



CHAPTER 3

Switch Management: Configuring Out-of-Band Deployment

This chapter describes how to configure Cisco NAC Appliance for Out-of-Band (OOB) deployment. Topics include:

- [Overview, page 3-1](#)
- [Deployment Modes, page 3-5](#)
- [Configure Your Network for Out-of-Band, page 3-14](#)
- [Configure Your Switches, page 3-15](#)
- [Configure OOB Switch Management on the CAM, page 3-22](#)
- [Configure Access to Authentication VLAN Change Detection, page 3-65](#)
- [Out-of-Band Users, page 3-66](#)
- [OOB Troubleshooting, page 3-69](#)
- [Troubleshooting SNMP, page 3-70](#)

See *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)* for additional information on L3 OOB deployment.

Overview

In a traditional in-band Cisco NAC Appliance deployment, all network traffic to or from clients goes through the Clean Access Server. For high throughput or highly routed environments, a Cisco NAC Appliance Out-of-Band (OOB) deployment allows client traffic to pass through the Cisco NAC Appliance network only in order to be authenticated and certified before being connected directly to the access network. This section discusses the following topics:

- [In-Band Versus Out-of-Band, page 3-2](#)
- [Out-of-Band Requirements, page 3-2](#)
- [SNMP Control, page 3-4](#)

In-Band Versus Out-of-Band

Table 3-1 summarizes different characteristics of each type of deployment.

Table 3-1 *In-Band vs. Out-of-Band Deployment*

In-Band Deployment Characteristics	Out-of-Band Deployment Characteristics
The Clean Access Server (CAS) is always inline with user traffic (both before and following authentication, posture assessment and remediation). Enforcement is achieved through being inline with traffic.	The Clean Access Server (CAS) is inline with user traffic only during the process of authentication, assessment and remediation. Following that, user traffic does not come to the CAS. Enforcement is achieved through the use of SNMP to control switches and VLAN assignments to ports.
The CAS can be used to securely control authenticated and unauthenticated user traffic by using traffic policies (based on port, protocol, subnet), bandwidth policies, and so on.	The CAS can control user traffic during the authentication, assessment and remediation phase, but cannot do so post-remediation since the traffic is out-of-band.
Does not provide switch port level control.	Provides port-level control by assigning ports to specific VLANs as necessary.
In-Band deployment is supported when deploying for wireless networks.	Wireless OOB requires a specific network topology and configuration. For more information, see Chapter 4, “Wireless LAN Controller Management: Configuring Wireless Out-of-Band Deployment.”
Cisco NAC Appliance In-Band deployment with supported Cisco switches is compatible with 802.1x	Cisco does not recommend using 802.1x in an OOB deployment, as conflicts will likely exist between Cisco NAC Appliance OOB and 802.1x to set the VLAN on the switch interfaces/ports.

Out-of-Band Requirements

Out-of-band implementation of Cisco NAC Appliance requires the following to be in place:

- Controlled switches must be supported models (or service modules) that use at least the minimum supported version of IOS or CatOS (supporting MAC change notification/MAC move notification or linkup/linkdown SNMP traps).

Supported switch models include:

- Cisco Catalyst Express 500 Series
- Cisco Catalyst 2900 XL
- Cisco Catalyst 2940/2950/2950 LRE/2955/2960
- Cisco Catalyst 3500 XL
- Cisco Catalyst 3550/3560/3750
- Cisco Catalyst 4000/4500/4948
- Cisco Catalyst 6000/6500

Supported 3750 service modules for Cisco 2800/3800 Integrated Services Routers (ISR) include:

- NME-16ES-1G
 - NME-16ES-1G-P
 - NME-X-23ES-1G
 - NME-X-23ES-1G-P
 - NME-XD-24ES-1S-P
 - NME-XD-48ES-2S-P
- Your Cisco NAC Appliance product license must enable OOB.

**Note**

Administrators can update the object IDs (OIDs) of supported switches through CAM updates (under **Device Management > Clean Access > Updates > Summary | Settings**). For example, if a new switch (such as C3750-XX-NEW) of a supported model (Catalyst 3750 series) is released, administrators only need to perform Cisco Updates on the CAM to obtain support for the switch OIDs, instead of performing a software upgrade of the CAM/CAS.

The update switch OID feature only applies to existing models. If a new switch series is introduced, administrators will still need to upgrade to ensure OOB support for the new switches. See [Configure and Download Updates, page 9-11](#).

**Note**

- With IOS release 12.2.25(SEG) for CE500, MAC notification SNMP traps are supported on all Smartport roles (including DESKTOP and IPPHONE roles). After upgrading to 12.2.25(SEG), customers can configure MAC notification for CE500 under **OOB Management > Devices > List > Config [Switch IP] > Config > Advanced** on the CAM. For Cisco NAC Appliance 3.6.2, 3.6.3, 4.0.0, 4.0.1, 4.0.2, CE500 supports linkup/linkdown SNMP notifications by default and the “OTHER role” warning message can be ignored when changing to MAC notification traps. In later Cisco NAC Appliance releases, this warning message is removed and the default control method for CE500 is MAC notification traps.
- If running an IOS version earlier than 12.2(25) SEG, the CE500 switch ports must be assigned to the OTHER role (not Desktop or IP phone) on the switch's Smartports configuration; otherwise, MAC notification is not sent.

**Note**

Cisco NAC Appliance OOB supports Cisco Catalyst 3750 StackWise technology. With stacks, when MAC notification is used and there are more than 252 ports on the stack, MAC notification cannot be set/unset for the 252nd port using the CAM. There are two workarounds: 1) Use linkup/linkdown SNMP notifications only. 2) If using MAC notification, do not use the 252nd port and ignore the error; other ports will work fine.

Clusters are not supported.

**Note**

For the most current details on switch model/IOS/CatOS version support, refer to [Switch Support for Cisco NAC Appliance](#).

SNMP Control

With out-of-band deployment, you can add switches to the Clean Access Manager's domain and control particular switch ports using the Simple Network Management Protocol (SNMP). SNMP is an application layer protocol used by network management tools to exchange management information between network devices. Cisco NAC Appliance supports the following SNMP versions:

CAM to OOB Switch	OOB Switch to CAM (Traps)
Read: <ul style="list-style-type: none"> SNMP V1 SNMP V2c (V2 with community string) Write: <ul style="list-style-type: none"> SNMP V1 SNMP V2c SNMP V3 	<ul style="list-style-type: none"> SNMP V1 SNMP V2c SNMP V3

You first need to configure the switch to send and receive SNMP traffic to/from the Clean Access Manager, then configure matching settings on the Clean Access Manager to send and receive traffic to/from the switch. This will enable the Clean Access Manager to get VLAN and port information from the switch and set VLANs for managed switch ports.

Cisco NAC Appliance also provides support for SHA-1 and 3DES encryption, which is required when configuring SNMP management on a CAM operating in a FIPS 140-2 compliant network.

Network Recovery for "Off Line" Out-of-Band Switches

Cisco NAC Appliance features configurable SNMP polling behavior for Out-of-Band managed switches to ensure that the CAM is able to communicate with switches experiencing network issues when they return to normal operation. Without this function, Cisco NAC Appliance might lose communication with managed switches altogether and remain undetected for some time, requiring the Cisco NAC Appliance administrator to manually step in and clear up the switch behavior and re-establish CAM-to-switch communication.

You can configure this feature using the following settings in the **smartmanager_conf** table of the CAM CLI:

- OobSnmpErrorLimit**—This is maximum number of consecutive SNMP timeout failures. If the number of consecutive failures reaches this value, the switch is disabled. If the administrator specifies the limit so that it is equal to or is less than 0, this feature is disabled. The default value is 10.
- OobSnmpRecoverInterval**—This is the internal time period (in minutes) that the recovery process waits to check disabled switches to see if they have come back online. The default value is 10.

Deployment Modes

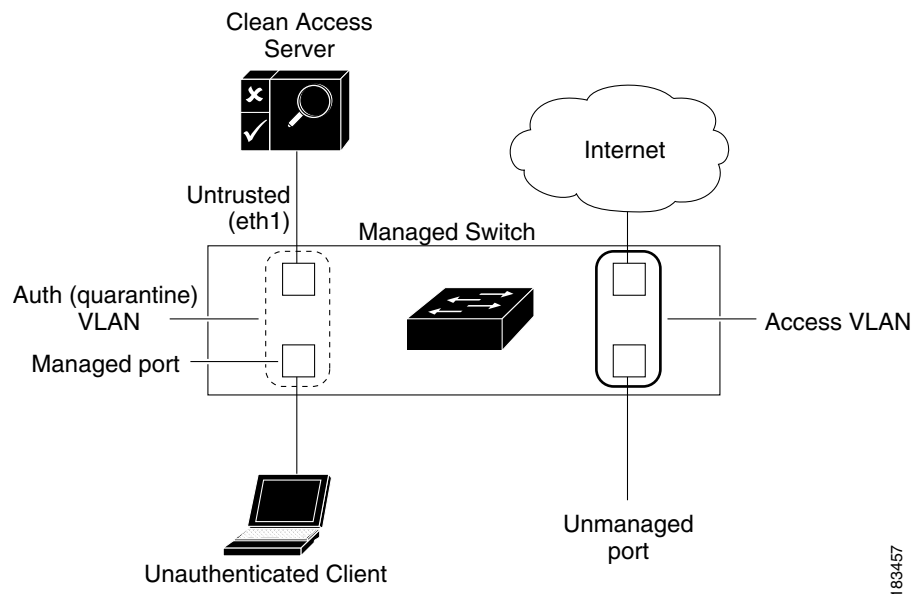
This section describes out-of-band deployment for Virtual Gateway and Real-IP. For all gateway modes, to incorporate Cisco NAC Appliance Out-of-Band in your network, you must add an Authentication VLAN to your network and trunk all Auth VLANs to the untrusted interface of the Clean Access Server.

- [Basic Connection, page 3-5](#)
- [Out-of-Band Virtual Gateway Deployment, page 3-6](#)
- [Out-of-Band Real-IP Gateway Deployment, page 3-10](#)
- [L3 Out-of-Band Deployment, page 3-13](#)

Basic Connection

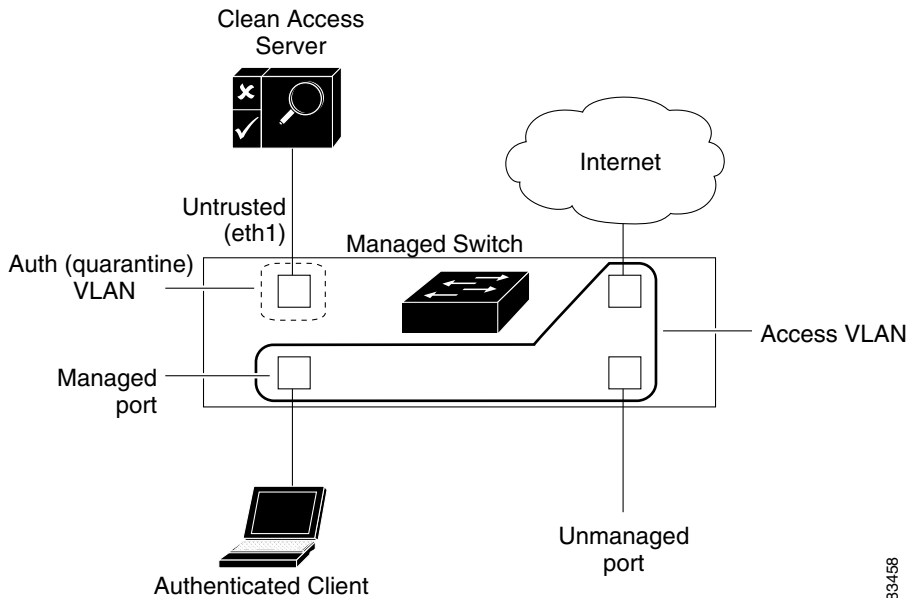
The following diagrams show basic “before” and “after” VLAN settings for a client attached to an out-of-band deployment. [Figure 3-1](#) illustrates the in-band client and [Figure 3-2](#) illustrates the client when out-of-band.

Figure 3-1 Before — Client is In-Band for Authentication/Certification



When an unauthenticated client first connects to a managed port on a managed switch ([Figure 3-1](#)), the CAM instructs the switch to change the client port from the authentication (quarantine) VLAN specified in the Port Profile for the port. The switch then sends all traffic from the Auth VLAN client to the untrusted interface of the Clean Access Server (CAS). The client authenticates through the CAS, and/or goes through Nessus Scanning/posture assessment as configured for the role or device. Because the client is on the authentication VLAN, all the client’s traffic must go through the CAS and the client is considered to be in-band.

183457

Figure 3-2 After — Client is Out-of-Band After Being Certified

Once the client is authenticated and certified (i.e. on the Certified Devices List), the CAM instructs the switch to change the VLAN of the client port to the Access VLAN specified in the Port Profile of the port (Figure 3-2). Once the client is on the Access VLAN, the switch no longer directs the client's traffic to the untrusted interface of the CAS. At this point the client is on the trusted network and is considered to be out-of-band.

In the event the user reboots the client machine, unplugs it from the network, or the switch port goes down, this triggers the switch to send a linkdown trap to the CAM. Thereafter, the client port behavior depends on the Port profile settings for the specific port (see [Add Port Profile](#), page 3-31 for details).

If the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to “kick” the user out, for example) and the switch changes the VLAN assignment for the client's access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see [Configure Access to Authentication VLAN Change Detection](#), page 3-65. (In earlier releases, the client machine would only learn of the switch after the DHCP lease for the client IP address had run out and could not reconnect.)

**Note**

You can configure the Initial VLAN of the port to be the Access VLAN. See [Add Port Profile](#), page 3-31 for details.

Out-of-Band Virtual Gateway Deployment

An out-of-band Virtual Gateway deployment provides the following benefits:

- The client never needs to change its IP address from the time it is acquired to the time the client gains actual network access on the Access VLAN.
- For L2 users, static routes are not required.

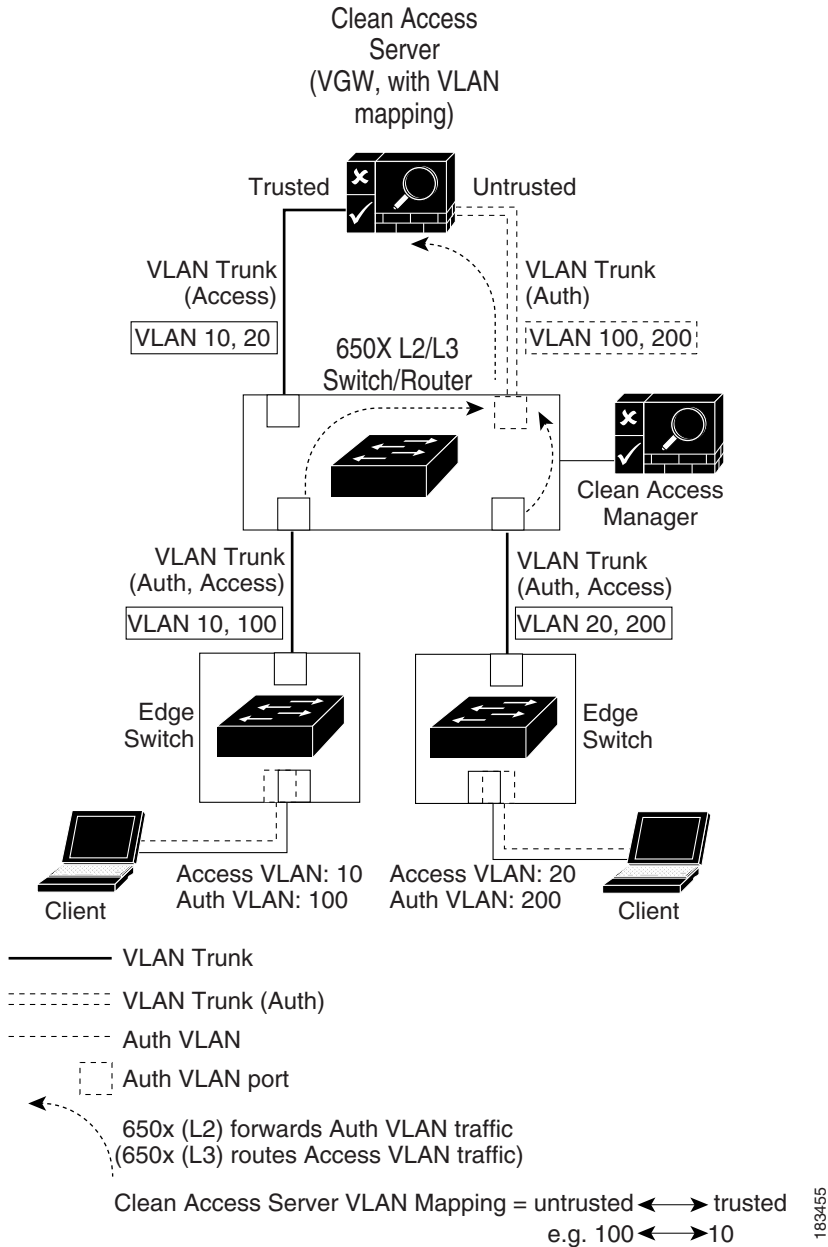
In out-of-band Virtual Gateway mode, the Clean Access Server uses the VLAN mapping feature to retag the unauthenticated client's allowed traffic (such as DNS or DHCP requests) from the Authentication VLAN to the Access VLAN and vice versa. In this way, no new client IP address is needed when the client is eventually switched to the Access VLAN, because the DHCP-acquired IP address is already paired with the Access VLAN ID.

**Note**

In an environment where there is an 802.1q trunk to the CAS, the CAS will bridge two VLANs together. This “retagging” is the rewriting of the 802.1q Ethernet header with a new VLAN ID. This feature does not apply when there is only one Authentication VLAN and one Access VLAN, as no frames are tagged.

[Figure 3-3](#) illustrates out-of-band Virtual Gateway mode using an L3 router/switch. The router/switch receives traffic from the Auth VLAN as Layer 2 traffic and forwards it to the untrusted side of the Clean Access Server. The Virtual Gateway Clean Access Server performs VLAN mapping for allowed traffic (DNS, DHCP) from the Auth VLAN (untrusted interface) to the Access VLAN (trusted interface) and vice versa. The router/switch receives traffic from the Access VLAN as Layer 3 traffic and routes it accordingly. [Figure 3-3](#) illustrates the client authentication and access path for the OOB Virtual Gateway example described below. In this example, the Authentication VLAN is 100, and the Access VLAN is 10.

Figure 3-3 Out-of-Band VGW Mode: Catalyst 6500 Series Example



Flow for OOB VGW Mode

1. The unauthenticated user connects the client machine to the network through an access layer switch.
2. The switch sends MAC notification or linkup/linkdown SNMP traps for the client to the CAM. Because the client is not on the Certified Devices List/Online Users List yet, the CAM sends an SNMP SET trap to the switch instructing it to change the client port to the Auth VLAN specified in the Port Profile (100), and the CAM places the client on the out-of-band Wired Clients list (**OOB Management > Devices > Discovered Clients > Wired Clients**).

**Note**

To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

3. The client attempts to acquire a DHCP address. The core L2 switch forwards all Auth VLAN traffic to the out-of-band Virtual Gateway CAS.
4. The CAS receives the VLAN 100 traffic on its untrusted interface (via the 802.1q trunk).
5. With VLAN mapping rules already configured to map the Auth VLAN to the Access VLAN (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**), the CAS retags the allowed DHCP traffic from VLAN 100 on its untrusted side to VLAN 10 on its trusted side and forwards the retagged traffic on its trusted interface to the L3 router/DHCP server.

**Note**

When the CAS is a Virtual Gateway, it can only be in DHCP Passthrough mode. When VLAN mapping is used for out-of-band, the default permissions on the filters transparently allow DNS and DHCP traffic from the untrusted interface, and no additional traffic control policies need to be configured. See the [Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7\(5\)](#) for details on VLAN mapping.

6. From the router's point of view, this is a request from VLAN 10. The router returns the DHCP response to VLAN 10 on the CAS.
7. With VLAN mapping rules enabled, the CAS retags the allowed traffic (on the 802.1q trunk) from VLAN 10 to VLAN 100 and forwards the DHCP response to the initiating client.
8. The client authenticates through the Clean Access Server via web login or the Agent. If configured, the client goes through posture assessment, all the while transmitting and receiving traffic on the Auth VLAN (100) to the CAS. All traffic that is permitted for remediation is allowed to pass through the CAS, and is placed on VLAN 10. If the traffic is not permitted, it is dropped. When certified, the client is placed on the Certified Devices List.
9. At this point, CAM sends an SNMP SET trap to the switch instructing it to change the client port from the Auth VLAN (100) to the Access VLAN (10) (as specified in the Port Profile), and puts the MAC address of the client in the OOB Online Users list (**Monitoring > Online Users > View Online Users > Out-of-Band**).
10. Because this is an OOB Virtual Gateway deployment, and the client already has an IP address associated with the Access VLAN, the client port is not bounced after it is switched to the Access VLAN.
11. Once the client is on the Access VLAN, the client is on the trusted network and the client's traffic no longer goes through the Clean Access Server.

**Note**

If the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to "kick" the user out, for example) and the switch changes the VLAN assignment for the client's access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see [Configure Access to Authentication VLAN Change Detection, page 3-65](#).

12. For certified clients, the Port Profile form (**OOB Management > Profiles > Port > New or Edit**) provides the following options (see [Add Port Profile, page 3-31](#) for details). You can switch the client to:
 - The Access VLAN specified in the Port Profile form.
 - The Access VLAN specified for the *user role* of the client, if you choose to use a role-based port profile (see [Figure 3-9 on page 3-24](#) for details).
 - The initial VLAN of the port. For this configuration, the client port is switched to the Auth VLAN for authentication/certification, then when the client is certified, the port is switched back to the initial VLAN of the port saved by the CAM when the switch was added.

Note also that:

- If the client's MAC address is on the Certified Devices List, but not on the out-of-band Online Users list (in other words, the client is certified but logged off the network), you can keep the client on the Access VLAN at the next login (allowing trusted network access), or you can put the client on the Auth VLAN at the next login to force the user to re-authenticate through the CAS. Because the client is already certified, the client does not go through Nessus Scanning, only posture assessment.
- Removing an OOB client from the Certified Devices List removes the out-of-band user from the Out-of-Band Online Users List. You can optionally configure the port also to be bounced.
- Client machine shutdown/reboot will trigger a linkdown trap (if set up on the switch) sent from the switch to the CAM. The behavior of the client (Agent or web login) depends on the Port Profile setting for that specific port.
- If the CAM is down and the CAS is performing VLAN mapping in "fail open" state, do not reboot the CAS because the VLAN mapping capability will be lost until the CAM comes back online.

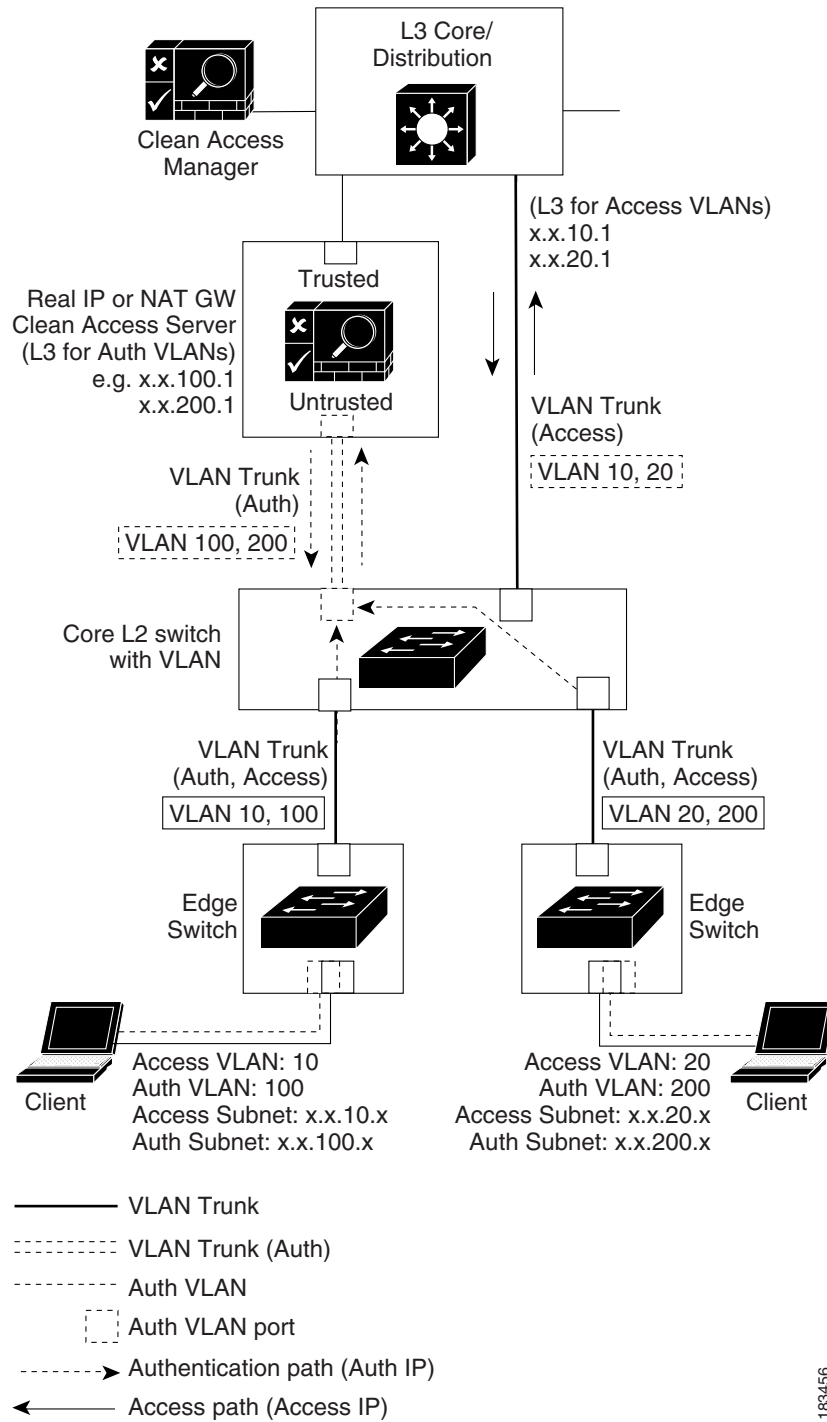
For additional configuration information, see the "Understanding VLAN Settings" and "VLAN Mapping in Virtual Gateway Mode" sections of the [Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7\(5\)](#).

Out-of-Band Real-IP Gateway Deployment

In out-of-band Real-IP gateway deployment, the client IP address has to change when the port is changed from the Auth VLAN to the Access VLAN.

[Figure 3-4](#) illustrates the sequence described below. In this example, the Authentication VLAN is 100, and the Access VLAN is 10.

Figure 3-4 Out-of-Band Real-IP Gateway Deployment



183456

Flow for OOB Real-IP Gateway Mode

1. The unauthenticated user connects the client machine to the network through an edge switch.
2. The switch sends MAC notification or linkup/linkdown SNMP traps for the client to the CAM. Because the client is not on the Certified Devices List/Online Users List yet, the CAM sends an SNMP SET trap to the switch instructing it to change the client port to the Auth VLAN specified in the Port Profile (100), and the CAM places the client on the out-of-band Wired Clients list (**OOB Management > Devices > Discovered Clients > Wired Clients**).



Note

To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

3. The unauthenticated client requests and receives an IP address on the Auth VLAN (x.x.100.x).
4. The client authenticates through the CAS via web login or the Agent. If configured, the client goes through posture assessment, all the while transmitting and receiving traffic on the Auth VLAN (100) to the CAS. When clean, the client is placed on the Certified Devices List. The CAS acts as the default gateway while the client remediates. Only permitted traffic is allowed to pass through from the untrusted to trusted interface.
5. At this point, the CAM instructs the switch to change the client switch port from the Authentication VLAN (100) to the Access VLAN (10) (according to the Port Profile), and puts the client MAC address on the out-of-band Online Users list (**Monitoring > Online Users > View Online Users > Out-of-Band**).
6. The client port is switched to the Access VLAN and is bounced (as set in the Port Profile). When the port is bounced, the client acts as if the network cable is unplugged, thus releasing its DHCP binding on the interface. Once the port is brought back up from the shutdown state, the client performs a DHCP renewal or discovery, as if it were connecting to the network for the first time. Since the switch port is now on a different VLAN, the client receives a new IP address that is valid for the access subnet.
7. With an IP address on the Access VLAN (x.x.10.x), the client now transmits traffic on the trusted network, on the Access VLAN specified in the Port Profile.
8. Once the client is on the Access VLAN, the client's traffic no longer goes through the CAS.



Note

If the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to “kick” the user out, for example) and the switch changes the VLAN assignment for the client's access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see [Configure Access to Authentication VLAN Change Detection, page 3-65](#).

9. For certified clients, the Port Profile form (**OOB Management > Profiles > Port > New/Edit**) provides the following options (see [Add Port Profile, page 3-31](#)). You can switch the client to:
 - The Access VLAN specified in the Port Profile form.
 - The Access VLAN specified for the *user role* of the client, if you choose to use a role-based port profile (see [Figure 3-9 on page 3-24](#) for details).

- The initial VLAN of the port. For this configuration, the client port is switched to the Authentication VLAN for authentication/certification, then when the client is certified, the port is switched back to the initial VLAN of the port saved by the CAM when the switch was added.

**Note**

- If the client's MAC address is on the Certified Devices List, but not on the out-of-band Online Users list (in other words, the client is certified but logged off the network), you can keep the client on the Access VLAN at the next login (allowing trusted network access), or you can put the client on the Authentication VLAN at the next login to force the user to re-authenticate through the CAS. Because the client is already certified, the client does not go through Nessus Scanning, only posture assessment.
- Removing an OOB client from the Certified Devices List removes the out-of-band user from the Out-of-Band Online Users List and bounces the port. You can optionally configure the Port Profile not to bounce the port.

L3 Out-of-Band Deployment

For details on L3 OOB, refer to the following sections:

- [Enable Web Client for Login Page, page 5-5](#)
- “Configuring Layer 3 Out-of-Band (L3 OOB)” in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(5)*.

Configure Your Network for Out-of-Band

The Clean Access Manager (CAM) manages out-of-band Clean Access Servers (CASs) and switches through the admin network. The trusted interface of the CAS connects to the admin/management network, and the untrusted interface of the CAS connects to the managed client network.

When a client connects to a managed port on a managed switch, the port is set to the authentication VLAN and the traffic to/from the client goes through the Clean Access Server. After the client is authenticated and certified through the Clean Access Server, the port connected to the client is changed to the access VLAN. Once on the access VLAN, traffic to and from certified clients bypasses the Clean Access Server.

In most OOB deployments (except L2 OOB Virtual Gateway where the Default Access VLAN is the Access VLAN in the Port profile), the client needs to acquire a different IP address from the Access VLAN after posture assessment.

For Real-IP Gateway setup, the client port is bounced to prompt the client to acquire a new IP address from the admin/access VLAN.

The next sections describe the configuration steps needed to set up your OOB deployment:

- [Configure Your Switches, page 3-15](#)
- [Configure OOB Switch Management on the CAM, page 3-22](#)
- [Configure Access to Authentication VLAN Change Detection, page 3-65](#)

**Note**

If configuring the CAS as an OOB Virtual Gateway, do not connect the untrusted interface to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See the [Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7\(5\)](#) for details.

Configure Your Switches

This section describes the steps needed to set up switches to be used with Cisco NAC Appliance Out-of-Band.

- [Configuration Notes, page 3-15](#)
- [Example Switch Configuration Steps, page 3-16](#)
- [OOB Network Setup/Configuration Worksheet, page 3-21](#)

Configuration Notes

The following considerations should be taken into account when configuring switches for OOB:

- Before you configure the CAM to manage switches in your network, Cisco recommends updating the switch OIDs on the CAM via the **Device Management > Clean Access > Updates > Update** web console page to ensure you have the most up-to-date switch support available.
- Because Cisco NAC Appliance OOB can control switch trunk ports, ensure the uplink ports for managed switches are configured as “unmanaged” ports after upgrade. This can be done in one of two ways:
 - Before upgrade, change the **Default Port Profile** for the entire switch to “unmanaged” (see [Config Tab, page 3-60](#)).
 - After upgrade, change the **Profile** for the applicable uplink ports of the switch to “unmanaged” (see [Ports Management Page, page 3-51](#)).

This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile.

- Cisco NAC Appliance OOB supports 3750 StackWise technology. With stacks, when MAC notification is used and there are more than 252 ports on the stack, MAC notification cannot be set/unset for the 252nd port using the CAM. There are two workarounds:
 - Use linkup/linkdown SNMP notifications only
 - If using MAC notification, do not use the 252nd port and ignore the error; other ports will work fine
- Switch clusters are not supported. As a workaround, assign an IP address to each switch.
- Cisco recommends enabling ifindex persistence on the switches.
- Cisco recommends turning on portfast on access ports (those directly connected to client machines).
- Cisco recommends setting the mac-address aging-time to a minimum of 3600 seconds.
- On some models of Cisco switches (e.g. 4507R, IOS Version 12.2(18) EW), the MAC address(es) connected to a particular port may not be available after Port Security is enabled.
- If implementing High-Availability, do not enable Port Security on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.
- You must ensure your switch has the Access VLAN in its VLAN database to ensure proper switching behavior. On some models of Cisco switches (e.g. 6506, IOS Version 12.2(18) SXD3), MAC address(es) connected to a particular port may not be available when the Access VLAN of the port does not exist in the VLAN database.
- Only Ethernet (Fa, Gi, fiber) port types (reported by SNMP) are displayed.

- If no healthy Clean Access Manager is in service, ports remain in the VLAN they are in until connectivity to the CAM is restored.
- For SNMP V3, each switch to be managed by the CAM must have unique Engine ID.
- The syntax for "mac-address notification" commands varies for different switch versions. When a switch is upgraded, the change in the syntax should be evaluated. The modified commands should be re-applied to the switch configuration after upgrading and reloading the switch.

Example Switch Configuration Steps

- Step 1** Connect the machines and switches. Write down the admin VLAN, Access VLAN, Authentication VLAN and other information (see [Table 3-2](#) for a detailed list).

Clean Access Manager (CAM):	172.16.1.61
CAM management VLAN:	VLAN 2
Clean Access Server (CAS):	10.60.3.2
CAS management VLAN:	VLAN 3
Access VLANs:	10, 20
Authentication VLANs:	31, 41
Switch (Catalyst 2950):	172.16.1.64

The trusted interface of the CAS is connected to the trunk port for Access VLANs 10, 20 and the untrusted interface of the CAS is connected to the trunk port for Auth VLANs 31, 41.

Refer the switch documentation for details on configuring your specific switch model.

- Step 2** Configure the switch IP address (172.16.1.64) and Access VLANs (10, 20).
- Step 3** When using Virtual Gateway with VLAN mapping, make sure there is no VLAN interface for any of the Auth VLANs on your existing Layer 3 switch or router (e.g. CAT 6500). For example, for an Access VLAN 10 and Auth VLAN 31 for which VLAN mapping has been configured on the CAS, and if an interface already exists on the L3 switch/router for the Auth VLAN, you can turn it off using the following commands:

```
(config)# no int vlan 31
(config)# vlan 31
```

The first command turns off the interface and the second ensures VLAN 31 (Auth VLAN) is in the VLAN database table. You will also need to Enable VLAN Mapping in the CAS as described in [Figure 3-8 on page 3-24](#).



Note

If the CAM is down and the CAS is performing VLAN mapping in “fail open” state, do not reboot the CAS because the VLAN mapping capability will be lost until the CAM comes back online.

- Step 4** For Real-IP Gateways, add static routes on the L3 switch or router to route traffic for the managed subnets to the trusted interface of the respective CASs.
- Step 5** Configure SNMP miscellaneous settings:

```
(config)# snmp-server location <location_string>
(config)# snmp-server contact <admin_contact_info>
```



Note When configuring SNMP settings on switches, never use the “@” character in the community string.

Step 6 Configure the SNMP read community string used in [Configure Switch Profiles, page 3-27](#). The SNMP read-only community string is “c2950_read:”

```
(config)# snmp-server community c2950_read RO
```

Step 7 Configure the SNMP write community string (V1/V2c) or username/password (V3) used in [Configure Switch Profiles, page 3-27](#).

- SNMP V1/V2c settings (SNMP read-write community string is “c2950_write”):

```
(config)# snmp-server community c2950_write RW
```

- SNMP V3 settings:

For auth (username: “c2950_user;” password: “c2950_auth”):

```
(config)# snmp-server view v1default iso included
(config)# snmp-server group c2950_group v3 auth read v1default write v1default
(config)# snmp-server user c2950_user c2950_group v3 auth md5 c2950_auth
```

For priv (username: “c2950_user;” password: “c2950_priv”):

```
(config)# snmp-server view v1default iso included
(config)# snmp-server group c2950_group v3 priv read v1default write v1default
(config)# snmp-server user c2950_user c2950_group v3 auth md5 c2950_auth priv des
c2950_priv
```

Step 8 Enable MAC notification or linkup/linkdown SNMP traps and set MAC address table aging-time when necessary for the switch.

To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps. If enabling MAC notification traps, the MAC address table aging-time must be set to a non-zero value. Cisco recommends setting the MAC address table aging-time to at least 3600 seconds for switches that have limited space for MAC addresses, and to a higher value (e.g. 1000000) if your switches support a sufficiently large number of MAC entries. If a switch supports MAC notification traps, Cisco NAC Appliance uses the MAC change notification/MAC move notification trap by default, in addition to linkdown traps (to remove users). If the switch does not support MAC change notification/MAC move notification traps, the Clean Access Manager uses linkup/linkdown traps only.

```
(config)# snmp-server enable traps mac-notification
(config)# snmp-server enable traps snmp linkup linkdown
(config)# mac-address-table aging-time 3600
```

Step 9 Enable the switch to send SNMP MAC notification and linkup traps to the Clean Access Manager. The switch commands used here depend on the SNMP version used in the SNMP trap settings in [Configure SNMP Receiver, page 3-42](#).



Note For better security, Cisco recommends administrators use SNMP V3 and define ACLs to limit SNMP write access to the switch.

To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

- SNMP v1 (SNMP community string is “cam_v1”):

```
(config)# snmp-server host 172.16.1.61 traps version 1 cam_v1 udp-port 162
mac-notification snmp
```

- SNMP V2c (SNMP community string is “cam_v2”):

```
(config)# snmp-server host 172.16.1.61 traps version 2c cam_v2 udp-port 162
mac-notification snmp
```

- The following commands should be run in the order of: group, user, and host.

For auth (SNMP username/password is “cam_user”/“cam_auth”)

```
(config)# snmp-server group cam_group v3 auth read vldefault write vldefault notify
vldefault
(config)# snmp-server user cam_user cam_group v3 auth md5 cam_auth
(config)# snmp-server host 172.16.1.61 traps version 3 auth cam_user udp-port 162
mac-notification snmp
```

For priv (SNMP username/password is “cam_user”/“cam_priv”)

```
(config)# snmp-server group cam_group v3 priv read vldefault write vldefault notify
vldefault
(config)# snmp-server user cam_user cam_group v3 auth md5 cam_auth priv des cam_priv
(config)# snmp-server host 172.16.1.61 traps version 3 priv cam_user udp-port 162
mac-notification snmp
```

- Step 10** Enable the Port Fast command to bring a port more quickly to a Spanning Tree Protocol (STP) forwarding state. You can do this at the switch configuration level for all interfaces, or at the interface configuration level for each interface:

- Switch configuration level:

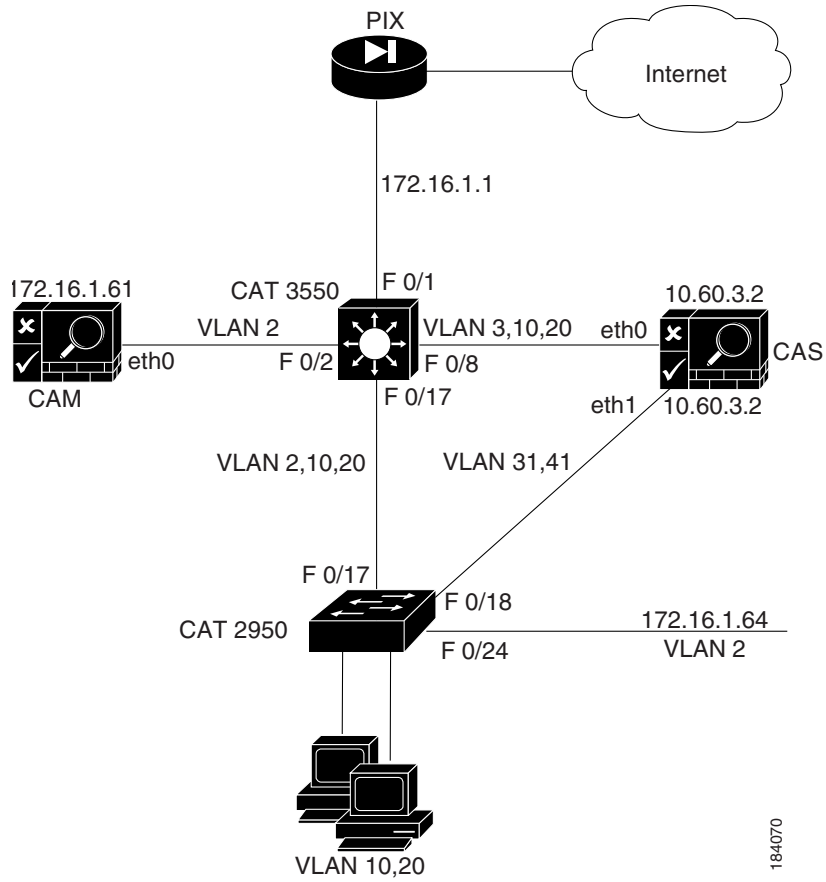
```
(config)# spanning-tree portfast default
```

- Interface configuration level:

```
(config-if)# spanning-tree portfast
```

Figure 3-5 illustrates an example OOB setup.

Figure 3-5 Example Physical Setup



Note

The CAS interfaces should be on a separate VLAN from the CAM VLAN and access VLANs.

Figure 3-6 Example L3 Switch Configuration

```

!To PIX
interface FastEthernet0/1
switchport access vlan 2
switchport mode access
! To Manager
interface FastEthernet0/2
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/8
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 3,10,20
switchport mode trunk
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/17
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2,10,20
switchport mode trunk
!
interface VLAN1
ip address 192.168.1.61 255.255.255.0
shutdown
!
interface VLAN2
ip address 172.16.1.60 255.255.255.0
!
interface VLAN3
ip address 10.60.3.1 255.255.255.0
!
interface VLAN10
ip address 10.60.10.1 255.255.255.0
!
interface VLAN20
ip address 10.60.20.1 255.255.255.0
!!
ip default-gateway 172.16.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
ip http server
!

```

Note: No int vlan 31 or 41

184141

OoB Network Setup/Configuration Worksheet

Table 3-2 summarizes information needed to configure switches and the Clean Access Manager.

Table 3-2 Configuration Worksheet

Configuration Settings	Value
Switch Configuration	
Switch IP Address:	
Access VLANs:	
Auth VLANs:	
location_string:	
admin_contact_info:	
SNMP version used:	
SNMP (V1/V2c) read community string:	
SNMP (V1/V2c) write community string:	
SNMP (V3) auth method/ username/password:	
MAC notification or linkup:	
SNMP Trap V1/V2c community string, or SNMP Trap V3 auth method/usr/pwd (to send traps to CAM):	
CAM/CAS Configuration	
CAM IP address:	
CAS Trusted IP address:	
CAS Untrusted IP address:	
CAM VLAN (management):	
CAS VLAN (management):	
CAM SNMP Trap Receiver:	
Community string for SNMP Trap V1 switches:	
Community string for SNMP Trap V2c switches:	
Auth method/username/password for SNMP Trap V3 switches:	

Configure OOB Switch Management on the CAM

This section describes the web admin console configuration steps to implement out-of-band. In general, you first configure Group, Switch, and Port profiles, as well as the Clean Access Manager's SNMP Receiver settings, under **OOB Management > Profiles**. After profiles are configured, add the switches you want to control to the Clean Access Manager's domain under **OOB Management > Devices**, and apply the profiles to the switches.

After switches are added, the ports on the switch are discovered, and the **Port** and **Config** buttons and pages for each switch appear on **OOB Management > Devices > Devices > List**.

Clicking the manage **Ports** button brings up the **Ports** tab. The **Ports** page is where you apply a managed Port Profile to a specific port(s) to configure how a client's traffic is temporarily routed through the CAS for authentication/certification before being allowed on the trusted network.

The configuration sequence is as follows:

1. Plan your settings and configure the switches to be managed, as described in previous section, [Configure Your Switches, page 3-15](#)
2. [Add Out-of-Band Clean Access Servers and Configure Environment, page 3-22](#)
3. [Configure Global Device Filters to Ignore IP Phone MAC Addresses, page 3-25](#)
4. [Configure Group Profiles, page 3-25](#)
5. [Configure Switch Profiles, page 3-27](#)
6. [Configure Port Profiles, page 3-30](#)
7. [Configure VLAN Profiles, page 3-37](#)
8. [Configure SNMP Receiver, page 3-42](#)
9. [Add and Manage Switches, page 3-45](#)
10. [Manage Switch Ports, page 3-50](#)

Add Out-of-Band Clean Access Servers and Configure Environment



Note

In order to establish the initial secure communication channel between a CAM and CAS, you must import the root certificate from each appliance into the other appliance's trusted store so that the CAM can trust the CAS's certificate and vice-versa.

Almost all the CAM/CAS configuration for Out-of-Band deployment is done directly in the **OOB Management** module of the web admin console. Apart from the **OOB Management** module configuration, OOB setup is almost exactly the same as traditional in-band setup, except for the following differences:

-
- Step 1** Choose an Out-of-Band gateway type when you add your Clean Access Server(s) ([Figure 3-7](#)).

Figure 3-7 Add New OOB Server

The out-of-band **Server Types** appear in the dropdown menu to add a new Clean Access Server:

- Out-of-Band Virtual Gateway
- Out-of-Band Real-IP Gateway

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



Note

- For Virtual Gateway (In-Band or OOB), do not connect the untrusted interface (eth1) of the CAS to the switch until **after** the CAS has been added to the CAM via the web console.
- For Virtual Gateway with VLAN mapping (In-Band or OOB), do not connect the untrusted interface (eth1) of the CAS to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See the [Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7\(5\)](#) for details.

- Step 2** For OOB Virtual Gateways, you must enable and configure VLAN mapping (Figure 3-8) on the CAS for each Auth/Access VLAN pair configured on the switch. This is required in order to retag an unauthenticated client's allowed traffic (e.g. DHCP/DNS) from the Auth VLAN to the Access VLAN (and vice-versa). You can also enable VLAN pruning for CAS appliances operating in Virtual Gateway mode. See the [Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7\(5\)](#) for further details on VLAN mapping and VLAN pruning.

Figure 3-8 Enable VLAN Mapping for Out-of-Band Virtual Gateways

Device Management > Clean Access Servers > 10.201.241.32

Managed Subnet · **VLAN Mapping** · NAT · 1:1 NAT · Static Routes · ARP · Proxy

VLAN Packet Handling

Enable VLAN Pruning

When enabled along with VLAN Mapping, disallows any VLAN Packet to pass through to other interface in either direction if VLAN mapping cannot be done for the packet. If enabled alone, discards all VLAN packets from passing through in either direction.

Enable VLAN Mapping

VLAN Mapping Assignments

Untrusted network VLAN ID: (-1 for non-VLAN)

Trusted network VLAN ID: (-1 for non-VLAN)

Description:

Untrusted VLAN ID	Trusted VLAN ID	Description	Del
10	100	student	✗
20	200	staff	✗

- Step 3** If you plan to use role-based port profiles (see [Configure Port Profiles, page 3-30](#)), specify the Access VLAN in the **Out-of-Band User Role VLAN** field when you create a new user role ([Figure 3-9](#)). See [Add New Role, page 6-7](#) for details.

Figure 3-9 Configure User Role with Access VLAN

User Management > User Roles

List of Roles | Edit Role | Traffic Control | Bandwidth | Schedule

Disable this role

Role Name:

Role Description:

Role Type:

*VPN Policy:

*Dynamic IPsec Key: Enable Disable

*Max Sessions per User Account (Case-Insensitive): (1 - 255; 0 for unlimited)

Rate of Trusted-side Egress Traffic with VLAN (In-Band): (0 - 4095, or leave it blank)

*Out-of-Band User Role VLAN:

Add Access VLAN here to use role-based port profiles

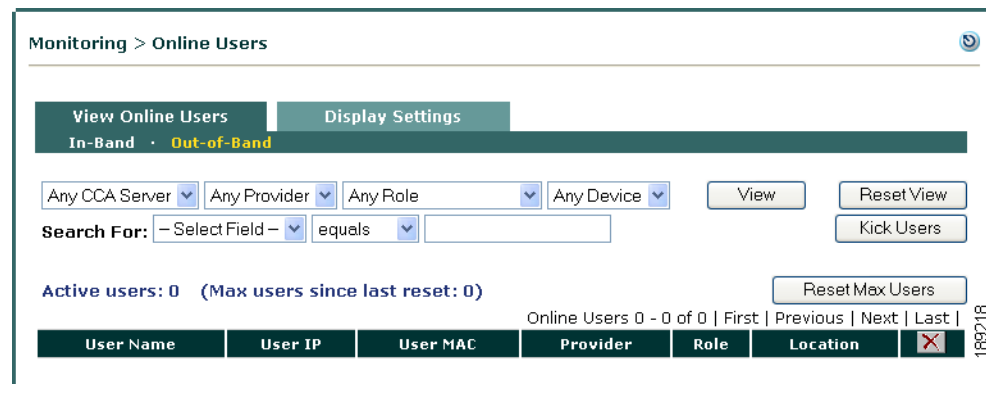
Role Name	Role Description	Role Type	*VPN Policy	*Dynamic IPsec Key	*Max Sessions per User Account	*Out-of-Band User Role VLAN
Role for unauthenticated users	Role for unauthenticated users	deny	deny			
Role for users to download requirements	Role for users to download requirements	deny	deny			
Role for quarantined users	Role for quarantined users	deny	deny			
Role1	Agent Role	deny	deny			3
Role2	network scanning role	deny	deny			
Role3	Agent & network scanning	deny	deny			

**Note**

You can specify a VLAN Name or VLAN ID in the Port Profile or for the Out-of-Band User Role VLAN. You can specify only numbers for VLAN ID. VLAN Name is case-sensitive, but you can specify wildcards for a VLAN Name. The switch will use the first match for the wildcard VLAN Name.

- Step 4** When out-of-band is enabled, the **Monitoring > View Online Users** page displays links for both **In-Band** and **Out-of-Band** users and display settings (Figure 3-10). See [Out-of-Band Users, page 11-21](#) for details.

Figure 3-10 View Out-of-Band Online Users



Configure Global Device Filters to Ignore IP Phone MAC Addresses

An important feature of any OOB configuration is to ensure IP phones through which client machines connect to the network do not inadvertently terminate the client connection when MAC notification events from the IP phone initiate a change in the network connection like a VLAN change. To do this:

- Configure a global Device Filter (**Device Management > Filters > Devices > New** or **Edit**) with the “Ignore” option for the IP phone MAC address to ensure Cisco NAC Appliance ignores SNMP trap events from the IP phone
- Enable the **Change VLAN according to global device filter list** option when you configure the Port Profile, as described in [Add Port Profile, page 3-31](#).

For more information, see [Device Filters for Out-of-Band Deployment Using IP Phones, page 2-15](#). For detailed configuration instructions, see [Add Global Device Filter, page 2-19](#).

Configure Group Profiles

When you first add a switch to the Clean Access Manager’s domain (under **OOB Management > Devices**), a Group profile must be applied to add the new switch. There is a predefined Group profile called **default**, shown in [Figure 3-11](#). All switches are automatically put in the **default** group when you add them. You can leave this default Group profile setting, or you can create additional Group profiles as needed. If you are adding and managing a large number of switches, creating multiple Group profiles allow you to filter which sets of devices to display from the list of switches (under **OOB Management > Devices > Devices > List**).

Figure 3-11 Group Profiles List

OOB Management > Profiles

Group	Device	Port	VLAN	SNMP Receiver
List · New				
Group Name	Description	Devices	Edit	Delete
group1	test			
default	Default Group			

189219

Add Group Profile

- Step 1** Go to **OOB Management > Profiles > Group > New** (Figure 3-12).

Figure 3-12 New Group

OOB Management > Profiles

Group · Device · Port · VLAN · SNMP Receiver

List · New

Group Name

Description

Add

189220

- Step 2** Enter a single word for the **Group Name**. You can use digits and underscores, but no spaces.
- Step 3** Enter an optional **Description**.
- Step 4** Click **Add**. The new Group profile appears under **OOB Management > Profiles > Group > List**.

Edit Group Profile

- Step 1** To edit the profile later, after actual switches are added, go to **OOB Management > Profiles > Group > List** and click the **Edit** button for the new Group profile.
- Step 2** The **Edit** page appears (Figure 3-13).

Figure 3-13 Edit Group

Step 3 You can toggle the switches that belong in the Group profile by selecting the IP address of the switch from the **Member Switches** or **Available Switches** columns and clicking the **Join** or **Remove** buttons as applicable.

Step 4 Click the **Update** button when done to save your changes.



Note To delete a group profile, you must first remove the joined switches from the profile.

Configure Switch Profiles



Note Before you configure the CAM to manage switches in your network, Cisco recommends updating the switch OIDs on the CAM via the **Device Management > Clean Access > Updates > Update** web console page to ensure you have the most up-to-date switch support available.

A Switch profile must first be created under **OOB Management > Profiles > Device > New**, then applied when a new switch is added. A Switch profile classifies switches of the same model and SNMP settings, as shown in [Figure 3-14](#). The Switch profile configures how the CAM will read/write/change port settings, such as Access/Auth VLAN, on a switch of this particular type.

Figure 3-14 Switch Profiles List

Group	Device	Port	VLAN	SNMP Receiver		
List · New						
Profile Name	Device Model	SNMP Port	Description	Devices	Edit	Delete
c2960	Cisco Catalyst 2960 series	161	c2960			
c3750	Cisco Catalyst 3750 series	161	c3750			
L3c2960	Cisco Catalyst 2960 series	161	L3 C2960			
wlc2100	Cisco Wireless LAN Controllers	161	wlc2100			
wlc4400	Cisco Wireless LAN Controllers	161	wlc4400			

The Switch profiles list under **OOB Management > Profiles > Device > List** provides three buttons:

- **Devices**—Clicking this button brings up the list of added switches and WLCs under **OOB Management > Devices > Devices > List** (see [Figure 3-28](#)).
- **Edit**—Clicking this button brings up the **Edit Switch profile** form (see [Figure 3-16](#)).
- **Delete**—Clicking this icon deletes the Switch profile (a confirmation dialog will appear first).

Add Switch Profile

Use the following steps to add a Switch profile.

- Step 1** Go to **OOB Management > Profiles > Device > New** ([Figure 3-15](#)).

Figure 3-15 New Switch Profile

OOB Management > Profiles

Group Device Port VLAN SNMP Receiver

List · New

(These settings must match the device setup to ensure that the Clean Access Manager can read/write to the device correctly)

Profile Name

Device Model

SNMP Port

Description

SNMP Read Settings

SNMP Version

Community String

SNMP Write Settings

SNMP Version

Community String

- Step 2** Enter a single word for the **Profile Name**. You can use digits and underscores but no spaces.

**Note**

It is a good idea to enter a Switch Profile name that identifies the switch model and SNMP read and write versions, for example “2950v2v3.”

- Step 3** Choose the **Device Model** for the profile from the dropdown menu.
- Step 4** Enter the **SNMP Port** configured on the switch to send/receive traps. The default port is 161.
- Step 5** Enter an optional **Description**.
- Step 6** Configure **SNMP Read Settings** to match those on the switch.
- Choose the **SNMP Version**: SNMP V1 or SNMP V2C.
 - Type the **Community String** configured for the switch.
- Step 7** Configure **SNMP Write Settings** to match those on the switch.
- Choose the **SNMP Version**: SNMP V1, SNMP V2C, or SNMP V3.
 - Type the **Community String** for SNMP V1 or SNMP V2C configured for the switch.
- Step 8** If SNMP v3 is used for SNMP write settings on the switch, configure the following settings to match those on the switch:
- Choose a **Security Method** from the dropdown menu: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES-CBC), or AuthPriv(SHA+DES-CBC).
 - Type the **User Name**.
 - Type the **User Auth**.
 - Type the **User Priv**.
- Step 9** Click **Add** to add the Switch profile to **OOB Management > Profiles > Device > List** (Figure 3-28). Figure 3-16 illustrates a switch profile defining Cisco Catalyst 2950 switches with the same SNMP settings: SNMP V2c with read community string “c2950_read” and write community string “c2950_write.”

Figure 3-16 Example Switch Profile

OOB Management > Profiles

Group Device Port VLAN SNMP Receiver

List · New

(These settings must match the device setup to ensure that the Clean Access Manager can read/write to the device correctly)

Profile Name

Device Model

SNMP Port

Description

SNMP Read Settings

SNMP Version

Community String

SNMP Write Settings

SNMP Version

Community String

188224

Configure Port Profiles

The Port profile determines whether a port is managed or unmanaged, the Authentication and Access VLANs to use when switching the client port, and other behavior for the port (see [Ports Management Page, page 3-51](#)). There are four types of port profiles for switch ports (shown in [Figure 3-17](#)):

- Unmanaged – For uncontrolled switch ports that are not connected to clients (such as printers, servers, switches, etc.). This is typically the default Port profile.
- Managed with Auth VLAN/Default Access VLAN – Controls client ports using the Auth VLAN and Default Access VLAN defined in the Port profile.
- Managed with Auth VLAN/User Role VLAN – Controls client ports using the Auth VLAN defined in the Port profile and the Access VLAN defined in the user role (see [Figure 3-9 on page 3-24](#)).
- Managed with Auth VLAN/ Initial Port VLAN– Controls client ports using the Auth VLAN defined in the Port profile and the Access VLAN defined as the initial port VLAN of the switch port.

Regular switch ports that are not connected to clients use the unmanaged Port profile. Client-connected switch ports use managed Port profiles. When a client connects to a managed port, the port is set to the authentication VLAN. After the client is authenticated and certified, the port is set to the access VLAN specified in the Port profile (Default Access VLAN, or User Role VLAN, or Initial Port VLAN).

In OOB Real-IP gateway mode, the CAM enables port bouncing to help clients acquire a new IP address after successful authentication and certification. In OOB Virtual Gateway mode, port bouncing is not necessary as the client uses the same IP address after successful authentication and certification.

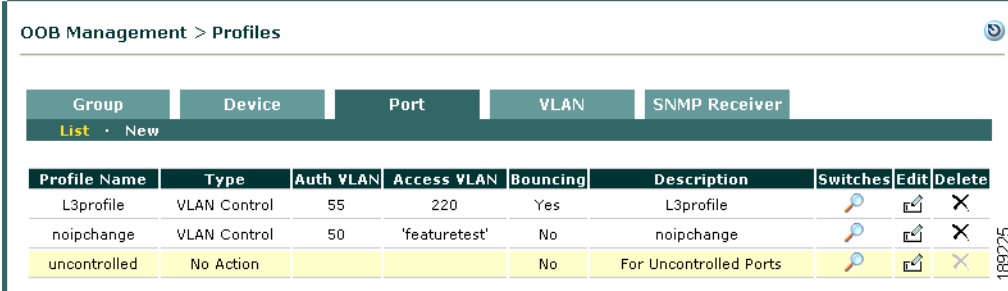


Note

If the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to “kick” the user out, for example) and the switch changes the VLAN assignment for the client’s access port from the Access VLAN back to the Authentication VLAN, the client machine

discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see [Configure Access to Authentication VLAN Change Detection](#), page 3-65.

Figure 3-17 Port Profiles List



Profile Name	Type	Auth VLAN	Access VLAN	Bouncing	Description	Switches	Edit	Delete
L3profile	VLAN Control	55	220	Yes	L3profile			
noipchange	VLAN Control	50	'featuretest'	No	noipchange			
uncontrolled	No Action			No	For Uncontrolled Ports			



Note

The Policy Sync feature allows OOB Port Profiles and VLAN Profiles to be exported from a Master CAM to Receiver CAMs. Refer to [Policy Import/Export](#), page 14-29 for details.

Add Port Profile

You will need to add a Port profile for each set of Auth/Access VLANs you configure on the switch.



Note

For OOB Virtual Gateways, you must enable and configure VLAN mapping on the CAS for each Auth/Access VLAN pair configured on the switch. See [Figure 3-8 on page 3-24](#) for more details.

Step 1 Go to **OOB Management > Profiles > Port > New** ([Figure 3-18](#))

Figure 3-18 New Port Profile

OOB Management > Profiles

Group Device Port VLAN SNMP Receiver

List · New

Profile Name

Description

Manage this port by

VLAN Settings

Supported VLAN Name format: `abc`, `*abc`, `abc*`, `*abc*`. The switch will use the first match for wildcard VLAN Name.

Auth VLAN

Default Access VLAN

Access VLAN

VLAN Profile

Options: Device Connected to Port

The CAM discovers the device connected to the switch port when it receives SNMP mac-notification or linkup traps for the device. The CAM then instructs the switch to assign the **Auth VLAN** to the port if the device is not certified, or **Access VLAN** if the device is certified and user is authenticated. You can additionally configure the following options:

Change VLAN according to global device filter list (device must be in list).
When set, the VLAN of the port will be assigned by global device filter settings (ALLOW=Default Access VLAN, DENY=Auth VLAN, ROLE/CHECK=User Role VLAN, IGNORE=ignore SNMP traps from managed switches (IP Phones)).

Change to if the device is certified but not in the out-of-band user list.
Select the VLAN to assign when device is certified and user is reconnecting to network.

Bounce the port after VLAN is changed.
Check this box to help clients update their IP settings for Real-IP/NAT Gateways. You can leave this field unchecked for Virtual Gateways.

Bounce the port based on role settings after VLAN is changed.

Generate event logs when there are multiple MAC addresses detected on the same switch port.

Options: Device Disconnected from Port

The device is considered disconnected after: SNMP linkdown trap received or admin removal of user. Additional configuration options are:

Remove out-of-band online user when SNMP linkdown trap is received, and then .
Ensure Access VLAN client is removed from OOB online user list if disconnecting/reconnecting to same port.

Remove other out-of-band online users on the switch port when a new user is detected on the same port.
Ensure only one valid user is allowed on one switch port at the same time.

Remove out-of-band online user without bouncing the port.
This prevents port bouncing for IP phone connected users.

189226

Step 2 Type a single word for the **Profile Name**. You can use digits and underscores, but no spaces. The name should reflect whether the Port profile is managed or unmanaged.



Note

In addition to providing a Port Profile name that reflects whether the port to which this profile is applied is managed or unmanaged, Cisco recommends you also provide information about the nature of the port profile if the purpose is to ensure reliable client machine connection through a network IP phone.

Step 3 Type an optional **Description** for the Port profile.

Step 4 Click the checkbox for **Manage this port** to enable configuration of this Port Profile. This enables the port management options on the page.

Step 5 For **Auth VLAN**, choose either **VLAN ID** (default) or **VLAN Name** from the dropdown menu and type the corresponding authentication/quarantine VLAN ID or name to be used for this port profile:

- If choosing **VLAN ID**—you can specify only numbers in the text field.
- If choosing **VLAN Name**—the text field is case-sensitive. You can specify wildcards for the VLAN name, such as: `abc`, `*abc`, `abc*`, or `*abc*`. The switch will use the first match for the wildcard VLAN name. You can also use special characters in the name.

- Step 6** For **Default Access VLAN**, choose either **VLAN ID** (default) or **VLAN Name** from the dropdown and type the corresponding VLAN ID or name to be used as the default access VLAN for this port profile.
- If choosing **VLAN ID**—you can specify only numbers in the text field.
 - If choosing **VLAN Name**—the text field is case-sensitive. You can specify wildcards for the VLAN name, such as: abc, *abc, abc*, or *abc*. The switch will use the first match for the wildcard VLAN name. You can also use special characters in the name.



Note If the switch cannot find the VLAN specified (e.g. VLAN Name is mistyped), the error will appear on the perfigo.log (not the Event Log).

- Step 7** For **Access VLAN**, choose one of the following options from the dropdown menu:
- **Default Access VLAN**—The CAM will put authenticated users with certified devices on the Default Access VLAN specified in the Port Profile.
 - **User Role VLAN**—The CAM will put authenticated users with certified devices on the Access VLAN specified in the User Role (for details, see [Figure 3-9: Configure User Role with Access VLAN](#) and [Out-of-Band User Role VLAN](#), page 6-10).
 - **Initial Port VLAN**—The CAM will put authenticated users with certified devices on the **Initial VLAN** specified for the port in the **Ports** configuration page (see [Ports Management Page](#), page 3-51 for details). The initial VLAN is the value saved by the CAM for the port when the switch is added. Instead of using a specified Access VLAN, the client is switched from the initial port VLAN to an Auth VLAN for authentication and certification, then switched back to the initial port VLAN when the client is certified.
- Step 8** If you want to specify the Access VLAN using a VLAN profile definition, choose one of the **VLAN Profile** names you created in [Add VLAN Profile](#), page 3-39 or choose **Default** from the dropdown menu to specify the VLAN profile to associate with this port profile.



Note If you choose Default, or if you have not yet created any custom VLAN profiles, the CAM queries only the managed switch in question for the VLAN name-to-VLAN ID mapping to determine the user's Access VLAN.

Port Profile Options when Device is Connected to Port

The CAM discovers the device connected to the switch port from SNMP MAC change notification/MAC move notification or linkup traps received. The port is assigned the **Auth VLAN** if the device is not certified, or **Access VLAN** if the device is certified and user is authenticated. You can additionally configure the following options:

Step 9 **Change VLAN according to global device filter list**

Click this option if you have configured a global Device Filter to ignore MAC addresses for IP phones in your network or if you want to use the CAM's global Device Filter rules to set the VLAN of the port. You must have device filters added under **Device Management > Filters > Devices** for this feature to work. For OOB, the device filter rules are as follows:

- **ALLOW**—bypass login and posture assessment (certification) and assign **Default Access VLAN** to the port
- **DENY**—bypass login and posture assessment (certification) and assign **Auth VLAN** to the port
- **ROLE**—bypass login and L2 posture assessment (certification) and assign **User Role VLAN** to the port (see [Out-of-Band User Role VLAN](#), page 6-10)

- **CHECK**—bypass login, apply posture assessment, and assign **User Role VLAN** to the port (see [Out-of-Band User Role VLAN, page 6-10](#))
- **IGNORE**—ignore SNMP traps from managed switches (IP Phones)



Note Rules configured for MAC addresses on the global Device Filter list have the highest priority for user/device processing in both OOB and IB deployments. See [Device Filters for Out-of-Band Deployment, page 2-14](#) for further details.

For more information on In-Band vs. Out-of-Band client machine behavior based on specified Device Filter type, see [In-Band and Out-of-Band Device Filter Behavior Comparison, page 2-15](#).

Step 10 Change to [Auth VLAN | Access VLAN] if the device is certified, but not in the out-of-band user list

This option is automatically enabled when a port is managed. Choose which VLAN to use when the device is certified and the user is reconnecting to the port:

- **Default Auth VLAN**—Force Access VLAN clients on this port to re-authenticate on the Authentication VLAN the next time they connect to the network.
- **Default Access VLAN**—Allow clients to stay on the trusted network without having to login again the next time they connect to the network.

Step 11 Bounce the port after VLAN is changed

- For Real-IP gateways, check this box to prompt the client to get a new IP address once switched to the Access VLAN.
- For Virtual gateways, leave this box unchecked.



Note If using a version 4.1.2.0 or later Windows Agent, ActiveX Control, or Java Applet to refresh client DHCP IP addresses, the **Bounce the switch port after VLAN is changed** option in the Port profile can be left disabled. Refer to [DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6](#), [Configure Access to Authentication VLAN Change Detection, page 3-65](#), and see [Advanced Settings, page 3-43](#) for additional details on configuring DHCP Release, VLAN Change, and DHCP Renew delays.

Step 12 Bounce the port based on role settings after VLAN is changed

When you enable this option, the switch defers to the associated user role to determine port bouncing and/or IP address refresh/renew behavior when the VLAN of the port through which the user is accessing the network switches from the authentication to the access VLAN. Both of the user role options are on the **User Management > User Roles > New Role** page



Note If you enable the **Bounce the port after VLAN is changed** option in step 11 above, this option is inaccessible.

Step 13 Generate event logs when there are multiple MAC addresses detected on the same switch port

You can check this box to generate event logs when multiple MAC addresses are found on the same switch port.

Port Profile Options when Device is Disconnected from Port

A device is considered disconnected after one of the following events occurs:

- User disconnects from network and CAM receives SNMP linkdown trap
- Administrator removes user from OOB users list

Figure 3-19 Options: Device Disconnected from Port

Options: Device Disconnected from Port

The device is considered disconnected after: SNMP linkdown trap received or admin removal of user. Additional configuration options are:

Remove out-of-band online user when SNMP linkdown trap is received, and then change to Restricted VLAN: ▾

VLAN ID do nothing.

Ensure Access VLAN client is removed from OOB online user list if disconnecting/reconnecting. change to Auth VLAN.

Remove other out-of-band online users on the switch port when a new user is detected on the same port. change to Restricted VLAN:

Ensure only one valid user is allowed on one switch port at the same time.

Remove out-of-band online user without bouncing the port.

This prevents port bouncing for IP phone connected users.

Add

188917

To remove OOB users from the OOB Online Users list and determine VLAN assignments for switch ports where client machines have disconnected from the network, you can configure the following options:

Step 14 Remove out-of-band online user when SNMP linkdown trap is received, and then [do nothing | change to Auth VLAN | change to Restricted VLAN]

Click this option to specify which VLAN the CAM assigns to a switch port after receiving a linkdown trap from the switch when a client disconnects from the Cisco NAC Appliance network. (See [Advanced, page 3-61](#) for details on linkdown traps.)

- If this option is checked and specifies to **do nothing**, when the client disconnects (causing a linkdown trap to be sent), the switch port remains on the last VLAN assigned, or re-assigned to the VLAN specified in the **Change to [Auth VLAN | Access VLAN] if the device is certified, but not in the out-of-band user list** option.



Note If the client is not on the Certified Devices List, the client is put on the Authentication VLAN.

- If this option is checked and specifies to **change to Auth VLAN**, the CAM puts the switch port on the Authentication VLAN after receiving a linkdown SNMP trap regardless of whether or not the client is on the Certified Devices List.
- If this option is checked and specifies to **change to Restricted VLAN**, the CAM either assigns the switch port to a previously-configured **VLAN Name** (see [Configure VLAN Profiles, page 3-37](#) for more details), or to a specific **VLAN ID** number you enter in the text field that appears under this setting. As with the **change to Auth VLAN** option, this VLAN assignment takes place when the CAM receives a linkdown trap regardless of whether or not the client is on the Certified Devices List.

Step 15 Remove other out-of-band online users on the switch port when a new user is detected on the same port

This feature enables administrators to remove other online out-of-band users on the switch port when a new user is detected on the same port. It also allows for the modification of the port profile if an existing user is seen on a different switchport.

Checking this option ensures that only one valid user is allowed on one switch port at the same time. If an online user (e.g. "user1") is currently on a switch port (e.g. "fa0/1" on switch "c2950") and this option is enabled for the Port Profile applied to that port, "user1" will be removed if another user (e.g. "user2") signs in from the same switch port or moves to this port from another location.



Note Online user is an endpoint or a PC connected to the switch port. If another user logs in to the same PC with different credentials, it is not detected as a different user, as the endpoint is identified only by the MAC Address and not by the login credentials.

Step 16 Remove out-of-band online user without bouncing the port

When any user is removed from the OOB Online User list, the port is changed from the Access VLAN to the Authentication VLAN. Also note that users removed from the Certified Device list are also always removed from the Online User list (IB or OOB). If the **Remove out-of-band online user without bouncing the port** option is checked, the port will not be bounced when a user is removed from the OOB Online User list. If this option is not checked, the port will be bounced when a user is removed from the OOB Online User list.

This option is intended to prevent bouncing the switch port to which a client machine is connected through a IP phone. The feature allows Cisco NAC Appliance to authenticate/assess/quarantine/remediate a client machine (laptop/desktop) without affecting the operation of a IP phone connected to the switch port. When this option is checked for OOB Virtual Gateways, the client port will not be bounced when:

- Users are removed from the Out-of-Band Online Users List, or
- Devices are removed from the Certified Devices list

Instead, the port Access VLAN will be changed to the Auth VLAN.

Step 17 Click **Add** to add the port profile to the **OOB Management > Profiles > Port > List**.

See [Manage Switch Ports, page 3-50](#) for further details on Port profiles and the **Ports** config page.

See [Interpreting Event Logs, page 13-4](#) for further details on monitoring online users.

Configure VLAN Profiles

You can use VLAN profiles on your Cisco NAC Appliance to resolve VLAN name-to-VLAN ID mappings while simultaneously ensuring uniform L3 OOB support for multiple access points on your network. VLAN profiles work in conjunction with port profiles to specify the Access VLAN for a user session based on a set of VLAN name-to-VLAN ID mappings. If you have a single access point for remote users on your network, VLAN profiles likely serve very little purpose. If, however, your network includes two, three, or even dozens of different access points, VLAN profiles can help you dynamically assign Access VLAN IDs for remote users based on a “user friendly” VLAN name assignment associated with the user’s profile configured on the system.

When a remote user accesses the network for authentication, the Cisco NAC Appliance assigns the user session to an Authentication VLAN before granting network access. Once the user is authenticated, the CAM instructs the access switch (the switch through which the user is accessing the network) to assign a VLAN ID to the managed port, based on Default Access VLAN, User Role VLAN, or Initial Port VLAN definitions.

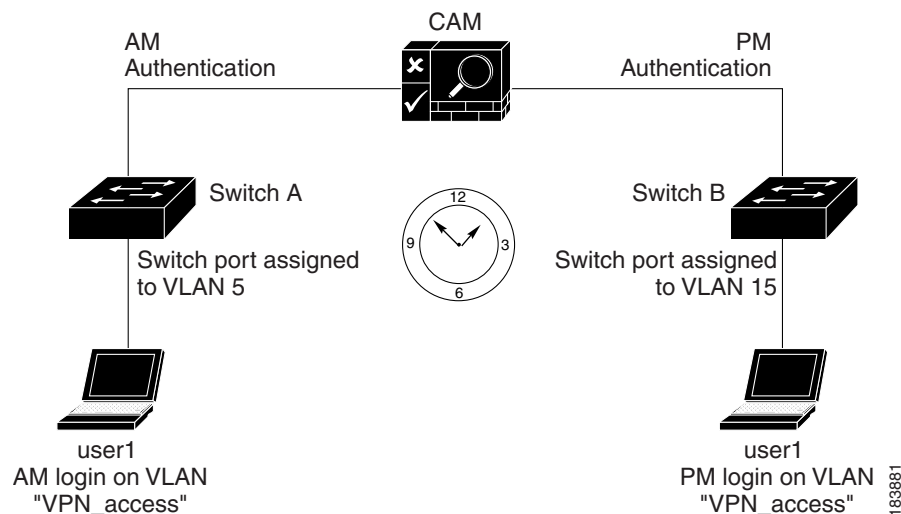
There are two methods to determine VLAN name-to-VLAN ID mapping criteria:

- Querying local (CAM) VLAN profiles
- Querying the VLAN name-to-VLAN ID maps on the access switch, itself

You can configure the CAM to query only the local database, only the switch database, or both sources in the order you specify. When a user logs in to the network from a given access point and has been authenticated, they may be assigned one VLAN ID for one switch and a different VLAN ID for another.

Figure 3-20 provides an example of this feature in a remote-access scenario.

Figure 3-20 VLAN Profile Feature Example



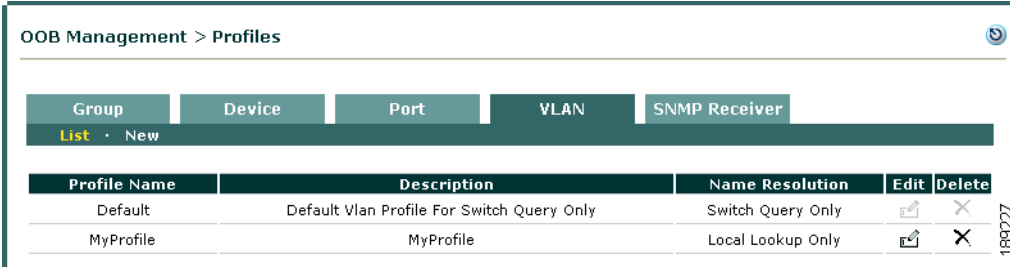
1. In the morning, user1 attempts to remotely access the network and his session arrives via switch A. Switch A allows the user authentication-level access and user1 passes authentication credentials on to the CAM.
2. Upon receiving the authentication request, the CAM discovers the Access VLAN for user1’s session is defined in the associated user role, which specifies a VLAN name “VPN_access.”
3. The CAM queries VLAN profile assignments for the VLAN ID corresponding to “VPN_access” and discovers a VLAN profile associated with the port profile for Switch A indicating VLAN 5.

4. User1 is authenticated and the CAM instructs switch A to assign VLAN 5 to the managed port.
5. User1 achieves VPN access to the internal network.
6. Later in the day, while visiting a client, user1 again attempts to access the network, but this time user1's session arrives at access switch B.
7. As with switch A earlier that day, switch B allows the user authentication-level access and user1 passes authentication credentials on to the CAM, where the same user role association specifies that the Access VLAN for user1's session should be the VLAN name "VPN_access."
8. The CAM queries VLAN profile assignments for the VLAN ID corresponding to "VPN_access" and, because switch B employs a different VLAN ID assignment model addressed in the relevant CAM switch profile mappings, the CAM discovers a VLAN profile associated with the port profile for Switch B indicating VLAN 15.
9. The CAM instructs switch B to assign VLAN 15 to the managed switch port and grant VPN access to user1.

As this example demonstrates, the VLAN access name is the same for both sessions, but two separate VLAN profiles on the CAM ensure user1 receives the same level of authentication from both access points on the network.

Figure 3-21 illustrates the VLAN Profiles List page.

Figure 3-21 VLAN Profiles



Group	Device	Port	VLAN	SNMP Receiver
List	New			
Profile Name	Description	Name Resolution	Edit	Delete
Default	Default Vlan Profile For Switch Query Only	Switch Query Only		
MyProfile	MyProfile	Local Lookup Only		



Note

The Policy Sync feature allows OOB Port Profiles and VLAN Profiles to be exported from a Master CAM to Receiver CAMs. Refer to [Policy Import/Export, page 14-29](#) for details.

Add VLAN Profile

To create a new VLAN profile:

- Step 1** Go to **OOB Management > Profiles > VLAN > New** (Figure 3-22).

Figure 3-22 New VLAN Profile

OOB Management > Profiles

Group Device Port **VLAN** SNMP Receiver

List · New

Profile Name

Description

VLAN Name Resolution Local Lookup Only

VLAN Name Mapping
Only Alphanumerics and _ allowed in VLAN Name.

VLAN Name

VLAN ID

Add

189228

- Step 2** Specify a unique **Profile Name** for the new VLAN profile.
- Step 3** Type an optional **Description** for the VLAN profile.
- Step 4** Choose a **VLAN Name Resolution** method from the dropdown list:
- **Local Lookup Only**—Instructs the CAM to resolve the specified VLAN name using only local mappings as the possible resolved values. If you select this option, the CAM will not attempt to resolve the VLAN name using any data available on the access switch.
 - **Switch Query Preferred**—Instructs the CAM to resolve the specified VLAN name by first searching data available from the access switch, *then* (if not found) attempting to resolve the name in the VLAN Name-to-ID mappings found in the VLAN profile.
 - **Local Lookup Preferred**—Instructs the CAM to resolve the specified VLAN name by first searching name in the VLAN Name-to-ID mappings found in the VLAN profile, *then* (if not found) attempting to resolve the name by searching data available from the access switch.
- Step 5** Enter the **VLAN Name** for the access VLAN (the assigned “common” name of the VLAN users can access the network) the CAM uses to grant access to the remote user. This function allows you to use VLAN names instead of specific VLAN numbers to identify the VLAN ID the CAM should instruct the access switch(es) to assign to the port over which the user accesses the network. Since the user may access the network from one of several access switches residing at different network access points, the VLAN name-to-VLAN ID mapping function enables you to associate a specific VLAN name with a user or group profile and grant access over a broad range of access devices all around the network, based on a single VLAN profile definition.
- Step 6** Enter the **VLAN ID** for the VLAN policy. This is the actual VLAN number the CAS tells the switch to assign to the remote user’s switch port once the user logs in and has been “cleared” to access the internal network. Because VLAN IDs from different switches may be (and probably are) different, you can grant access to a user or group profile based on the VLAN name-to-VLAN ID mapping defined on the CAM and/or the access switch, itself.

Step 7 Click **Add**.

Edit VLAN Profile

To edit an existing VLAN profile:

Step 1 Go to **OOB Management > Profiles > VLAN > List** (Figure 3-23).

Figure 3-23 VLAN Profiles

Profile Name	Description	Name Resolution	Edit	Delete
Default	Default Vlan Profile For Switch Query Only	Switch Query Only		
MyProfile	MyProfile	Local Lookup Only		

Step 2 Click the **Edit** icon for the existing VLAN profile you want to update.

The Edit VLAN Profile window (Figure 3-24) appears.

Figure 3-24 Edit VLAN Profile

VLAN Name	VLAN ID	Edit	Delete
featuretest	544		
restrictedvlan	555		

VLAN Name	VLAN ID	Map
<input type="text"/>	-1	<input type="button" value="Map"/>

Step 3 Enter a new **Profile Name**, **Description**, and/or specify a different **VLAN Name Resolution** lookup method for the VLAN profile and click **Update**.

Step 4 To update VLAN name-to-VLAN ID mappings:

- a. If you want to add a new VLAN name-to-VLAN ID mapping, specify the additional **VLAN Name** and **VLAN ID** under Add a New VLAN Name Mapping and click **Map**.

- b. If you want to reassign one or more VLAN name-to-VLAN ID mappings, click the **Edit** icon corresponding to the mapping you want to update, specify a new **VLAN ID** under Edit VLAN Name Mapping, and click **Update**. (See [Figure 3-25](#).)

Figure 3-25 Edit VLAN Name Mapping—VLAN ID

The screenshot shows the 'OOB Management > Profiles' configuration page. At the top, there are tabs for 'Group', 'Device', 'Port', 'VLAN', and 'SNMP Receiver'. Below the tabs is a navigation bar with 'List', 'New', 'Edit', and 'Map' options. The main content area shows the profile details for 'MyProfile' with a description of 'MyProfile'. Below this is the 'Edit VLAN Name Mapping' section, which includes a table with the following data:

VLAN Name	VLAN ID
restrictedvlan	555

Below the table is an 'Update' button. On the right side of the page, there is a vertical text label '1899230'.

Configure SNMP Receiver

The **SNMP Receiver** form configures how the SNMP Receiver running on the Clean Access Manager receives and responds to SNMP trap notifications from all managed switches when MAC change notification/MAC move notification or linkup/linkdown user events occur (such as when a user plugs into the network). The configuration on the switch must match the CAM's SNMP Receiver configuration in order for the switch to send traps to the CAM.

Cisco NAC Appliance also provides support for SHA-1 and 3DES encryption, which is required when configuring SNMP management on a CAM operating in a FIPS 140-2 compliant network.

SNMP Trap

This page configures settings for the SNMP traps the CAM receives from all switches. The Clean Access Manager SNMP Receiver can support simultaneous use of different versions of SNMP (V1, V2c, V3) when controlling groups of switches in which individual switches may be using different versions of SNMP.

Step 1 Go to **OOB Management > Profiles > SNMP Receiver > SNMP Trap** (Figure 3-26).

Figure 3-26 CAM SNMP Receiver

Step 2 Use the default **Trap Port on Clean Access Manager** (162) or enter a new port number here.

Step 3 For **SNMP V1 Settings**, type the **Community String** used on switches using SNMP V1.

Step 4 For **SNMP V2c Settings**, type the **Community String** used on switches using SNMP V2c.

Step 5 For **SNMP V3 Settings**, configure the following fields used on switches using SNMP V3:

- Specify the SNMP V3 authentication and privacy combination using the **Security Method (Auth/Priv)** dropdown menus:
 - NoAuth, MD5 (non-FIPS only), SHA-1
 - NoPriv, DES (non-FIPS only), 3DES



Note If you are specifying an authentication/privacy combination for a FIPS 140-2 compliant CAM, the only settings available are the SHA-1 authentication and 3DES privacy types.

- Type the **User Name**.
- Type the **User Auth**.
- Type the **User Priv**

Step 6 Click **Update** to save settings.

Advanced Settings

This page configures advanced timeout and delay settings for the SNMP traps received and sent by the Clean Access Manager (CAM). To change the default settings, use the following steps. You can use the page to fine-tune settings from their defaults once switches are added and configured.

To Change Default SNMP

Step 1 Go to **OOB Management > Profiles > SNMP Receiver > Advanced Settings** (Figure 3-27).

Figure 3-27 *SNMP Receiver > Advanced Settings*

OOB Management > Profiles

Group Device Port VLAN SNMP Receiver

SNMP Trap · **Advanced Settings**

MAC-NOTIFICATION Trap Timeout seconds
(Period after which received traps are dropped. If set to zero, traps are never dropped)

Linkup Trap Bounce Timeout seconds
(Period after which to bounce the port to generate new trap if MAC address query failed)

Linkup Trap Retry Query Interval seconds
(Delay before retrying MAC address query)

Port-Security Delay seconds
(Delay before setting port-security information on the switch)

DHCP Release Delay seconds
(Delay between user login and DHCP release)

VLAN Change Delay seconds
(Delay between user login and VLAN Change)

Port Bounce Interval seconds
(Delay between port-off and port-on)

DHCP Renew Delay seconds
(Delay between DHCP release and DHCP renew)

Redirection Delay without Bouncing seconds
(Delay between vlan change and webpage redirection for ports without bouncing option checked)

Redirection Delay with Bouncing seconds
(Delay between port bouncing and webpage redirection for ports with bouncing option checked)

SNMP Timeout seconds
(Timeout value for SNMP requests from CAM to managed devices)

189232

Step 2 Configure optional Advanced Settings as follows:

- **MAC-NOTIFICATION Trap Timeout** (default is 60 seconds)—The CAM timestamps the MAC change notification/MAC move notification traps it receives, and examines the timestamp when the trap is processed. If the time difference between the timestamp and the current time is greater than the **MAC-NOTIFICATION Trap Timeout**, the trap is dropped. This configuration field ensures the CAM only processes timely traps.
- **Linkup Trap Bounce Timeout** (default is 180 seconds)—When the CAM receives a linkup trap, it tries to resolve the MAC address connected to the port. The MAC address may not be available at that time. If the CAM cannot get the MAC address, it makes another attempt after the number of seconds specified in the **Linkup Trap Retry Query Interval** field. In order to keep the port controlled and limit the number of times the CAM tries to resolve the MAC address, the CAM bounces the port after the number of seconds specified in the **Linkup Trap Bounce Timeout** to force the switch to generate a new linkup trap.
- **Linkup Trap Retry Query Interval** (default is 4 seconds)—When the CAM receives a linkup trap, it needs to query the switch for the MAC address connected to the port. If the MAC address is not yet available, the CAM waits the number of seconds specified in the **Linkup Trap Retry Query Interval** field, then tries again.
- **Port-Security Delay** (default is 3 seconds)—If port-security is enabled on the switch, after the VLAN is switched, the CAM must wait the number of seconds specified in the **Port-Security Delay** field before setting the port-security information on the switch.



Note

To refresh the DHCP IP address, typically the Agent or ActiveX/Java Applet performs a DHCP release before the VLAN change, followed by a DHCP renew after the VLAN change. The delays to perform DHCP Release, VLAN Change, DHCP Renew are configurable. See [DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6](#) for additional details. See also [Configure Access to Authentication VLAN Change Detection, page 3-65](#) if you are using DHCP release/renew instead of port bouncing.

- **DHCP Release Delay** (default is 1 second)—This field configures the delay between user login and DHCP release.
- **VLAN Change Delay** (default is 2 seconds)—This field configures the delay between user login and VLAN Change. This value should be greater than the **DHCP Release Delay**.



Note

The **VLAN Change Delay** setting should be greater than the **DHCP Release Delay**, but less than the combined duration of the **DHCP Release Delay** and **DHCP Renew Delay**. This is to ensure that DHCP release happens before VLAN change and DHCP renew happens after VLAN change.

- **Port Bounce Interval** (default is 5 seconds)—The **Port Bounce Interval** is the time delay between turning off and turning on the port. This delay is inserted to help client machines issue DHCP requests.
- **DHCP Renew Delay** (default is 3 seconds)—This field configures the delay between DHCP release and DHCP renew. This value should be greater than the **VLAN Change Delay** minus the **DHCP Release Delay**.
- **Redirection Delay without Bouncing** (default is 1 second)—This field configures the delay between VLAN change and webpage redirection (after client posture assessment) for ports with no port bouncing in the Port Profile. This allows you to minimize redirection time if no port bouncing

is required. When the Port Profile does not require bouncing the port after the VLAN is changed (e.g. Virtual Gateway), configuring this option will redirect the user page after the number of seconds specified here (e.g. 1 second).

When the port is not bounced, the total redirection interval that the user experiences is the value of the **Redirection Delay without Bouncing** field.

**Note**

When the user continues to be redirected to the login page after login/posture assessment, this typically means the web page redirection is occurring before the switch is able to change the VLAN of the port (from Auth to Access). In this case, increase the Redirection Delay to 2 or 3 seconds to resolve this issue.

- **Redirection Delay with Bouncing** (default is 15 seconds)—This field configures the delay between port bouncing and webpage redirection (after client posture assessment) for ports with the **Bounce the port after VLAN is changed** option checked on the Port Profile. This allows you to configure the time needed for port bouncing.

When the port is bounced, the total redirection interval that the user experiences is the sum of 2 fields: **Redirection Delay with Bouncing** and **Port Bounce Interval**.

If the Port Profile requires bouncing the port after the VLAN is changed, then after user login, the user will see “Renewing IP address” page after the sum of the number of seconds specified in this field and the number of seconds specified in the **Port Bounce Interval**. For example:

Port Bounce (5 seconds) + Redirection Delay (15 seconds) = Redirection interval (20 seconds total)

- **SNMP Timeout** (default is 5 seconds)—This field enables you to specify the SNMP timeout value (in seconds) for SNMP trap message response from a managed switch that saves its current (running) configuration when instructed by the Clean Access Manager.

Step 3 Click **Update** to save settings.

Add and Manage Switches

The pages under the **OOB Management > Devices > Devices** tab are used to discover and add new managed switches within an IP range, add new managed switches by exact IP address, and manage the list of controlled switches. There are two methods to add new managed switches

- [Add New Switch, page 3-46](#)
- [Search New Switches, page 3-47](#)

Figure 3-28 List of Switches

The screenshot shows the 'OOB Management > Devices' page. At the top, there are tabs for 'Devices' and 'Discovered Clients'. Below the tabs are filters: 'Device Group' (set to ALL), 'Device Profile' (set to ALL), 'Device IP' (empty), and 'Port Profile' (set to ALL). A table lists the devices with columns for IP, MAC, Model, Description, Profile, Config, Ports, and Delete. The table contains five entries: three switches and two WLCs. Each row has icons for Profile, Config, and Ports. A vertical ID '189233' is on the right side of the table.

IP	MAC	Model	Description	Profile	Config	Ports	Delete
10.201.220.2	00:17:0E:8C:F1:C5	Switch	L3 2960	L3c2960			
10.201.220.20	00:19:E7:15:41:C5	Switch	c3750	c3750			
10.201.220.51	00:17:0E:D2:2F:C4	Switch	c2960	c2960			
10.201.220.102	00:1E:13:2A:65:C3	WLC	wlc4400	wlc4400			
10.201.220.103	00:1D:45:ED:D9:80	WLC	wlc2100	wlc2100			

The list of switches under **OOB Management > Devices > Devices > List** displays all switches and WLCs added from the **New** or **Search** forms. Switch entries in the list include the switch’s IP address, MAC address, Description, and Switch Profile. You can sort the entries on the list by **Device Group**, **Device Profile**, or **Port Profile** dropdowns, or you can simply type a **Device IP** and hit Enter to search for a switch or WLC by its address. Additionally the List provides one control and three buttons:

- **Profile**—Clicking the **Profile** link brings up the Switch Profile (Figure 3-15).
- **Config**—Clicking the **Config** button brings up the **Config Tab**, page 3-60 for the switch.
- **Ports**—Clicking the **Ports** button brings up the **Ports Management Page**, page 3-51 for the switch.



Note WLC device profiles do not use Port Profile configurations. Therefore, the **Ports** icon remains “grayed out” for any WLC entries in the table.

- **Delete**—Clicking the **Delete** button deletes the switch from the list (a confirmation dialog will appear first).



Note

When adding a switch based on its loopback address, the **OOB Management > Devices > Devices List** will display a MAC address of 00:00:00:00:00:00 for the switch. This is expected behavior; the MAC address displayed on this interface is for information only and does affect OOB functionality.

Add New Switch

The **New** page allows you to add switches when exact IP addresses are already known.

- Step 1** Go to **OOB Management > Devices > Devices > New** (Figure 3-29).

Figure 3-29 Add New Switch

- Step 2** Choose the **Device Profile** from the dropdown menu to apply to the switches or WLCs to be added.
- Step 3** Choose the **Device Group** for the switches or WLCs from the dropdown menu.
- Step 4** Choose the **Default Port Profile** from the dropdown menu. Typically, the default port profile should be uncontrolled.
- Step 5** Type the **IP Addresses** of the switch(es) you want to add. Separate each IP address by line.
- Step 6** Enter an optional **Description** of the new switch.
- Step 7** Click the **Add** button to add the switch or WLC.
- Step 8** Click the **Reset** button to reset the form.

Search New Switches

The **Search** page allows you to discover and add unmanaged switches within an IP range.

- Step 1** Go to **OOB Management > Devices > Devices > Search** (Figure 3-30).

Figure 3-30 Search Switches

OOB Management > Devices

Devices | Discovered Clients

List · New · Search

Device Profile: c2950v2v2

IP Range: 10.201.3.14 - 10.201.3.20

Don't list devices already in the database Search

Add selected devices into database with the following device group and port profile:

Device Group: default

Default Port Profile: uncontrolled Commit

<input type="checkbox"/>	IP Address	MAC Address	Contact	Location
<input type="checkbox"/>	10.201.3.15	00:12:43:3C:60:00		Rack 1 @ LAB
<input type="checkbox"/>	10.201.3.16	00:0E:83:A5:16:00		Rack 1 @ LAB

189235

- Step 2** Select a **Device Profile** from the dropdown list. The read community string of the selected Device Profile is used to find switches with matching read settings.
- Step 3** Type an **IP Range** in the text box. Note that the maximum IP range is 256 for a search.
- Step 4** By default, the **Don't list devices already in the database** checkbox is already checked. If you uncheck this box, the resulting search will include switches and WLCs you have already added. Note, however, that the Commit checkboxes to the left of each entry will be disabled for switches that are already managed.
- Step 5** Choose a **Device Group** from the dropdown to apply to the unmanaged devices found in the search.
- Step 6** Choose a **Default Port Profile** from the dropdown to apply to the unmanaged devices found in the search.
- Step 7** Click the **checkbox** to the left of each unmanaged device you want to manage through the CAM. Alternatively, click the checkbox at the top of the column to add *all* unmanaged devices found from the search.

**Note**

While all switches matching the read community string of the Switch Profile used for the search are listed, only those switches matching the *read* SNMP version and community string can be added using the **Commit** button. A switch cannot be controlled unless its *write* SNMP settings match those configured for its Switch Profile in the Clean Access Manager.

- Step 8** Click the **Commit** button to add the new switches. These switches are listed under **OOB Management > Devices > Devices > List**.

Discovered Clients

Figure 3-31 shows the **OOB Management > Devices > Discovered Clients > Wired Clients** page. The Wired Clients page lists all clients discovered by the Clean Access Manager via SNMP MAC change notification/MAC move notification and linkup/linkdown traps. The page records the activities of out-of-band clients (regardless of VLAN), based on the SNMP trap information that the Clean Access Manager receives.

When a client connects to a port on the Auth VLAN, a trap is sent and the Clean Access Manager creates an entry on the Wired Clients page. The Clean Access Manager adds a client's MAC address, originating switch IP address, and switch port number to the out-of-band Discovered Clients list. Thereafter, the CAM updates the entry as it receives new SNMP trap information for the client.

Removing an entry from the Wired Clients list clears this status information for the out-of-band client from the CAM.



Note

An entry must exist in the Wired Clients list in order for the CAM to determine the switch port for which to change the VLAN. If the user is logging in at the same time that an entry in the Wired Clients list is deleted, the CAM will not be able to detect the switch port.

Figure 3-31 *Discovered Clients*

OOB Management > Devices

Devices | Discovered Clients

Wired Clients | Wireless Clients

(This page shows all the clients discovered from SNMP traps sent by Cisco Catalyst switches.)

Show clients connected to switch with IP: ALL

Show client with MAC:

Delete All Clients

Delete Selected

Clients/Page: 25

Clients 1-6 of 6 | First | Previous | Next | Last

MAC	IP	Switch	Switch Port	Auth VLAN	Access VLAN	Last Update	
00:14:22:9C:B0:C5	N/A	10.201.220.20	10010	50	N/A	2008-09-17 11:30:09.955	<input type="checkbox"/>
00:14:38:EB:B8:D3	N/A	10.201.220.51	10111	50	N/A	2008-09-17 12:40:05.361	<input type="checkbox"/>
00:14:6A:12:DA:66	N/A	10.201.220.20	10010	N/A	N/A	2008-09-17 11:30:10.085	<input type="checkbox"/>
00:14:6A:33:47:4E	N/A	10.201.220.20	10002	50	N/A	2008-09-12 10:55:05.042	<input type="checkbox"/>
00:14:BF:5A:A7:A1	10.201.244.234	10.201.220.2	10038	55	220	2008-09-15 11:01:06.051	<input type="checkbox"/>
00:15:60:A3:6A:B1	N/A	10.201.220.51	10108	50	N/A	2008-09-17 13:22:48.747	<input type="checkbox"/>

Elements of the page are as follows:

- **Show clients connected to switch with IP**—Leave the default of ALL switches displayed, or choose a specific switch from the dropdown menu. The dropdown menu displays all managed switches in the system.
- **Show client with MAC**—Type a specific MAC address and press Enter to display a particular client.
- **Clients/Page**—Leave the default of 25 entries displayed per page, or choose from the dropdown menu to displays 50, 100, 200, or ALL entries on the page.
- **Delete All Clients**—This button removes all clients on the list.
- **Delete Selected**—This button only removes the clients selected in the check column to the far right of the page.

- Note that you can click any of the following column headings to sort results by that column:
 - **MAC**—MAC address of discovered client
 - **IP**—IP address of the client
 - **Switch**—IP of the originating managed switch. Clicking the IP address brings up the **OOB Management > Devices > Switch [IP] > Config > Basic** page for the switch.
 - **Switch Port**—Switch port of the client. Clicking the port number brings up the **OOB Management > Devices > Switch [IP] > Ports** configuration page for the switch.
 - **Auth VLAN**—Authentication (quarantine) VLAN
A value of “N/A” in this column indicates that either the port is unmanaged or the VLAN ID for this MAC address is unavailable from the switch.
 - **Access VLAN**—Access VLAN of the client.
A value of “N/A” in this column indicates the Access VLAN ID is unavailable for the client. For example, if the user is switched to the Auth VLAN but has never successfully logged into Cisco NAC Appliance (due to wrong user credentials), this machine will never have been to the Access VLAN.
 - **Last Update**—The last time the CAM updated the information of the entry.

See [Out-of-Band Users, page 3-66](#) for additional details on monitoring out-of-band users.

Manage Switch Ports

Once a switch is added, the **Ports** and **Config** tabs/pages only appear after a switch is added to the **OOB Management > Devices > Devices > List**.

The Ports page is the central point of management for the ports on a switch. You can apply Port profiles to individual or multiple ports, change VLAN settings, bounce ports, and apply all changes to the switch configuration.

Switch ports that are not connected to clients typically use the unmanaged port profile. Switch ports connected to clients use managed port profiles. After switch ports are configured and the settings are saved by clicking the “**Update**” button, the switch ports need to be initialized by clicking the “**Setup**” button when the switch supports MAC notification.

Cisco NAC Appliance provides OOB support for Cisco IP Phone deployments where the port is a trunk port and the native VLAN is the data VLAN. The CAM can manage switch trunk ports in addition to switch access ports.



Note

Because Cisco NAC Appliance can control switch trunk ports for OOB (starting from release 3.6(1)+), make sure the uplink ports for managed switches are configured as “uncontrolled” ports after upgrade. This can be done in one of two ways:

- Before upgrading, change the **Default Port Profile** for the entire switch to “uncontrolled” under **OOB Management > Devices > Devices > List > Config[Switch_IP] > Default Port Profile | uncontrolled**
- After upgrading, change the **Profile** to “uncontrolled” for the applicable uplink ports of the switch under **OOB Management > Devices > Devices > List > Ports [Switch_IP] | Profile**

This prevents unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile.

Ports Management Page

The **Ports** management page populates information for all Ethernet ports on a switch (see [Figure 3-32](#) and [Figure 3-33](#)) according to the information the Clean Access Manager receives from direct SNMP queries. For example, if a switch added to the CAM has 24 Fast Ethernet ports and 2 Gigabit Ethernet uplinks, the **Ports** tab will display 26 rows, with one entry per port. Trunk ports configured on the switch are distinguished by blue background on the **Ports** page, and VLAN values for these ports refer to the trunk port native VLAN.

If the switch does not support MAC change notification/MAC move notification traps, the **Setup** button (**Set up mac-notification on managed switch ports**) and **MAC Notif.** column are not displayed on the page. In this case, linkup/linkdown traps must be supported and configured on the switch and Clean Access Manager. See [Manage Individual Ports \(Linkup/Linkdown\)](#), page 3-58 for the Ports management page controls for linkup/linkdown only ports.

Manage Individual Ports (MAC Notification)

This section describes the method you use to manage and/or assign a port profile to an individual switch port. This method works well for a small number of ports, but if you want to assign the same port profile to a large number of ports all at the same time, see [Assign a Port Profile to Multiple Ports Simultaneously](#), page 3-59.

Figure 3-32 Ports Tab

OOB Management > Devices > Switch[192.168.40.2]

Config Ports

List Manage

For trunk ports (blue background), the VLAN value refers to trunk native VLAN. For Private VLAN ports (green background), the VLAN value refers to private secondary VLAN.

Update Refresh << Simple

3 4

Set the initial VLANs for the ports to the current VLAN settings of the switch: Reset All Set New Ports

Set up mac-notification on managed switch ports: Setup

Save the switch running configuration into non-volatile memory: Save

5 6

Search For: -- Select Field -- starts with Unmanage All Show

1

Ports/Page: 12 Ports 1-12 of 28 | First | Previous | Next | Last

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	MAC Notif.	Client MAC	Profile	Note
Gi1/0/1	10101	GigabitEthernet1/0/1	●	10/100	15	27	X	🔍	Default [uncontrolled]	
Gi1/0/2	10102	GigabitEthernet1/0/2	●	10/100	1	1	X	🔍	Default [uncontrolled]	
Gi1/0/3	10103	GigabitEthernet1/0/3	●	10/100	5	5	X	🔍	Default [uncontrolled]	
Gi1/0/4	10104	GigabitEthernet1/0/4	●	10/100	1	1	X	🔍	Default [uncontrolled]	
Gi1/0/5	10105	GigabitEthernet1/0/5	●	10/100	1	30	X	🔍	Default [uncontrolled]	
Gi1/0/6	10106	GigabitEthernet1/0/6	●	10/100	1	1	X	🔍	Default [uncontrolled]	
Gi1/0/7	10107	GigabitEthernet1/0/7	●	10/100	150	150	X	🔍	Default [uncontrolled]	
Gi1/0/8	10108	GigabitEthernet1/0/8	●	10/100	1	1	X	🔍	Default [uncontrolled]	
Gi1/0/9	10109	GigabitEthernet1/0/9	●	10/100	1	1	X	🔍	Default [uncontrolled]	
Gi1/0/10	10110	GigabitEthernet1/0/10	●	10/100	1	1	X	🔍	Default [uncontrolled]	
Gi1/0/11	10111	GigabitEthernet1/0/11	●	10/100	14	14	X	🔍	Default [uncontrolled]	
Gi1/0/12	10112	GigabitEthernet1/0/12	●	10/100	15	15	X	🔍	Default [uncontrolled]	

2

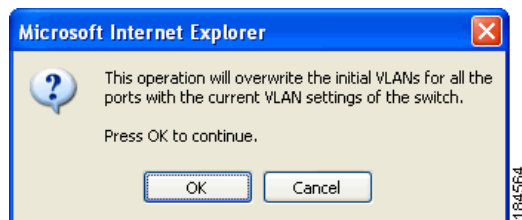
246923

After adding a new switch, set up the **Ports** configuration page (Figure 3-32) for the switch ports as follows:

- Step 1** If you want to limit the switch profiles displayed in the Ports list, specify search criteria and click **Show** (•[Show \(1\)](#), page 3-54).
- Step 2** Choose the **Profile** (•[Profile \(2\)](#), page 3-56) to use for the port, either managed or unmanaged.
- Step 3** Click **Update** (•[Update \(3\)](#), page 3-54) to save the Port Profile for the port to the CAM.
- Step 4** Click **Advanced/Simple** toggle button to reveal the advanced port assignment features available for the switch ports.
- Step 5** Click **Setup** (•[Setup button \(MAC notification switches only\) \(5\)](#), page 3-53) to initialize MAC change notification/MAC move notification on switch ports (if available on the switch).
- Step 6** Click **Unmanage All** to change all the managed ports to default port profile that was setup for the switch.
- Step 7** Click **Save** (•[Save \(6\)](#), page 3-53) to save the switch running configuration to the switch stored (startup) configuration.

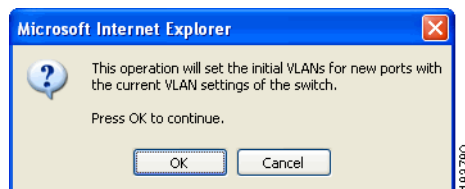
- **Reset All** (Initial VLAN Port Profiles only)

Clicking **Reset All** copies the switch's **Current VLAN** values (•[Current VLAN](#), page 3-55) for all ports and sets these as the **Initial VLAN** settings (for access ports) and trunk native VLAN settings (for trunk ports) (•[Initial VLAN \(Initial VLAN Port Profiles only\)](#), page 3-55) on the CAM and on the running configuration of the switch. This button allows you to change the Initial VLAN for all ports at the same time on the switch. Click **OK** in the confirmation to reset the values:



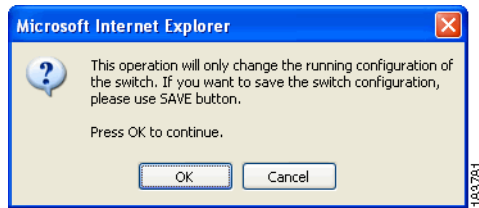
- **Set New Ports** (Initial VLAN Port Profiles only)

Clicking **Set New Ports** (Figure 3-32) preserves settings for existing ports, but copies the switch's **Current VLAN** values for new ports and sets these as **Initial VLAN** settings (for access ports) and trunk native VLAN settings (for trunk ports) on the CAM and on the switch running configuration. This is useful when new ports are added to a switch, such as when adding a new blade in a Catalyst 4500 series rack. In this case, when the new ports are added, the **Initial VLAN** column displays "N/A." Clicking **Set New Ports** copies the values from Current VLAN column to the Initial VLAN column for all "N/A" ports and sets these values on the CAM and switch. The Initial VLAN values for existing ports on the switch (i.e. not "N/A") will not change. Click **OK** in the confirmation to set the new values.



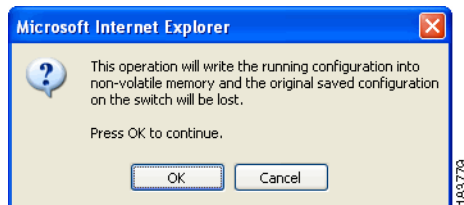
- **Setup** button (MAC notification switches only) (5)

For switches that support MAC change notification/MAC move notification traps, click the **Setup** button after updating the CAM to set up MAC notification on managed switch ports and save the running configuration of the switch. Click **OK** to initialize ports on the switch.



- **Save (6)**

Click the **Save** button to save the running configuration into non-volatile memory (startup configuration) on the switch. Click **OK** in the confirmation.



Note

The VLAN assignment of the port will not be changed in the startup configuration of the switch unless you click the **Save** button.

- **Update (3)**

After you configure managed ports by choosing the applicable Port Profile, you must click the **Update** button to save these settings on the CAM. Clicking **Update** does the following:

- Saves the Profile for the port to the CAM database.
- Saves any Notes for the port to the CAM database.

If the Port profile is configured with the **Initial Port VLAN** as the Access VLAN and set to “Change to **Access VLAN** if the device is certified and in the out-of-band user list,” clicking **Update** also does the following:

- Saves values in the Initial VLAN column for the port to the CAM database.
- If the Current VLAN value of the port is changed, saves the new VLAN ID for the port to the running configuration of the switch.

- **Show (1)**

To limit the range of switch ports displayed in the **Ports** tab view, you can specify search criteria using the **Search For** filtering functions and specify a text string for which to search. You can specify:

- The information type to search—either the **Port Name** or **Port Description**
- The information qualifier—select from **equals**, **starts with**, **ends with**, or **contains**
- The test string defining the search (like “/11” in our example below)

Once you have specified the search criteria, click **Show**.

OOB Management > Devices > Switch[192.168.40.2]

Config Ports

List Manage

For trunk ports (blue background), the VLAN value refers to **trunk native VLAN**.
For Private VLAN ports (green background), the VLAN value refers to **private secondary VLAN**.

Update Refresh << Simple

Set the initial VLANs for the ports to the current VLAN settings of the switch: Reset All Set New Ports

Set up mac-notification on managed switch ports: Setup

Save the switch running configuration into non-volatile memory: Save

Search For: -- Select Field -- starts with

Unmanage All Show

Ports/Page: 12 Ports 1-12 of 28 | First | Previous | Next | Last

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	MAC Notif.	Client MAC	Profile	Note
Gi1/0/1	10101	GigabitEthernet1/0/1			15	27	X		Default [uncontrolled]	
Gi1/0/2	10102	GigabitEthernet1/0/2			1	1	X		Default [uncontrolled]	
Gi1/0/3	10103	GigabitEthernet1/0/3			5	5	X		Default [uncontrolled]	

- **Name**

Port name, for example: Fa0/1, Fa0/24, Gi0/1, Gi0/21 (for Cisco switches)

- **Index**

The port number on the switch, for example: 1, 24, 25, 26

- **Description**

Type of port, for example: FastEthernet0/1, FastEthernet0/24, GigabitEthernet0/1, GigabitEthernet0/2

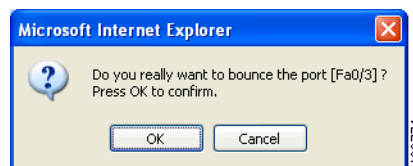
- **Status**

Connection status of the port.

- A green button indicates a device is connected to the port.
- A red button means no device is connected to the port.

- **Bounce**

Clicking this button bounces an initialized, managed port. A confirmation appears before the port is bounced. Note that this feature is only available for managed ports. A port that is connected but not managed cannot be bounced. By default, this feature is disabled for trunk ports.



- **Initial VLAN (Initial VLAN Port Profiles only)**

The Initial VLAN value saved by the CAM for this port. This column is only enabled for managed Port profiles configured with the **Initial Port VLAN** as the Access VLAN and set to “Change to Access VLAN if the device is certified and in the out-of-band user list” (see [Add Port Profile](#), page 3-31). When a switch is added, this column is identical to the Current VLAN column. When new ports are added to a switch, this column displays “N/A” for these ports until the **Set New Ports** button is clicked (• [Set New Ports \(Initial VLAN Port Profiles only\)](#), page 3-53).

To change the Initial VLAN of a port on-the-fly:

- a. Make sure the port's Port profile is configured with the **Initial Port VLAN** as the Access VLAN and set to "Change to Access VLAN if the device is certified and in the out-of-band user list"
- b. Type the modified VLAN for the port in the **Initial VLAN** field.
- c. Click the **Update** button to save the changed configuration on the CAM.

See also: [•Reset All \(Initial VLAN Port Profiles only\)](#), page 3-52, [•Set New Ports \(Initial VLAN Port Profiles only\)](#), page 3-53, and [•Save \(6\)](#), page 3-53.

- **Current VLAN**

The Current VLAN ID assigned to the port. When a new switch is added, the Current VLAN column reflects the VLAN assignments already configured on the switch by the network administrator. Thereafter, the values in this column are dynamic and reflect the current VLAN assignments on the switch (not necessarily the stored VLAN assignment). For trunk ports, the Current VLAN refers to the native VLAN of the trunk port.

To change the Current VLAN assignment for a port on-the-fly:

- a. Type the modified value for the port in the **Current VLAN** field.
- b. Click the **Update** button to save the changed configuration to the CAM and to the running configuration of the switch.
- c. Click the **Save** button to save the switch running configuration to the startup configuration of the switch.

See also [•Reset All \(Initial VLAN Port Profiles only\)](#), page 3-52, [•Set New Ports \(Initial VLAN Port Profiles only\)](#), page 3-53, and [•Save \(6\)](#), page 3-53.

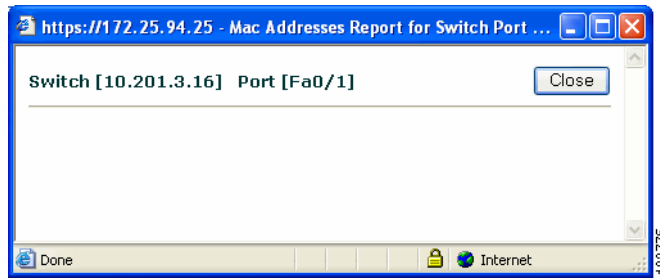
- **MAC Notif.**

MAC notification capability. The presence of this column indicates the switch is using SNMP MAC change notification/MAC move notification traps. If the switch does not support MAC notification traps, or if linkup notification is chosen in the Advanced configuration page (see [Advanced](#), page 3-61), the **MAC Notif.** column and **Setup** button are not displayed on the **Ports** config page. In this case, linkup/linkdown traps must be used.

- A green check in the **MAC Notif.** column means the corresponding port on the switch is enabled for this trap.
- A grey x means the port has not been enabled for this trap, or is not managed.
- A red exclamation point (!) next to either a green check or a grey x means an inconsistency exists between the port configuration on the switch and the port configuration in the Clean Access Manager. Exclamation points will appear after clicking **Update** and before clicking **Setup** to prompt the user to resolve the inconsistencies before attempting to save the settings to the switch.

- **Client MAC**

Clicking this button brings up a dialog with the MAC address of the client attached to this port, the IP address of the switch, and the Name of the port to which the client is connected. For a managed port, only one MAC address displays for the attached client device. For unmanaged ports, this dialog displays all the MAC addresses associated with this port, but will not indicate where the MAC addresses are located (could be on other switches).



Note The MAC address(es) connected to a particular port may not be available when the Access VLAN of the port does not exist in the VLAN database. This occurs on some models of Cisco switches (e.g. 6506, IOS Version 12.2(18) SXD3).

- **Profile (2)**

To control a port from the CAM, select a managed port profile from the dropdown menu, then click **Update** and **Setup**. Apply managed port profiles to ports on which clients are attached in order to get and set the SNMP traps from those ports. Profiles can also be applied to trunk ports. All other ports should be unmanaged. Port Profiles must already be configured under **OOB Management > Profiles > Port > New** (see [Configure Port Profiles, page 3-30](#)). There are always two default dropdown options: uncontrolled, and Default []. All ports are initially assigned the Default[uncontrolled] Port Profile. You can change the Default [] Port Profile assignment from the **OOB Management > Devices > Config** tab.



Note Because Cisco NAC Appliance OOB can control switch trunk ports, when upgrading, make sure uplink ports for managed switches are configured as “uncontrolled” ports. You can do this before upgrade by making sure the Default Port Profile for the entire switch is “uncontrolled” under **OOB Management > Devices > Devices > List > Config[Switch_IP] > Default Port Profile** (see [Config Tab, page 3-60](#)), or, after upgrade, you can change the **Profile** here in the **Ports** config page to “uncontrolled” for the applicable uplink ports of the switch. This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile.

- **Note**

This field allows you enter an optional description for ports you configure. Clicking **Update** saves the note for the port on the CAM.

Manage Individual Ports (Linkup/Linkdown)

If the switch does not support MAC change notification/MAC move notification traps, the **MAC Notif.** column and **Setup** button are not displayed on this page (Figure 3-33). In this case, linkup/linkdown traps must be supported and configured on the switch and Clean Access Manager.

See [Advanced, page 3-61](#) for additional information on the use of linkup/linkdown traps.

Figure 3-33 Ports Tab—Linkup/Linkdown

OOB Management > Devices > Switch[9.9.10.4]

Config Ports

List Manage

For trunk ports (blue background), the VLAN value refers to **trunk native VLAN**.
 For Private VLAN ports (green background), the VLAN value refers to **private secondary VLAN**.

Update Refresh << Simple

Set the initial VLANs for the ports to the current VLAN settings of the switch: Reset All Set New Ports

Save the switch running configuration into non-volatile memory: Save

Search For: -- Select Field -- starts with

Unmanage All Show

Ports/Page: 12 Ports 1-12 of 28 | First | Previous | Next | Last

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	Client MAC	Profile	Note
Gi1/0/1	10101	GigabitEthernet1/0/1	●		90	90		Default [uncontrolled]	
Gi1/0/2	10102	GigabitEthernet1/0/2	●		1	1		Default [uncontrolled]	
Gi1/0/3	10103	GigabitEthernet1/0/3	●		99	99		Default [uncontrolled]	
Gi1/0/4	10104	GigabitEthernet1/0/4	●		1	1		Default [uncontrolled]	
Gi1/0/5	10105	GigabitEthernet1/0/5	●		90	123		Default [uncontrolled]	
Gi1/0/6	10106	GigabitEthernet1/0/6	●		1	1		Default [uncontrolled]	
Gi1/0/7	10107	GigabitEthernet1/0/7	●		99	99		Default [uncontrolled]	
Gi1/0/8	10108	GigabitEthernet1/0/8	●		1	1		Default [uncontrolled]	
Gi1/0/9	10109	GigabitEthernet1/0/9	●		90	90		Default [uncontrolled]	
Gi1/0/10	10110	GigabitEthernet1/0/10	●		20	20		Default [uncontrolled]	
Gi1/0/11	10111	GigabitEthernet1/0/11	●		1	1		Default [uncontrolled]	
Gi1/0/12	10112	GigabitEthernet1/0/12	●		1	1		Default [uncontrolled]	

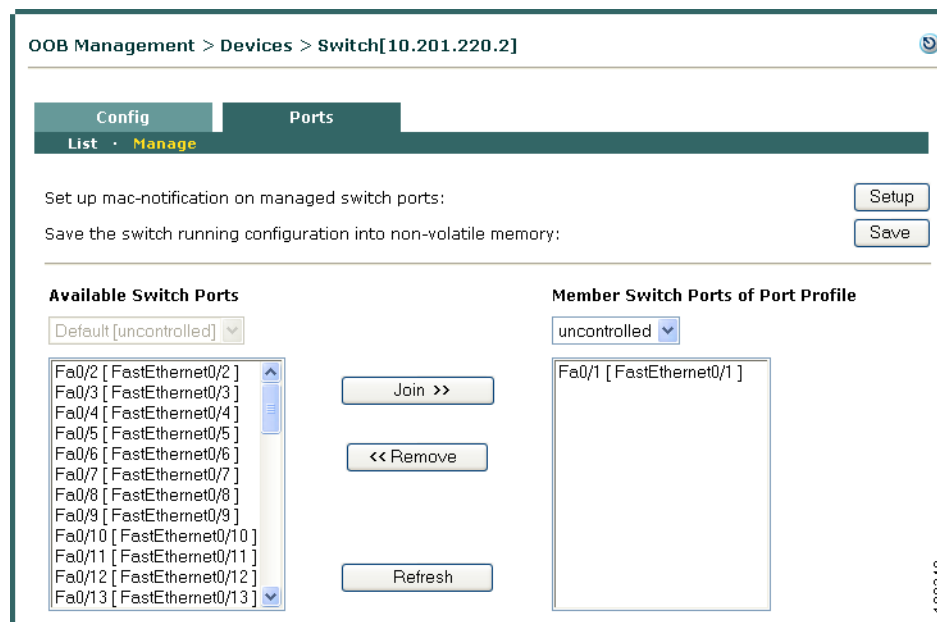
246921

Assign a Port Profile to Multiple Ports Simultaneously

If your switch configuration includes many access ports that all feature the same port profile assignments to provide remote users authentication and access to the network, you can use the **OOB Management > Devices > Switch [x.x.x.x] > Ports > Manage** page to assign the same port profile to many switch ports all at the same time. If you have only a couple or few ports to which you must assign port profiles, see the procedure in [Manage Individual Ports \(MAC Notification\)](#), page 3-51.

Step 1 Go to **OOB Management > Devices > Switch [x.x.x.x] > Ports > Manage** (Figure 3-34).

Figure 3-34 OOB Management > Devices > Switch [x.x.x.x] > Ports > Manage



- Step 2** Select the existing port profile you want to assign to the target switch ports from the **Member Switch Ports of Port Profile** dropdown menu.
- Step 3** Highlight one or more switch ports in the **Available Switch Ports** list to which you want to assign the specified port profile.
- Step 4** Click **Join >>**.
- Step 5** Click **Setup** ([•Setup button \(MAC notification switches only\) \(5\), page 3-53](#)) to initialize MAC change notification/MAC move notification on switch ports (if available on the switch).
- Step 6** Click **Save** ([•Save \(6\), page 3-53](#)) to save the switch running configuration to the switch stored (startup) configuration.

Config Tab

The Config tab allows you to modify Basic, Advanced, and Group profile settings for a particular switch:

- [Basic](#)
- [Advanced](#)
- [Group](#)

Basic

The Basic tab (Figure 3-35) shows the following values configured for the switch.

Figure 3-35 Basic Config

OOB Management > Devices > Switch[10.201.220.2]

Config Ports

Basic · Advanced · Group

IP Address	10.201.220.2
MAC Address	00:17:C5:8C:F1:C8
Location	lab (from device setup)
Contact	(from device setup)
System Info	WS-C2960-48 : Catalyst 2960 48 10/100 ports + 2 dual-purpose GE ports fixed configuration L2 Ethernet switch
Device Profile	L3c2960
Default Port Profile	uncontrolled
Description	L3 2960

Update Reset

189241

- The first values come from the initial configuration done on the switch itself:
 - IP Address
 - MAC Address
 - Location
 - Contact
 - System Info (translated from the MIB for the switch)
- **Device Profile**—Shows the Device Profile you are using for this switch configured under **OOB Management > Profiles > Device**. The Device Profile sets the model type, the SNMP port on which to send SNMP traps, SNMP version for read and write and corresponding community strings, or authentication parameters (SNMP V3 Write).
- **Default Port Profile**—Shows the default Port profile applied to unconfigured ports on the switch on the **Ports** tab. The “uncontrolled” port profile is the initial default profile for all ports, unless you change the setting here. You can change the Default Port Profile by selecting another profile from the dropdown menu and clicking **Update**.

**Note**

Because Cisco NAC Appliance OOB can control switch trunk ports, when upgrading, make sure uplink ports for managed switches are configured as “uncontrolled” ports. You can do this before upgrade by making sure the Default Port Profile for the entire switch is “uncontrolled” here, or, after upgrade you can change the Profile to “uncontrolled” for the applicable uplink ports of the switch under **OOB Management > Devices > Devices > List > Ports [Switch_IP] | Profile** (see [Ports Management Page, page 3-51](#)). This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile

- **Description**—Optional description of the switch. To change this field, type a new description and click **Update**.

Advanced

Use the Advanced Config page ([Figure 3-36](#)) to view or configure which SNMP trap notification type the CAM SNMP Receiver will use for a particular switch.

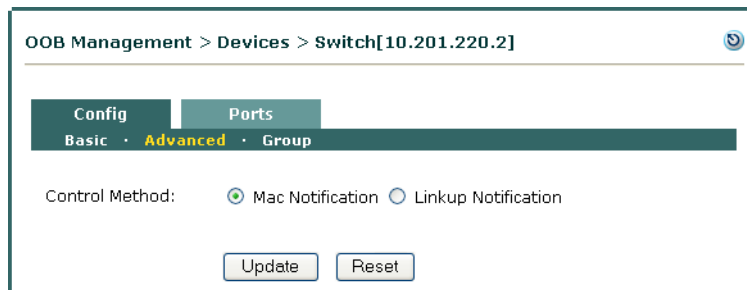
- **MAC Notification**—If a switch supports MAC Notification, the CAM automatically enables this option.

**Note**

To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

- **Linkup Notification**—If a switch does not support MAC Notification, the CAM enables the Linkup Notification option instead. In this case the administrator can optionally enable **Port Security** on the switch if the switch supports this feature. See [Port Security, page 3-62](#) for additional details.
- If a switch supports both **MAC Notification** and **Linkup Notification**, the administrator can optionally disable MAC notification by selecting **Linkup Notification** instead and clicking **Update**.

Figure 3-36 **Advanced Config**



Linkup/linkdown is a global system setting on the switch that tracks whether a connection has non-operating or operating status. With the linkup/linkdown trap method, the Clean Access Manager must poll each port to determine the number of MAC addresses on the port.

Linkdown Traps

A client machine shutdown or reboot triggers a linkdown trap sent from the switch to the CAM (if linkdown traps are set up on the switch and configured on the CAM via the Port profile). Thereafter, the client port behavior depends on the Port profile settings for that specific port.

Whether the SNMP receiver is configured for MAC notification or linkup, the CAM uses the linkdown trap to remove users. For example, the linkdown trap is used if:

- An OOB online user is removed and the Port Profile is configured with the **Kick Out-of-Band online user when linkdown trap is received** option.
- Port Security is enabled on the switch.

Port Security

Port Security is a switch feature that restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.

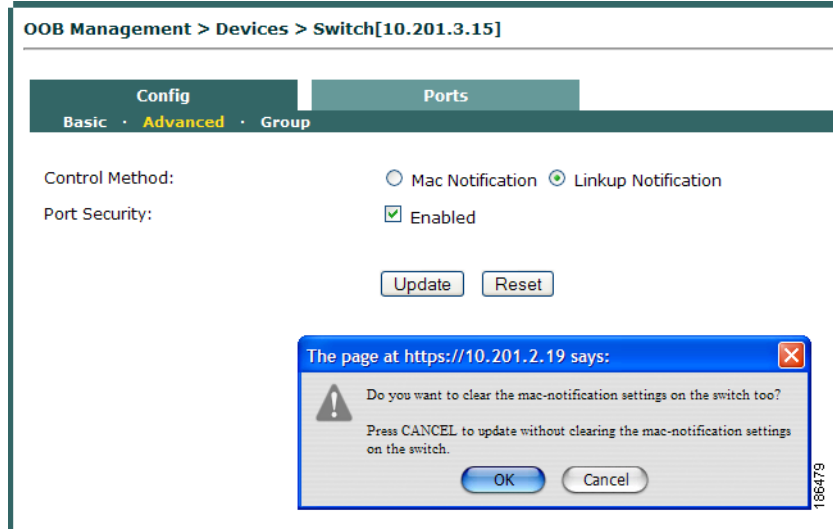
When you change the SNMP control method from **Mac Notification** to **Linkup Notification**, as described in [Enabling Port Security](#), the **Port Security** checkbox will appear on the **Advanced** page ([Figure 3-37](#)) if the switch supports the feature. When using linkup notification, the Port Security feature can provide additional security by causing the port to only allow one MAC address when a user authenticates. So even if the port is connected to a hub, only the first MAC that is authenticated is allowed to send traffic. Note that availability of the Port Security feature is dependent on the switch model and OS being used.

When you enable Port Security on the CAM, the switch configuration is not immediately changed. Instead, when the next client connects to that port, the switch will add the configuration for the port which turns on Port Security for that MAC address. The switch will add that MAC address as the only MAC address allowed to connect to that port if other connection attempts are made.

Enabling Port Security

-
- Step 1** Go to **OOB Management > Devices > List** and click the **Config** button for the switch you want to control.
 - Step 2** From the **Config** tab, click the **Advanced** link.
 - Step 3** Click the option for **Linkup Notification**. A checkbox for **Port Security** appears if the switch supports the feature.
 - Step 4** Click the **Enable** checkbox for **Port Security**.
 - Step 5** Click **Update**.
 - Step 6** A prompt ([Figure 3-37](#)) appears with the following message: “Do you want to clear the mac-notification settings on the switch too? Press CANCEL to update without clearing the mac-notification settings on the switch.”
 - If you click **OK**, the CAM saves the Port Security setting and the “snmp-server enable traps mac-notification” line is removed from the switch configuration.
 - If you click **Cancel**, the CAM saves the Port Security setting and the “snmp-server enable traps mac-notification” line is not removed from the switch configuration. This option can save some time if the administrator is planning to change the port back later to MAC Notification control. See [Re-Enabling MAC Notification](#), page 3-63 for details.)

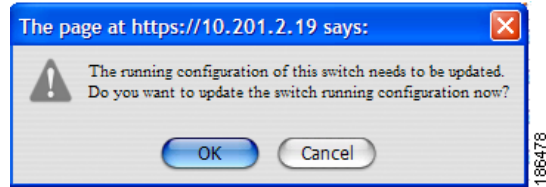
Figure 3-37 Enabling Port Security from the CAM

**Note**

- Port Security can only be enabled on a port set to Access mode (i.e not Trunk mode).
- The MAC address(es) connected to a particular port may not be available after Port Security is enabled. This occurs on some models of Cisco switches (e.g. 4507R, IOS Version 12.2(18) EW).
- If implementing High-Availability, ensure that Port Security is **not** enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.

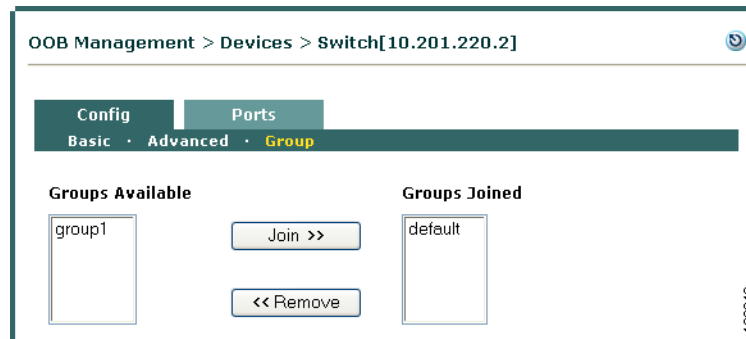
Re-Enabling MAC Notification

- Step 1** Go to **OOB Management > Devices > List** and click the **Config** button for the switch you want to control.
- Step 2** From the **Config** tab, click the **Advanced** link.
- Step 3** Click the option for **Mac Notification**.
- Step 4** Click **Update**.
- Step 5** A prompt (Figure 3-38) displays the following message “The running configuration of this switch needs to be updated. Do you want to update the switch running configuration?”
 - If you click **OK**, the running configuration is updated on the switch.
 - If you click **Cancel**, you will need to reconfigure the controlled ports on the Ports page, as described [Manage Individual Ports \(MAC Notification\)](#), page 3-51.

Figure 3-38 Reverting to MAC Notification from the CAM

Group

This page displays all the Group Profiles configured in the Clean Access Manager, and the Group Profiles to which the switch currently belongs. You can add the switch to other Groups, or you can remove the switch from a Group Joined. To change the Group membership for all switches, go to **OOB Management > Profiles > Group** (see [Configure Group Profiles, page 3-25](#)).

Figure 3-39 Config Group

Configure Access to Authentication VLAN Change Detection



Caution

The Access to Authentication VLAN Change Detection feature should only be used for OOB deployments that require client DHCP IP refresh/renew. DHCP refresh/renew is configured under **Administration > User Pages > Login Page > List > Edit > General | Use web client to release and renew IP address when necessary (OOB)**. If your OOB deployment makes use of port bouncing, this feature is not needed and should not be configured. Refer to [DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6](#) for additional details.

For In-Band clients and Out-of-Band clients which are still assigned to the Authentication VLAN, the Agent uses SWISS discovery packets to verify connectivity with the CAS. Once a client machine is on the out-of-band network and no longer communicates directly with the CAS, additional configuration is required for the client to determine whether it is still on the Access VLAN or moved to the Authentication VLAN. Versions prior to the 4.1.3.0 Agent cannot identify that the client port has switched from the Access VLAN to the Authentication VLAN and require the client machine's DHCP lease to run out in order to force the Agent to perform a DHCP release/renew to get a new IP address assignment.

To ensure OOB users are able to maintain network connection when the Cisco NAC Appliance administrator is forced to “kick” users out (and move the session back to the Authentication VLAN), you can configure the Cisco NAC Appliance system to have the Agent renew the IP address via DHCP release/renew.

This VLAN change detection behavior applies to the following scenarios:

- L3 OOB (Real-IP or Virtual Gateway)
- L2 OOB Real IP Gateway
- L2 OOB Virtual Gateway with user-role based VLAN assignment

If the Agent detects a change, the client machine automatically refreshes its IP address via DHCP release/renew. By default, the Agent automatically polls for the VLAN assignment on the switch every 5 seconds. If you want to increase or decrease that interval, users can adjust the “VlanDetectInterval” client setting.

For OOB deployments that require a client IP change, when the user is logged out and the client port changes from the Access VLAN to the Authentication VLAN, the IP address for the client machine also needs to change to come from the Authentication VLAN. In OOB, when the user is in the Access VLAN, the Agent no longer communicates with the CAM or CAS, so the Agent is not aware when the CAM changes the VLAN for the client port. Although the CAM can bounce the port to change the IP address on the client, this solution is not recommended for IP Phone environments, as it can disrupt voice services.

To enable and specify settings to support Access to Authentication VLAN Change Detection on a Windows client with the Cisco NAC Agent installed:

Step 1

Determine what settings you want to specify for the “RetryDetection,” “PingArp,” “PingMaxTimeout,” or “VlanDetectInterval” parameters to enable the Access to Authentication VLAN Change Detection feature within your network and the **NACAgentCFG.xml** Agent configuration file accordingly. (See [Cisco NAC Agent XML Configuration File Settings, page 9-20](#).)

Step 2 After you have specified the settings you want to use to guide Windows Cisco NAC Agent behavior, save the **NACagentCFG.xml** Agent configuration file locally, upload it to the CAM, and make this new version available to Windows client machine users when they next authenticate with Cisco NAC Appliance (see [Installation Page, page 9-17](#) for more information).

**Note**

The Cisco NAC Agent only requires administrative privileges on the client machine during initial installation. Once successfully installed on the client machine, the Cisco NAC Agent does not require the user to have the administrative privileges to perform functions like Access to Authentication VLAN Change Detection.

**Note**

For details on configuring the “VlanDetectInterval” setting on Windows and Mac OS X Clean Access Agent client machines, refer to the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5\(1\)](#) and [Release Notes for Cisco NAC Appliance, Version 4.5\(1\)](#).

Out-of-Band Users

OOB User Sessions

The following triggers detect when an OOB user has logged off and will force revalidation:

- Linkdown SNMP traps (when user unplugs or reboot)
- MAC notification traps

**Note**

To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

- Certified Timer expiration
- Session Timer expiration
- Manual removal from CAM

For additional details, see also [Interpreting Event Logs, page 13-4](#) and [Manage Certified Devices, page 11-10](#).

Wired and Wireless OOB User List Summary

[Table 3-3](#) describes the lists used to track out-of-band users.

Table 3-3 Out-of-Band User List Summary

User List	Description
In-Band Online Users	<ul style="list-style-type: none"> The In-Band Online Users list (Figure 11-14 on page 11-20) tracks in-band users logged into the network. The CAM adds a client IP/MAC address (if available) to this list after a user logs into the network either through web login or the Agent. Removing a user from this Online Users list logs the user off the in-band network.
Certified Devices List	<ul style="list-style-type: none"> The Certified Devices List (Figure 11-10 on page 11-13) lists the MAC addresses of all “certified” client devices—whether out-of-band or in-band—that have met Agent requirements. The CAM adds a client MAC address to the Certified Devices List after a client device goes through posture assessment and meets Agent requirements. Removing a client from the Certified Devices List: <ul style="list-style-type: none"> Removes an in-band user from the In-Band Online Users list Removes an OOB user from the Out-of-Band Online Users list (causing the port to be changed from the Access VLAN to the Authentication VLAN) and bounces the port, unless Remove out-of-band online user without bouncing the port is checked for the Port profile.
Wired Clients and Wireless Clients	<ul style="list-style-type: none"> The Wired Clients and Wireless Clients lists (Figure 3-31 on page 3-49 and Figure 4-17 on page 4-21) record the activities of out-of-band clients (regardless of VLAN), based on the SNMP trap information that the CAM receives. For Wired OOB clients, the CAM adds a client’s MAC address, originating switch IP address, and switch port number to the out-of-band Discovered Clients list after receiving SNMP trap information for the client from the switch. The CAM updates the entry as it receives SNMP trap information for the client. For Wireless OOB clients, the CAM adds a client’s MAC address, IP address, associated WLC, Access Point MAC address, and Authentication (Quarantine) and Access VLAN assignments to the Wireless Clients list. Thereafter, the CAM updates the entry as it receives new SNMP trap information for the wireless client. Removing an entry from the Wired Clients or Wireless Clients list clears this status information for the OOB client from the CAM. <p>Note For Wired OOB clients, an entry must exist in the Wired Clients list in order for the CAM to determine the switch port for which to change the VLAN. If the user is logging in at the same time that an entry in the Discovered Clients list is deleted, the CAM will not be able to detect the switch port.</p>

Table 3-3 Out-of-Band User List Summary

User List	Description
Out-of-Band Online Users	<ul style="list-style-type: none"> The Out-of-Band Online Users list (Figure 11-15 on page 11-21) tracks all authenticated out-of-band users that are on the Access VLAN (on the trusted network). The CAM adds the client MAC address to the Out-of-Band Online Users list after a client is switched to the Access VLAN. <p>Note The “User IP” of an OOB online user is the IP address of the user on the Authentication VLAN. By definition Cisco NAC Appliance does not track users once they are on the Access VLAN; therefore OOB users are tracked by the Authentication VLAN IP address they have while in the Cisco NAC Appliance network.</p> <ul style="list-style-type: none"> When a user is removed from the Out-of-Band Online Users list, the CAM instructs the switch or Wireless LAN Controller to change the VLAN of the port from the Access VLAN to the Authentication VLAN. <p>Note For Wired OOB clients, if the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to “kick” the user out, for example) and the switch changes the VLAN assignment for the client’s access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see Configure Access to Authentication VLAN Change Detection, page 3-65.</p> <ul style="list-style-type: none"> Additionally, if Bounce the port after VLAN is changed is checked for the Port Profile (Real-IP gateways), the following occurs: <ol style="list-style-type: none"> The CAM bounces the switch port (off and on). The switch resends SNMP traps to the CAM. The CAM discovers the device connected to the switch port from SNMP MAC change notification/MAC move notification or linkup traps received. The port is assigned the Auth VLAN if the device is not certified. The CAM changes the VLAN of the port according to the Port Profile configuration

OOB Troubleshooting

- [OOB Switch Trunk Ports After Upgrade, page 3-69](#)
- [Unable to Control <Switch IP>, page 3-70](#)
- [OOB Error: connected device <client_MAC> not found, page 3-70](#)

OOB Switch Trunk Ports After Upgrade

Because Cisco NAC Appliance can control switch trunk ports for OOB (starting from release 3.6(1) and above), uplink ports for managed switches need configured as “uncontrolled” ports either before or after upgrade (see “Settings That May Change With Upgrade” in the [Release Notes for Cisco NAC Appliance](#)).

This can be done in one of two ways:

- Before upgrading, change the **Default Port Profile** for the entire switch to “uncontrolled” under **OOB Management > Devices > Devices > List > Config [Switch_IP] > Default Port Profile | uncontrolled**
- After upgrading, change the **Profile** to “uncontrolled” for the applicable uplink ports of the switch under **OOB Management > Devices > Devices > List > Ports [Switch_IP] | Profile**

This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile

If for some reason the above steps are omitted and the switch becomes disconnected, use the following procedure:

-
- Step 1** Delete the switch from the List of Switches in the CAM (under **OOB Management > Devices > Devices > List**).
- Step 2** Configure the switch using its CLI to reverse the changes made to the uplink port by the CAM (trunk native VLAN and MAC change notification/MAC move notification), for example:
- ```
(config-if)# switchport trunk native vlan xxx
(config-if)# no snmp trap mac-notification added
```
- Step 3** Add the switch back to the CAM (under **OOB Management > Devices > Devices > New or Search**), applying “uncontrolled” as the Default Port Profile.
- Step 4** Specifically assign the “uncontrolled” port Profile to the uplink port and other uncontrolled ports (under **OOB Management > Devices > Devices [x.x.x.x] > Ports**).
- Step 5** Reset the Default Port Profile for the switch (under **OOB Management > Devices > Switches [x.x.x.x] > Config**).

Initialize the switch ports (under **OOB Management > Devices > Devices [x.x.x.x] > Ports**).

---

## Unable to Control <Switch IP>

If the error message **Unable to control “<Switch\_IP>”** displays on the console when attempting to add a switch under **OOB Management > Devices > Devices > New**:

- Make sure the switch profile matches the switch type. For example, if the switch is a 3750, but you specified it as a 2950 in the switch profile, the CAM will fail when it tries to add the 3750 using 2950 profile. Changing the profile to 3750 will resolve this issue.
- Make sure SNMP traps are enabled and that SNMP community strings are properly configured on the switch. See [Example Switch Configuration Steps, page 3-16](#) for details.

## OOB Error: connected device <client\_MAC> not found

Client connection errors can result from incorrect configuration of the switch profile. If attempting to log into the network using the Agent, and the Agent provides the following error: **“Login Failed! OOB Error: connected device <client\_MAC> not found. Please contact your network administration.”**

- Make sure the switch profile matches the switch type under **OOB Management > Devices > Devices > New**

For example, if the switch is a 3750, but you specified it a 2950 switch profile when adding the switch, when the CAM receives the SNMP linkup trap from the switch for the client that is connecting (with the MAC address specified in the Agent error message), the CAM will attempt to contact that switch to find that MAC address. If the wrong profile is specified for the switch, or the switch is not yet configured in the CAM, the CAM will not be able to contact that switch. Changing the switch profile to 3750 will resolve this issue.

## Troubleshooting SNMP

This section describes how to troubleshoot the common errors that occur in SNMP operations.

[Error: Unable to control “switch-ip-address”, page 3-70](#)

[Error: SNMP request timed out \[1.3.6.1.4.1.9.9.215.1.1.5.0\], page 3-71](#)

[Error: SNMP failure \[1.3.6.1.4.1.9.9.215.1.1.5.0\]: Unknown user name, page 3-71](#)

[Error: SNMP failure \[1.3.6.1.4.1.9.9.215.1.1.5.0\]: Wrong digest, page 3-71](#)

[Error: SNMP failure \[1.3.6.1.4.1.9.9.215.1.1.5.0\]: Authorization error, page 3-71](#)

[Error: SNMP failure \[1.3.6.1.4.1.9.9.215.1.1.5.0\]: Unsupported Security Level, page 3-72](#)

[Error: SNMP failure \[1.3.6.1.4.1.9.9.215.1.1.5.0\]: No access, page 3-72](#)

[Error: OOB Client MAC/IP not found. Please contact network administrator., page 3-72](#)

[Error: Message not within time window, page 3-72](#)

[Additional Information, page 3-73](#)

## Error: Unable to control “switch-ip-address”

This error may occur when a device is being added to CAM under **OOB Management > Devices > New**.

The CAM logs may contain an exception as shown in the following example:

```
2012-01-08 18:35:12.325 +0530 [TP-Processor23] TRACE
c.p.wlan.web.sms.cisco.AbstractDeviceController - SNMP request timed out
[1.3.6.1.2.1.1.2.0]. com.perfigo.wlan.web.sms.DeviceControlException: SNMP request timed
out [1.3.6.1.2.1.1.2.0].
```

The above may happen due to one of the following reasons:

- Switch IP address is not reachable via CAM.  
Perform a ping operation to the switch IP address to confirm that it is reachable.
- Mismatch in SNMP Read settings.  
The SNMP Read settings that are setup in the device profile under **OOB Management > Profiles > Device** and the settings in the switch configuration are not the same. Make sure the settings are the same.
- Supported OID not present in the CAM DB.  
Check the **sysobjectid** of the switch and make sure it is present in the “supported\_switch” table of CAM DB. The data under the “supported\_switch” table gets populated when update is performed from CAM using **Device Management > Clean Access > Updates**. The list of supported switch OIDs are maintained at the central perfigo site.

## Error: SNMP request timed out [1.3.6.1.4.1.9.9.215.1.1.5.0]

CAM logs contain the error as shown in the following example:

```
2012-01-08 18:41:57.010 +0530 [TP-Processor23] ERROR com.perfigo.wlan.web.sms.Switch
- switch [9.0.20.3] SNMP WRITE failed, 1 consecutive write failures!
2012-01-08 18:41:57.011 +0530 [TP-Processor23] ERROR com.perfigo.wlan.web.sms.SnmpManager
```

This error happens when there is a mismatch in the SNMP Write settings. When the admin clicks the ports for a switch, then this error is displayed in the CAM web console. I

The SNMP Write settings setup in the device profile under **OOB Management > Profiles > Device** are different from the settings in the switch configuration. Make sure the settings are the same.

## Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: Unknown user name

This error occurs when the SNMP V3 username mentioned in the device profile under **OOB Management > Profiles > Device** does not exist in the switch configuration.

## Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: Wrong digest

This error occurs when the SNMP V3 Auth password or Auth type mentioned in the device profile under **OOB Management > Profiles > Device** does not match with the one in the switch configuration.

## Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: Authorization error

This error occurs when the SNMP V3 Auth/Priv is not setup in the device profile under **OOB Management > Profiles > Device**, while the username in the switch configuration has been setup with the Auth/Priv security level.

## Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: Unsupported Security Level

This error occurs when the SNMP V3 Auth/Priv is setup in the device profile under **OOB Management > Profiles > Device**, while the username in the switch configuration is not using any Auth/Priv security level.

## Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: No access

This occurs when SNMP V3 user is not properly configured.

While creating a SNMP V3 user on the switch, the commands must be executed in the right order. The following order is recommended:

1. Create SNMP View
2. Create SNMP Group
3. Create SNMP User.

If there is a change in the above order, then the user is not properly bound to the correct Group or View. This causes issues to the user and throws the above error.

## Error: OOB Client MAC/IP not found. Please contact network administrator.

This error usually occurs when the user tries to login. This happens when CAM is not able to find a matching entry for the client's MAC address in the Discovered Clients list

Perform the following steps:

- Check whether the SNMP receiver settings that are defined in CAM under **OOB Management > SNMP Receiver > SNMP Trap** match those defined in the switch configuration. Make sure that the switch is configured to send traps to CAM.
- Perform port bounce on the port to which the user is connected. This would make the switch to send the traps to CAM. On processing the traps, CAM would add an entry to the Discovered Clients list.

After performing the above, the user will be able to login successfully.

## Error: Message not within time window

This error is seen in packet captures performed at CAM when SNMP V3 is used for write operations. CAM stores the `snmpEngineID`, `snmpEngineBoots` and `snmpEngineTime` for every switch in its memory. When a switch is re-configured then the `engineBoots` and `engineTime` are reset. When the switch sends request, then these values are matched with the values that are stored in CAM for that `engineID`. If they are different, then the error message "Message not within time window" is displayed.

### Workaround:

Update the switch profile. Go to the device profile under **OOB Management > Profiles > Device** for the corresponding switch and update it. This would allow the CAM to reset the `engineBoots` and `engineTime` for the switches to default values. Another workaround is to restart the CAM perfigo service.

**Note**

---

Ensure that the switches are not configured with the same **engineID**. This causes the CAM to send the **engineBoots** and **engineTime** of one switch to another switch as the **engineIDs** are same. This results in failure of SNMP write operations and the error “message not in time window”.

---

## Additional Information

In the CAM web console, navigate to **OOB Management > Profiles > Port > New**. When the option **Generate event logs when there are multiple MAC addresses detected on the same switch port** is enabled, there may be an impact on performance, as hub detection happens for every SNMP trap. Make sure this option is disabled when using switches with large number of ports like 6500.



