentication VLAN. • L3 Switch/router configuration: Configure CAS as default gateway for managed subnets.	• Clients are assigned real IP addresses. • Once successfully logged on, user traffic bypasses the CAS and traverse the switch ports directly. • Port bouncing not required. DHCP release/renew is triggered by 4.1.1.0+ Agent or ActiveX/ Java Applet downloaded from web login page.
OOB NAT Gateway	• CAS acts as an inline L3 router for the managed network only during the authentication, posture assessment and remediation process. • CAS can perform DHCP services, or act as a DHCP relay. • User obtains DHCP address from Authentication VLAN. • Allows private address range via NAT configuration. • L3 Switch/router configuration: Turn off routing for managed network on L3 Switch or router	• Clients are assigned NAT IP addresses while on Authentication VLAN. • Once successfully logged on, user traffic bypasses the CAS and traverses the switch ports directly. • Need to bounce interface for client to acquire new DHCP address from Access VLAN.