



CHAPTER 3

Configuring Layer 3 Out-of-Band (L3 OOB)

This chapter provides a general overview of the configuration needed for Layer 3 Out-of-Band deployment.

For general information on configuring the Cisco NAC Appliance for out-of-band deployment, see “Switch Management and Configuring Out-of-Band (OOB) Deployment” and “Enable the Login Page for L3 OOB” in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(6)*.

Overview

Multi-hop L3 support for **in-band** (wired) deployments enables administrators to deploy the Clean Access Server (CAS) in-band centrally (in core or distribution layer) to support users behind L3 Switches (e.g. routed access) and remote users behind VPN Concentrators or remote WAN routers. With L3 IB, users more than one L3 hop away from the CAS are supported and their traffic always goes through Cisco NAC Appliance.

Multi-hop L3 support for **out-of-band** (wired) deployments enables administrators to deploy the CAS out-of-band centrally (in core or distribution layer) to support users behind L3 Switches (e.g. routed access) and remote users behind WAN routers in some instances. With L3 OOB, users more than one L3 hop away from the CAS are supported and their traffic only has to go through Cisco NAC Appliance for authentication/posture assessment only.

Administrators have the option of deploying a remote CAS or L3 IB CAS for remote WAN users, and in some instances using L3 OOB.

Client MAC Address Detection—Clean Access Agent/Cisco NAC Web Agent or ActiveX/Java Applet

The MAC detection mechanism of the Clean Access Agent/Cisco NAC Web Agent will automatically acquire the client MAC address in L3 OOB deployments.

Users performing web login will download and execute either an ActiveX control (for IE browsers) or Java applet (for non-IE browsers) to the client machine prior to user login to determine the user machine’s MAC address. This information is then reported to the CAS and the CAM to provide the IP address/ MAC address mapping.

ActiveX/Java Applet and Browser Compatibility

- ActiveX is supported on IE 6.0 for Windows XP and Windows 2000 systems.
- **IE 7.0 Beta is not supported when the Clean Access Agent is installed.** For the Agent to login and perform other operations, users must uninstall IE 7.0 Beta 2.

- Java applets are supported for major browsers including Safari 1.2+, Mozilla (Camino, Opera), and Internet Explorer on Windows XP, Windows 2000, Mac OS X, and Linux operating systems.
- Due to Firefox issues with Java, Java applets are not supported for Firefox on Mac OS X. See the Firefox release notes (<http://www.mozilla.com/firefox/releases/1.5.0.3.html>) for details.

**Note**

For MAC OS X Clients: On Apple Mac OS X, the browser settings to bypass proxy must have the full CAS IP address (e.g. 10.201.217.93) in order for the client machine to load the Java Applet and login successfully.

**Note****For Linux OOB Clients:**

Because Linux machines behave differently than Windows/Mac OS X clients (i.e. do not release IP address when NIC is down and renew IP address when NIC is up), use the following steps for OOB Linux clients:

1. Set a short lease time (e.g. 60 seconds) for the DHCP server on the Auth VLAN.
2. In the **Port Profile**, disable (uncheck) the **“Remove out-of-band online user when SNMP linkdown trap is received”** option.

This will cause the Linux client to renew its IP address shortly after authentication/certification.

Note Because Linux shuts down/restarts the NIC when renewing the IP address, if this option is enabled (checked) in the Port Profile, the renewal will set the port back to the Auth VLAN.

3. Alternatively, you can set the Port Profile to: **“Change to [Access VLAN] if the device is certified but not in the out-of-band user list.”** This ensures the port stays on the Access VLAN for an authenticated/certified Linux client that is reconnecting to the port after renewing its DHCP lease.

This new feature modifies the following web admin console pages:

- A new checkbox and dropdown menu is added for **“Use ActiveX or Java Applet to detect client MAC address when Clean Access Server cannot detect the MAC address”** in the following user login configuration pages:
 - CAM web console: **Administration > User Pages > Login Page > List [Edit] | General**
 - CAS management pages: **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Login Page > List [Edit] > General**
- **Device Management > Clean Access > Updates** (version information for updates to L3 Java Applet Web Client and L3 ActiveX Web Client)

In addition, the web login pages for L3 OOB users will reflect status information related to loading the ActiveX control or Java applet, and renewing the client IP address.

Layer 3 Out-of-Band Deployment Use Cases

- OOB is for wired deployments only
- L3 OOB is best used in Routed Access deployments
- L3 OOB can also be used for Remote WAN sites but considerations/tradeoffs with other deployments, such as:
 - Remote CAS to WAN sites

- L3 IB CAS in Central site to support WAN sites

Layer 3 Out-of-Band L2 vs L3 OOB Implementation

In L2 OOB:

- Users are Layer 2 adjacent to the CAS
- User device connects to switch, switch sends SNMP trap to CAM
- CAM gets device mac and port information from switch
- CAS receives packets and sends source IP/MAC info to CAM
- CAM now has complete mapping IP/MAC/Port
- Once device is certified to be compliant, CAM knows which port to change VLAN

In L3 OOB

- Users are one or more hops away from the CAS
- CAM still gets device MAC and port information from switch
- CAS receives packets with user's IP
- CAS gets MAC information from either Agent or web-login page enabled for ActiveX/Java Applet to determine device MAC address and report it back to CAS
- CAS informs CAM of IP/MAC of device
- CAM has complete IP-MAC-Port mapping

Layer 3 Out-of-Band L3 OOB Details

Using the Clean Access Agent/Cisco NAC Web Agent

The Agent will inform CAS of the device MAC address.

Without the Clean Access Agent/Cisco NAC Web Agent (using weblogin)

- Web-login page will download ActiveX Control or Java Applet to determine device MAC address and report it back to CAS
- CAS informs CAM of IP/MAC of device
- CAM has complete IP-MAC-Port mapping

Layer 3 OOB: Configuration

With Clean Access Agent/Cisco NAC Web Agent

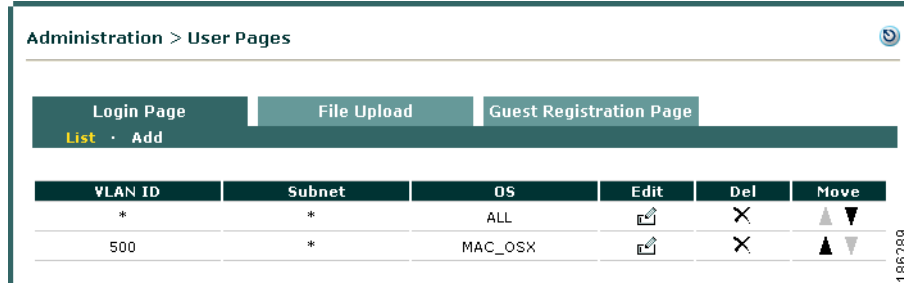
- Agent informs CAS of MAC address
- No additional configuration is needed

Without Clean Access Agent/Cisco NAC Web Agent (using Web Login)

Configure the Login Page

- On CAM: **Administration > User Pages > Login Page > Add/Edit**
- Or CAS: **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Login Page | [Override Global Settings]**

Figure 3-1 Administration User Page



Layer 3 OOB: Configuration

- On Login Page, there is a checkbox and a “Use ActiveX or Java Applet to detect client MAC address when Clean Access Server cannot detect the MAC address” dropdown menu with the following options:
 - ActiveX Only
 - Java Applet Only
 - ActiveX Preferred
 - Java Applet Preferred
 - ActiveX on IE, Java Applet on non-IE Browser
- For “Preferred” options, the preferred option is loaded first; if it fails, the other option is loaded
 - ActiveX is fastest with IE
 - ActiveX is preferred and faster than applet
- ActiveX supported on IE 6.0 on Windows XP/2000
- Java Applet supported on most browsers



Note

DHCP IP addresses can be refreshed for client machines using the Clean Access Agent or ActiveX Control/Java Applet without requiring port bouncing after authentication and posture assessment. See “Enable Web Client for Login Page” in the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1\(6\)](#) for further details.

For detailed information on Access to Authentication VLAN change detection, refer to the “Configuring Access to Authentication VLAN Change Detection” section in the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1\(6\)](#).

Figure 3-2 Administration User Page Edit

Administration > User Pages

Login Page | File Upload

List · Add · Edit

General | Content | Style

Enable this login page

VLAN ID *
(separate multiple VLANs with a comma)

Subnet (IP/Mask) * / *

Operating System ALL

Page Type Frameless

Page Description

Web Client (ActiveX/Applet) ActiveX Only

Use web client to detect client MAC address and Operating System.

Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)

Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)

183506

Layer 3 OOB: Important Configuration Notes

- If a Managed Subnet is configured, Cisco NAC Appliance does not use L3 OOB for those subnets.
- Managed subnets are for L2 users only.
- You must click the **Enable L3 support** checkbox under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.

Figure 3-3 Enabling L3 Support

The screenshot shows the configuration page for a Clean Access Server (IP: 10.201.5.120) in the 'Network' tab. The 'Clean Access Server Type' is set to 'RealIP Gateway'. Three checkboxes are present: 'Enable L3 support' (unchecked), 'Enable L3 strict mode to block NAT devices with Clean Access Agent' (unchecked), and 'Enable L2 strict mode to block L3 devices with Clean Access Agent' (unchecked). The platform is 'APPLIANCE'. The 'Trusted Interface' (to protected network) has IP Address 10.201.5.120, Subnet Mask 255.255.255.0, and Default Gateway 10.201.5.1. The 'Untrusted Interface' (to managed network) has IP Address 192.168.241.31, Subnet Mask 255.255.255.0, and Default Gateway 192.168.241.1. Both interfaces have 'Set management VLAN ID' set to 0. A note states: '(Make sure the Clean Access Server is on VLAN n before you set its management VLAN ID to n.)'. 'Update' and 'Reboot' buttons are at the bottom right.

281258

- Client machines should be able to execute either ActiveX or Java Applet.
- When the CAM changes the VLAN on the switch port from the Authentication VLAN to the Access/User Role VLAN, port bouncing is required.
 - In Port profiles (**Switch Management > Profiles > Port > New/Edit**), make sure **Bounce the port after VLAN is changed** is checked.
 - or
 - If using the 4.1.2.0 and later Windows Clean Access 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. If you use this method, be sure to follow the guidelines and warnings detailed in the “DHCP Release/Renew with Agent/ActiveX/Java Applet,” “Configuring Access to Authentication VLAN Change Detection,” and “Advanced Settings” sections of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(6)*.

Figure 3-4 VLAN Setting Changes to Bounce a Port

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

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.

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

183553

- In Port profiles, make sure **Remove out-of-band online user without bouncing the port** is unchecked.

Figure 3-5 Unchecked OOB Selection

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.
 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.

183814

Layer 3 OOB: Networking

- L3 OOB will typically be used in Routed Access environments.
- With OOB, the goal is to make user traffic flow through the CAS during Authentication, Posture Assessment and Remediation only.
 - CAS challenges user for credentials and also acts as policy enforcement device in the Unauthenticated and Quarantine/Temporary roles.
- Once the user is certified to be compliant, it bypasses the CAS.
- Use networking technologies (such as PBR or VRF) to achieve this goal.

