CHAPTER 5

Wireless NAC Appliance Integration

This chapter provides design guidance for deploying Cisco Network Admission Control (NAC) appliance endpoint security in a Cisco Unified Wireless Network deployment. These best practice recommendations assume that a Cisco Unified Wireless Network has been deployed in accordance with the guidelines provided in the *Enterprise Mobility Design Guide 4.1*, which is available at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

This chapter discusses how to implement, in a reliable and scalable manner, the Cisco NAC appliance (formerly Cisco Clean Access) with Cisco Unified Wireless architecture. It is not intended to be a comprehensive guide on the Cisco NAC appliance solution itself. This chapter focuses on implementation details that are not otherwise addressed in the Cisco Clean Access or Cisco Unified Wireless end user guides.

Introduction

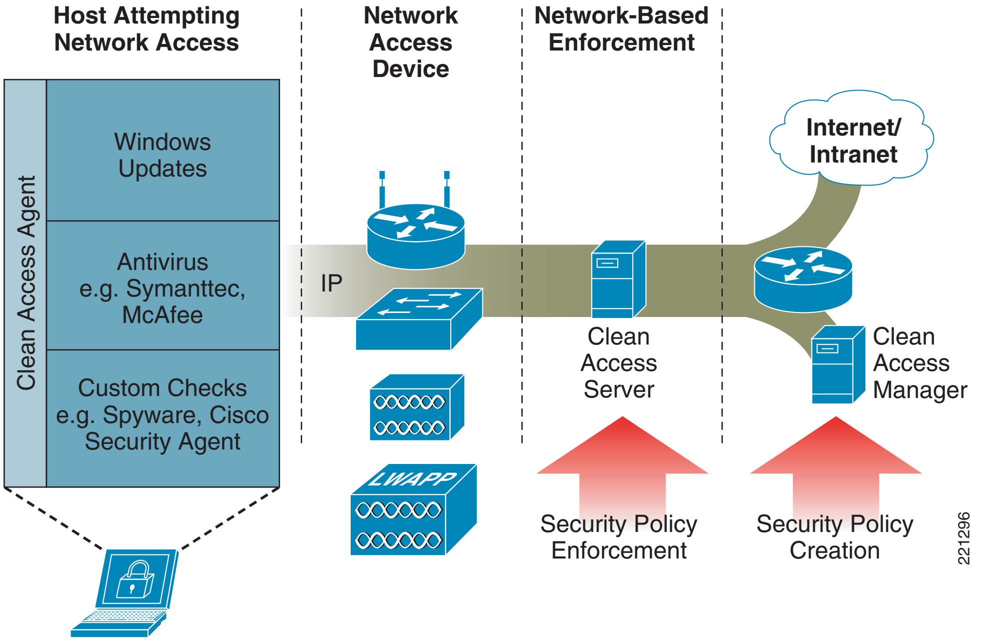
Cisco NAC appliance is an easily deployed NAC product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With Cisco NAC appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. The Cisco NAC appliance identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with network security policies, and repairs any vulnerabilities before permitting access to the network.

When deployed, Cisco NAC appliance provides the following benefits:

- Recognizes users, their devices, and their roles in the network. This first step occurs at the point of authentication, before malicious code can cause damage.
- Evaluates whether machines are compliant with security policies. Security policies can include specific anti-virus or anti-spyware software, operating system (OS) updates, or patches. Cisco NAC appliance supports policies that vary by user type, device type, or operating system.
- Enforces security policies by blocking, isolating, and repairing non-compliant machines.

Non-compliant machines are redirected to a quarantine network, where remediation occurs at the discretion of the administrator. Figure 5-1 shows a generic NAC appliance topology.

Figure 5-1 In-band Clean Access Topology with Wireless Access


Host Attempting Network Access
Network Access Device
Network-Based Enforcement
Clean Access Agent
Windows Updates
Antivirus e.g. Symanttec, McAfee
Custom Checks e.g. Spyware, Cisco Security Agent
IP
LWAPP
Internet/ Intranet
Clean Access Server
Clean Access Manager
Security Policy Enforcement
Security Policy Creation
221296

For a more in-depth overview of the Clean Access Server and Clean Access Manager, see the following documents at the URL below:

- *Cisco NAC Appliance—Clean Access Server Installation and Administration Guide*
- *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*

  http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

NAC Appliance and WLAN 802.1x/EAP

In the context of an enterprise wireless LAN deployment, the Cisco NAC appliance solution should not be considered an alternative to implementing 802.1x/EAP-based authentication. The access control and remediation services offered by the NAC appliance solution are complementary and provide additional security in addition to the inherent access control offered by 802.1x/EAP.

Although it is true that the NAC appliance can be used as a common control point for all access and authentication into a network, it is not able to provide wireless data privacy. For this reason, 802.1x/EAP in conjunction with WPA/WPA2 is still necessary to ensure data privacy and to mitigate against other wireless security threats.

After a wireless user is authenticated and granted access to the wireless portion of the network, the NAC appliance applies yet another layer of security by further restricting access into the wired portion of the network until the following occurs:

- The end user has been verified/authenticated. This is beneficial in wired networks, but is a redundant function in the wireless network because it repeats what has already been accomplished through 802.1x/EAP authentication.
- The end-user device (computer) passes security policy compliance checks; for example, ensuring that the laptop of a wireless user is running the latest version of antivirus software.

Therefore, one of the challenges in introducing NAC services into a Unified Wireless deployment is dealing with the challenge of "double" authentication. This topic is addressed further in Cisco Clean Access Authentication in Unified Wireless Deployments, page 5-10.

NAC Appliance Modes and Positioning within the Unified Wireless Network

Modes of Operation

The NAC appliance can function in the following four modes of operation:

- Out-of-band virtual gateway
- Out-of-band IP gateway
- In-band virtual gateway
- In-band real IP gateway

Out-of-Band Modes, page 5-3, and In-Band Modes, page 5-4, provide further details.

For an in-depth discussion of each mode, see the server appliance installation documentation at the following URL: http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Out-of-Band Modes

Out-of-band deployments, whether Layer 2 mode (virtual gateway) or Layer 3 mode (real IP gateway), require user traffic to traverse through the NAC appliance only during authentication, posture assessment, and remediation. When a user is authenticated and passes all policy checks, their traffic is switched normally through the network and bypasses the appliance. Cisco Unified Wireless support for NAC out-of-band gateway was added in Software Release 5.1.151.0. The Unified Wireless software release that was used in this design guide cannot be deployed as with a NAC Appliance out-of-band gateway, because it has no method for the CAM to dynamically change WLAN to VLAN mappings at the WLC. This is addressed in the Wireless LAN Controller Software Release 5.1.151.0. For further information about out-of-band NAC features in the Cisco Unified Wireless Network can be found at the following URLs:

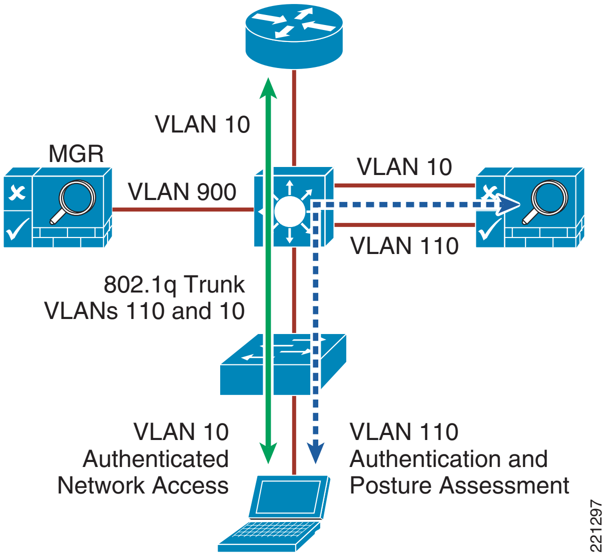
http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml

http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

For further information, see Chapter 4 of the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following URL: http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Figure 5-2 shows a Layer 2 out-of-band topology example.

Figure 5-2 Layer 2 Out-of-Band Topology



To deploy the NAC appliance in this manner, the client device must be directly connected to the network via a Catalyst switch port. After the user is authenticated and passes posture assessment, the Clean Access Manager (CAM) instructs the switch to map the user port from an unauthenticated VLAN (which switches or routes user traffic to the NAC) to an authenticated (authorized) VLAN that offers full access privileges.

In-Band Modes

When the NAC appliance is deployed in-band, all user traffic, both unauthenticated and authenticated, passes through the NAC appliance, which may be positioned logically or physically between end users and the network(s) being protected. See Figure 5-3 for a logical in-band topology example and Figure 5-4 for a physical in-band topology example.

Figure 5-3 In-Band Virtual Gateway Topology

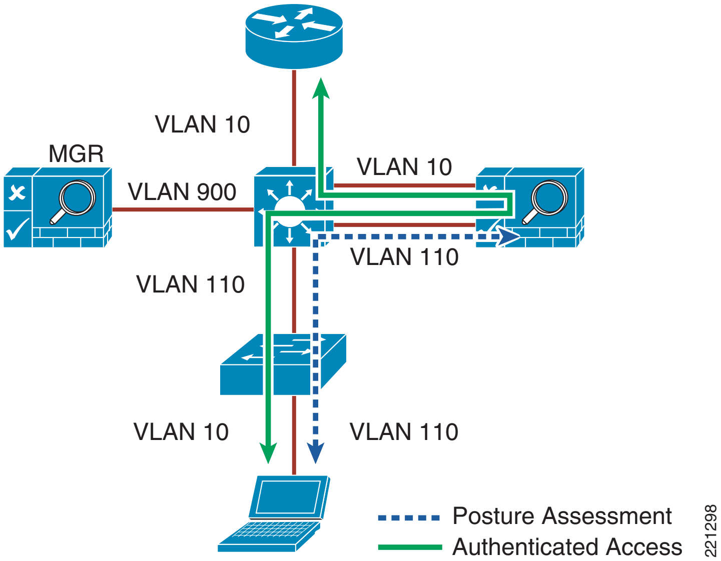
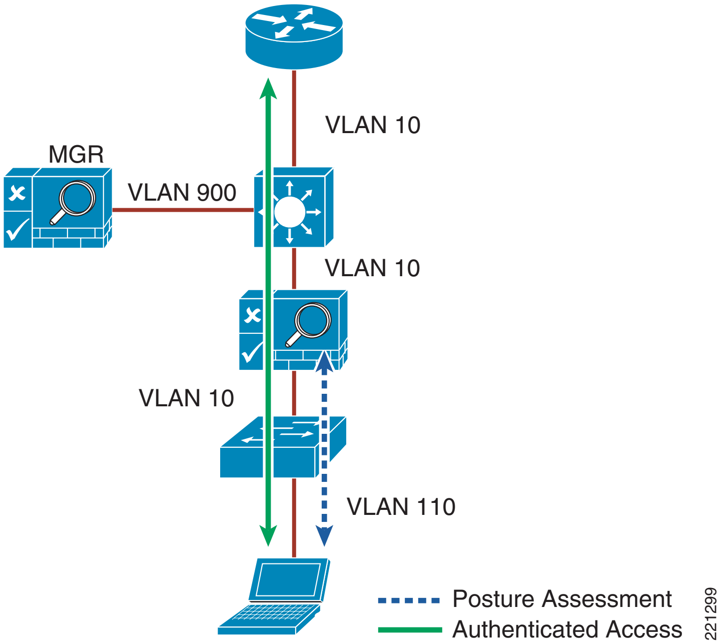


Figure 5-4 Physical In-Band Topology



The in-band mode is the only method that can currently be used with the Cisco Unified Wireless Network software used in this design guide, but out-of-band is supported in 5.1 or later software releases. As discussed in Modes of Operation, page 5-3, the NAC appliance can operate either as a virtual gateway or a real IP gateway. Both gateway methods are compatible with a Unified Wireless deployment and are discussed in this guide.

In-Band Virtual Gateway

When the NAC appliance is configured as a virtual gateway, it acts as a bridge between end users and the default gateway (router) for the client subnet being managed. The following two bridging options are supported by the NAC appliance:

- Transparent—For a given client VLAN, the NAC appliance bridges traffic from its untrusted interface to its trusted interface. Because the appliance is aware of "upper layer protocols", by default it blocks all traffic except for Bridge Protocol Data Unit (BPDU) frames (spanning tree) and those protocols explicitly permitted in the "unauthorized" role; for example, DNS and DHCP. In other words, it permits those protocols that are necessary for a client to connect to the network, authenticate, undergo posture assessment, and remediation. This option is viable when the NAC appliance is positioned physically in-band between end users and the upstream network(s) being protected, as shown in Figure 5-4.
- VLAN mapping—This is similar in behavior to the transparent method except that rather than bridging the same VLAN from the untrusted side to the trusted side of the appliance, two VLANs are used. For example, Client VLAN 131 is defined between the wireless LAN controller (WLC) and the untrusted interface of the NAC appliance. There is no routed interface or switched virtual interface (SVI) associated with VLAN 131. VLAN 31 is configured between the trusted interface of the NAC appliance and the next-hop router interface/SVI for the client subnet. A mapping rule is made in the NAC appliance that forwards packets arriving on VLAN 131 and forwards them out VLAN 31 by swapping VLAN tag information. The process is reversed for packets returning to the client. Note that in this mode, BPDUs are not passed from the untrusted-side VLANs to their trusted-side counterparts.

The VLAN mapping option is usually selected when the NAC appliance is positioned logically in-band between clients and the networks being protected. This is the bridging option that should be used if the NAC appliance is going to be deployed in virtual gateway mode with a Unified Wireless deployment.

Note Extreme caution must be exercised when NAC appliances (configured as in-band virtual gateways with VLAN mapping) are deployed in a high availability configuration. Under certain isolated conditions, Layer 2 looped topologies can form if improperly configured. This is discussed further in High Availability Failover Considerations, page 5-29 and NAC Appliance Configuration Considerations, page 5-40.

In-Band Real IP Gateway

When the NAC appliance is configured as a "real" IP gateway, it behaves like a router and forwards packets between its interfaces. In this scenario, one or more client VLAN/subnets reside behind the untrusted interface. The NAC appliance acts as a default gateway for all clients residing on those networks. Conversely, a single VLAN/subnet is defined on the trusted interface, which represents the path to the protected upstream network(s).

After successful client authentication and posture assessment, the NAC appliance by default routes traffic from the untrusted networks to the trusted interface, where it is then forwarded based on the routing topology of the network.

The NAC appliance is not currently able to support dynamic routing protocols. As such, static routes must be configured within the trusted side of the Layer 3 network for each client subnet terminating on or residing behind the untrusted interface. These static routes should reference, as a next hop, the IP address of the trusted interface of the NAC.

If one or more Layer 3 hops exist between the untrusted NAC interface and the end-client subnets, static routes to the client networks must be configured in the NAC appliance. Likewise, a static default route (0/0) is required within the downstream Layer 3 network (referencing the IP address of the untrusted NAC interface) to facilitate default routing behavior from the client networks to the NAC appliance.

Depending on the topology, multiple options exist to facilitate routing to and from the NAC appliance, including static routes, VRF-Lite, MPLS VPN, and other segmentation techniques. It is beyond the scope of this design guide to examine all possible methods.

Gateway Method to Use with Unified Wireless Deployments

As stated previously, either gateway method is compatible with a Cisco Unified Wireless deployment. There are no critical disadvantages with respect to the service options or capabilities that can be implemented if one gateway method is chosen over the other. However, from an overall deployment perspective, the following considerations may create a preference for one gateway method:

- Real IP gateway does *not support* multicast services. If there is a requirement for the wireless network to support multicast, virtual gateway mode should be used.
- With regard to quality-of-service (QoS), both real IP gateway and virtual gateway modes forward type-of-service (ToS)/differentiated services code point (DSCP) values transparently without changing or acting upon a given QoS value.
- Real IP gateway mode requires static routes to be configured upstream of the NAC appliance to support proper routing to the untrusted client subnets. Depending on the topology downstream (untrusted side) of the NAC appliance, additional static route configuration may be required.
- Real IP gateway mode requires additional configuration to support centralized DHCP services. Specifically, filters must be defined in the NAC appliance for each WLC dynamic interface that sources DHCP relay messages to a centralized server. Alternatives include hosting DHCP services on the NAC appliance itself or at the WLC. However, this is not generally recommended for large-scale deployments.
- In real IP gateway mode, the trusted-side VLAN/subnet is used for both management communication with the CAM as well as supporting user traffic.

NAC Appliance Positioning in Unified Wireless Deployments

The Cisco NAC appliance solution supports two deployment models: centralized and edge. In the context of a Cisco Unified Wireless deployment, either location is acceptable as long as the NAC appliance is positioned logically in-band between the wireless users and the upstream networks.

Edge Deployments

Current Cisco best practice for campus network designs recommends a Layer 3 access/distribution model. If a WLAN controller is located at the distribution layer, the NAC appliance should also be positioned in the distribution layer.

The NAC appliance can be configured either as a virtual or real IP gateway; however, in either case it is strongly recommended that the NAC appliance be Layer 2-adjacent to the WLC with no Layer 3 hops in-between. This allows 802.1q trunking to be established between the NAC appliance and the WLC, thereby giving an administrator control over which WLC interfaces are mapped to the NAC appliance. Because the NAC appliance must reside in-band to user traffic, the goal is to forward only untrusted wireless user traffic through the appliance versus all controller traffic; for example, RADIUS, SNMP, LWAPP control/data, and mobility tunnels.

If the distribution layer switch block is designed for high availability (HA) and the NAC appliance is also being deployed in an HA configuration, 802.1q trunking must be established between the distribution switches (see Figure 5-5 and Figure 5-6).

Figure 5-5 Distributed WLC/NAC Deployment

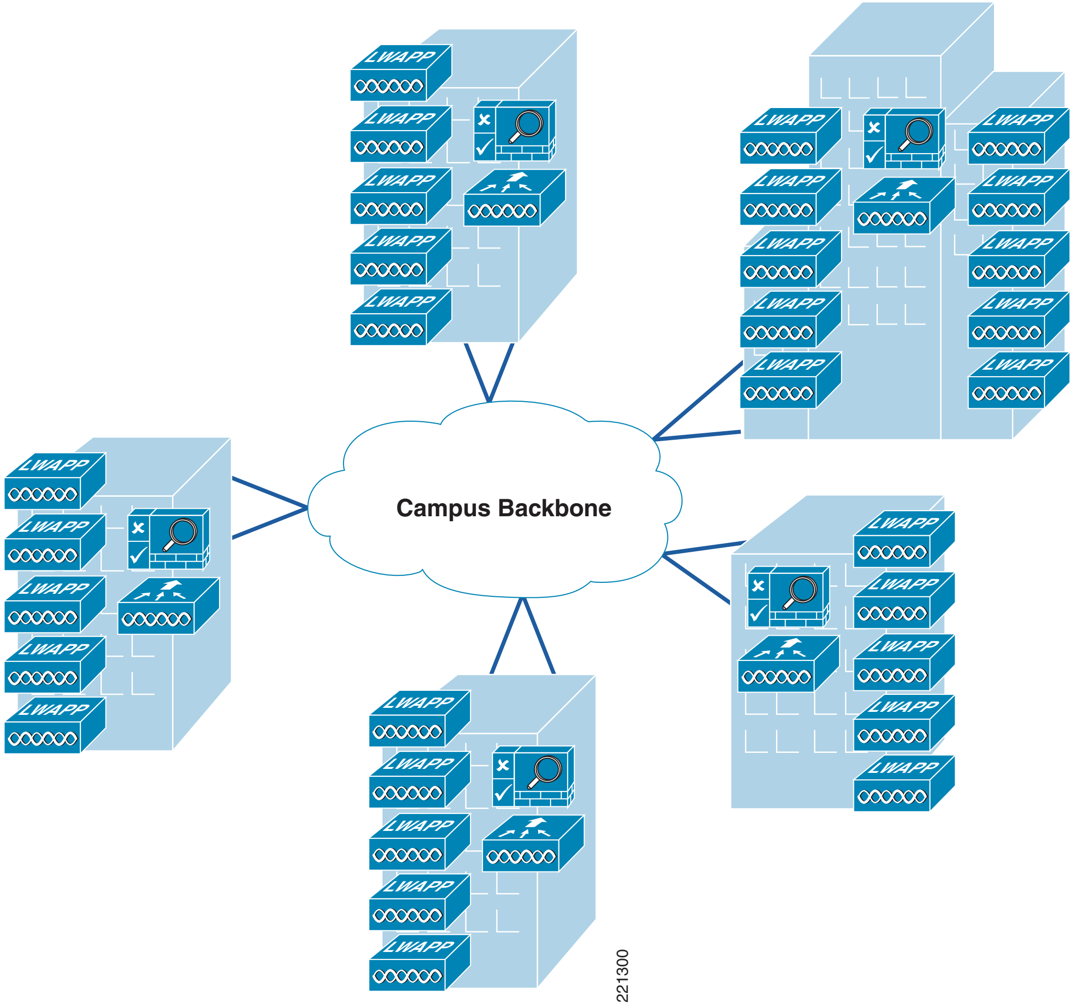
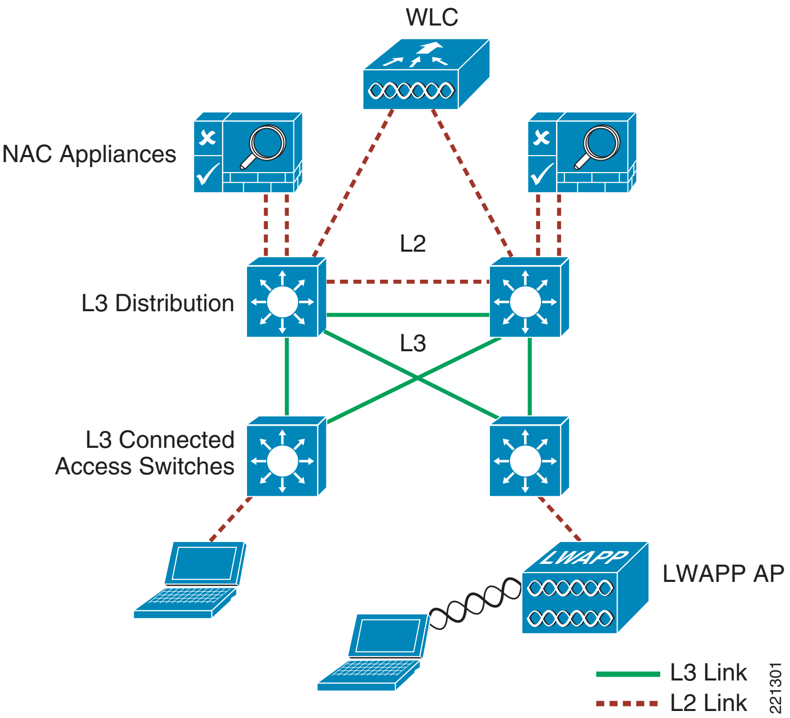


Figure 5-6 Layer 3 Access/Distribution with Unified Wireless and NAC Appliances



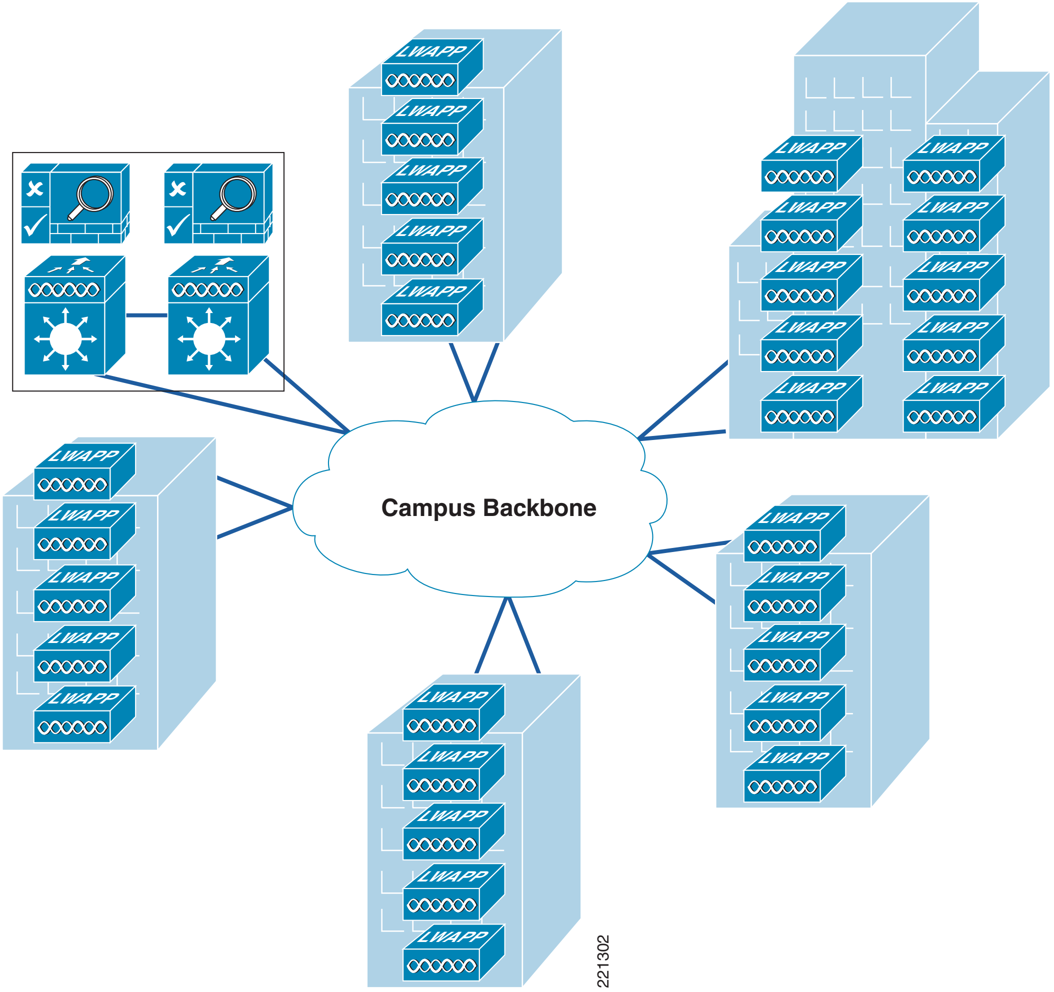
As seen above, the introduction of NAC services at the distribution layer has the potential to introduce Layer 2 complexities in what would otherwise be a straightforward Layer 3 access/distribution design. Also, positioning the NAC appliance at the distribution layer with the WLAN controller(s) may not represent the most economical approach if multiple locations are involved and/or other common services such as firewall and/or IDS/IPS services are being deployed.

Note Although it is possible to implement the NAC appliance with one or more Layer 3 hops between it and the WLAN controller, it is not recommended. To do so would require the introduction of potentially complex segmentation and/or policy routing techniques (depending on the underlying network) to facilitate reliable and predictable transport of untrusted client traffic to the NAC appliance. Complexities associated with the proper handling of non-user, controller-based traffic such as RADIUS, LWAPP, and mobility tunnels must also be taken into consideration.

Centralized Deployments

Current Cisco Unified Wireless best practice recommends that the WLAN controllers be *centrally* located within the campus; for example, collocated at a data center or attached as a service module. Cisco therefore recommends that the WLCs and NAC appliance make up their own switch block that maintains Layer-2 adjacency between the WLC and the NAC appliance within the data center, and be separate from the data center server switch building block (see Figure 5-7). For additional information, see Chapter 2 of the *Enterprise Mobility 4.1 Design Guide* at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

Figure 5-7 Centralized WLC/NAC Deployment



Summary

The NAC appliance offers several deployment options and modes of operation. However, when current campus and mobility best practices are taken into consideration, Cisco recommends that the NAC appliance be deployed centrally with the WLAN controllers as an in-band gateway. This topology is examined further in Implementing NAC Appliance High Availability with Unified Wireless, page 5-22.

Cisco Clean Access Authentication in Unified Wireless Deployments

As discussed in NAC Appliance Modes and Positioning within the Unified Wireless Network, page 5-3, one of the primary functions of the NAC appliance is to identify and authenticate users. Because NAC user authentication is mandatory, the challenge becomes authenticating enterprise wireless users who have already authenticated using 802.1x/EAP. Unfortunately, there is currently no way for the NAC appliance to be directly aware of the authentication state of a wireless user, or to act as a RADIUS proxy for wireless authentication. In place of any such capability, NAC authentication options include the following:

- Web authentication
- Clean Access Agent
- Single sign-on (SSO) with Clean Access Agent with the following:
  - VPN RADIUS accounting
  - Active Directory

Web Authentication

Web authentication requires wireless users to authenticate via the web portal of the NAC appliance. This method is undesirable for enterprise users because the user must open a web browser, be redirected to an authentication page, and enter credentials. Questions include the following:

- Whether to use existing or new credentials
- Whether to use the local NAC database or an external database

On the other hand, web authentication *is* useful and highly desirable in guest access deployment scenarios where the WLAN is otherwise "open", and a universal access method such as web redirect with portal authentication can be used to control access.

Clean Access Agent

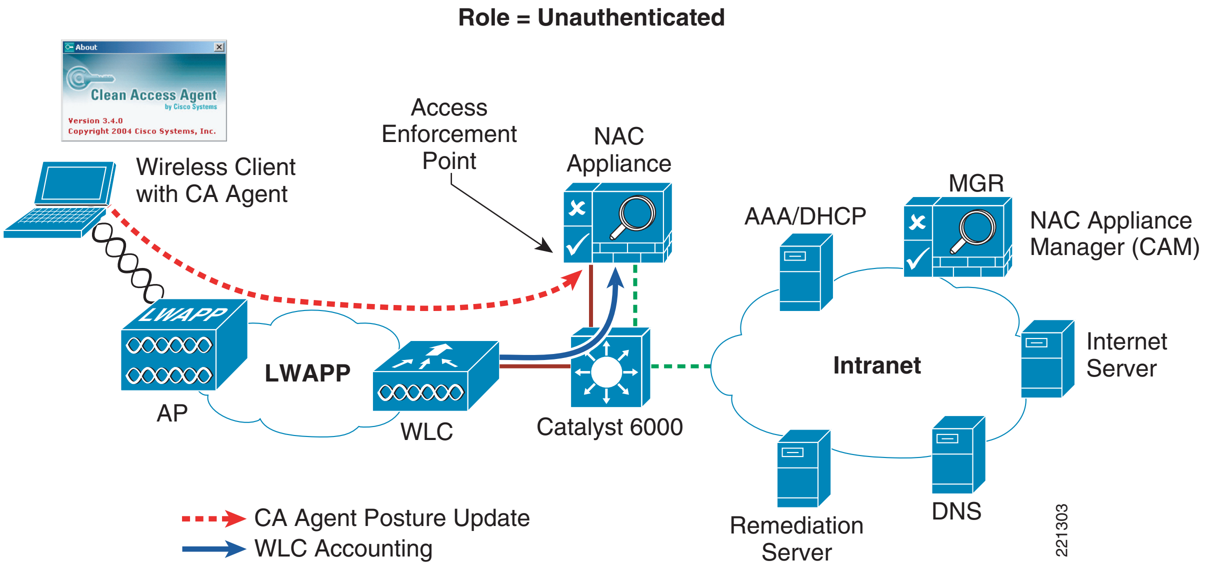
Users authenticate through the Clean Access Agent user interface. In this scenario, the wireless client computer is running Cisco Clean Access Agent software, which automatically detects a Clean Access-protected network and prompts the user for credentials. This is somewhat better than the web method above. However, it requires Clean Access Agent software to be installed on the PC, and the user is still required to manually enter credentials.

Single Sign-On-VPN

Single sign-on (SSO) VPN is an option that does not require user intervention and is relatively straightforward to implement. It makes use of the VPN SSO capability of the NAC solution, coupled with using Clean Access Agent software running on the client PC. VPN SSO uses RADIUS accounting records to notify the NAC appliance about authenticated remote access users connecting to the network. In the same way, this feature can be used in conjunction with the WLAN controller to automatically inform the NAC server about authenticated wireless clients connecting to the network.

See Figure 5-8 through Figure 5-12 for an example showing a wireless client performing SSO authentication, posture assessment, remediation, and network access through the NAC appliance.

Figure 5-8 Wireless VPN SSO—Wireless Authentication/Association



The following sequence is shown in Figure 5-8:

Step 1 The wireless user performs 802.1x/EAP authentication through the WLAN controller to an upstream AAA server.

Step 2 The client obtains an IP address from either AAA or a DHCP server.

Step 3 After the client receives an IP address, the WLC forwards a RADIUS accounting (start) record to the NAC appliance, which includes the IP address of the wireless client.

Note The WLC controller uses a single RADIUS accounting record (start) for 802.1x client authentication and IP address assignment, while Cisco Catalyst switches send two accounting records: an accounting start is sent after 802.1x client authentication, and an interim update is sent after the client is assigned an IP address.

Step 4 After detecting network connectivity, the Clean Access Agent attempts to connect to the CAM. Traffic is intercepted by the NAC appliance, which in turn queries the CAM to determine whether the user is in the online user list. Only clients that are authenticated will be in the online user list, which is the case in the example above as a result of the RADIUS update in Step 3.

Step 5 The Clean Access Agent performs a local assessment of the security/risk posture of the client machine, and forwards the assessment to the NAC appliance for network admission determination.

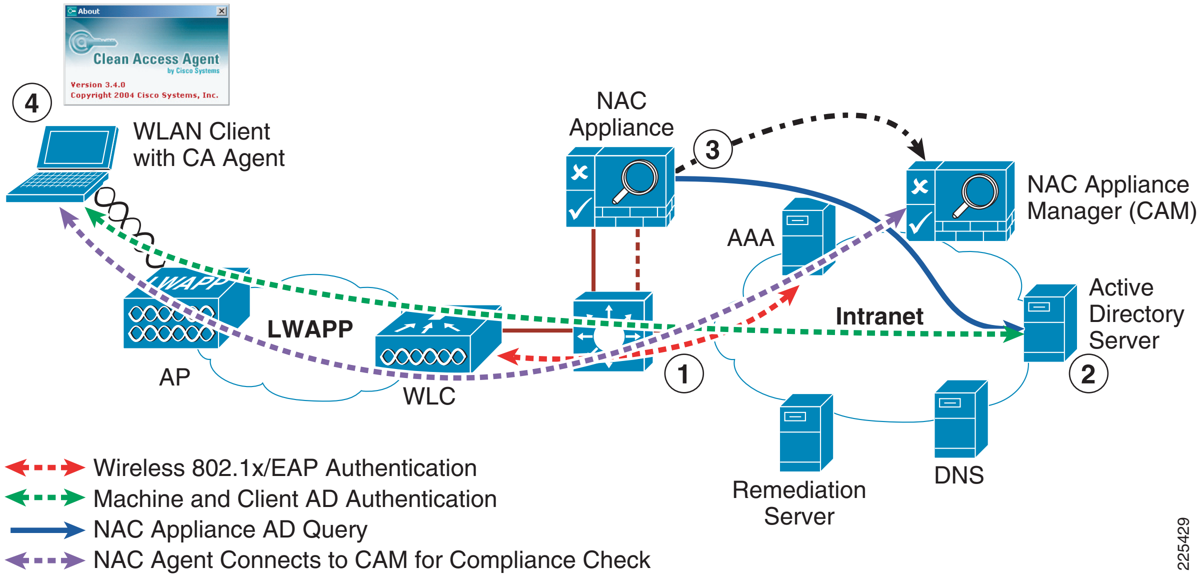
Single Sign-On Active Directory

Single sign-on (SSO) Active Directory is an option that does not require user intervention and is also relatively straightforward to implement. It makes use of Window Client authentication to an Active Directory Domain and capability of the NAC solution to query that domain. Coupled with using Clean

Access Agent software running on the client PC. Active Directory SSO uses the Active Directory database records to inform the NAC appliance about authenticated Windows users connected to the network.

See Figure 5-9 through Figure 5-12 for an example showing a wireless client performing SSO authentication, posture assessment, remediation, and network access through the NAC appliance.

Figure 5-9 Wireless AD SSO—Wireless Authentication/Association



The following sequence is shown in Figure 5-9:

Step 1 The wireless user performs 802.1x/EAP authentication through the WLAN controller to an upstream AAA server.

Step 2 The client obtains an IP address from either AAA or a DHCP server.

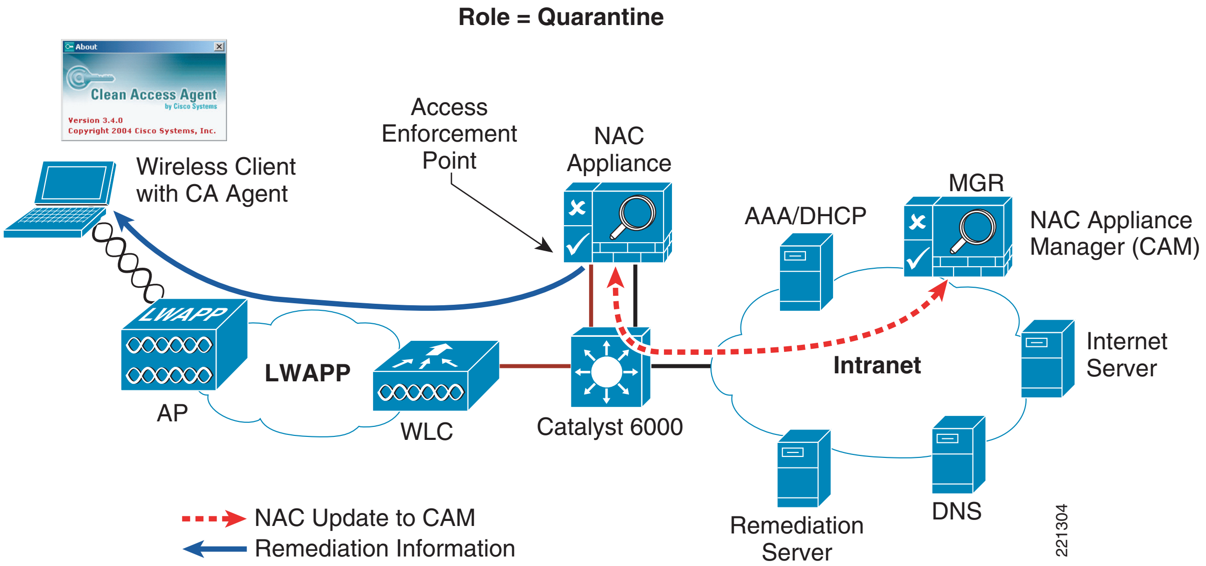
Step 3 After the client receives an IP address, the Windows client attempts to authentication the host (machine), and the client with its Active Directory domain.

Note The WLAN client supplicant needs to be configured to allows windows client authentication and Active Directory Domain rather than using cached credentials. The native Windows supplicant, third-party supplicants such as the Cisco Secure Services Client (CSSC) support this feature. After detecting network connectivity, the Clean Access Agent attempts to connect to the CAM. Traffic is intercepted by the NAC appliance, which queries Active Directory to determine whether the user has authenticated to the Active Directory. Only clients that are authenticated will be in the online user list. The NAC appliance updates the CAM.

Step 4 The Clean Access Agent performs a local assessment of the security/risk posture of the client machine, and forwards the assessment to the NAC appliance for network admission determination.

Posture Assessment and Remediation

Figure 5-10 Wireless SSO—Posture Assessment



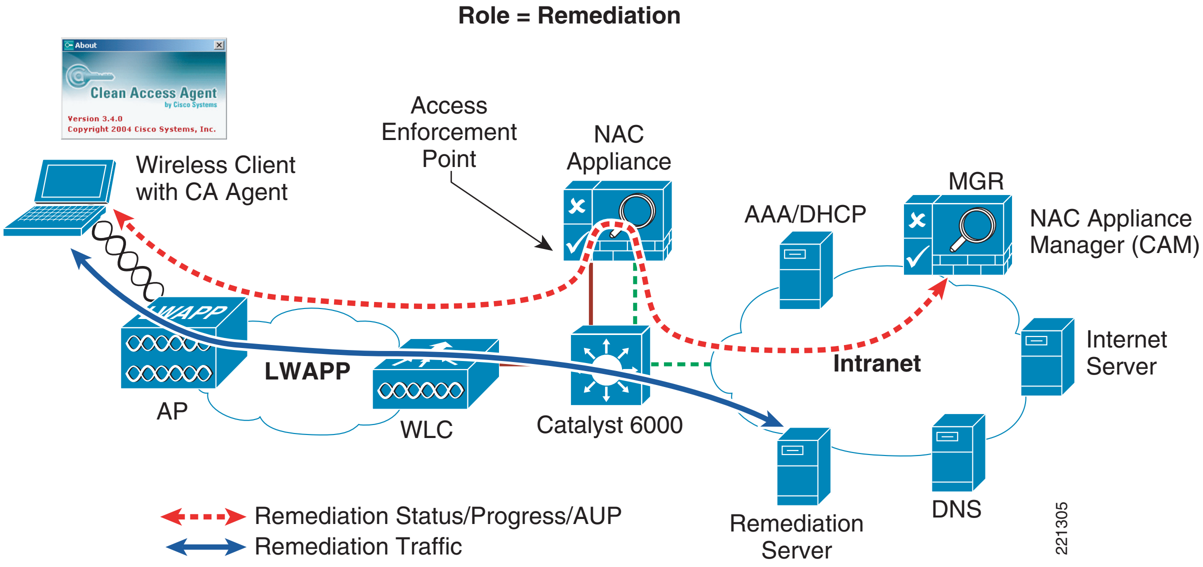
The following sequence takes place in Figure 5-10:

Step 1 The NAC appliance forwards the agent assessment to the NAC appliance manager (CAM).

Step 2 In this example, the CAM determines that the client is not in compliance and instructs the NAC appliance to put the user into a quarantine role.

Step 3 The NAC appliance then sends remediation information to the client agent.

Figure 5-11 Wireless SSO—Remediation



The following sequence takes place in Figure 5-11:

Step 1 The Client Agent displays time remaining to accomplish remediation.

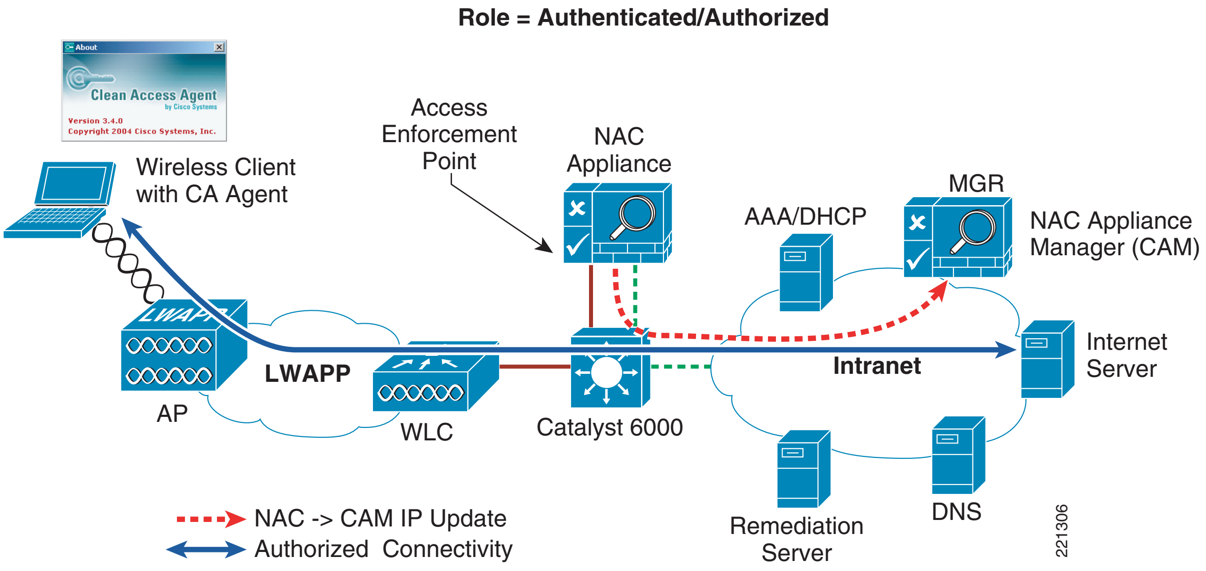
Step 2 The Agent guides the user step-by-step through the remediation process; for example, updating the anti-virus definition file.

Step 3 After remediation completion, the agent updates NAC appliance.

Step 4 The CAM displays an Acceptable Use Policy (AUP) statement to the user.

Note The AUP is optional and can be configured on a per-user role basis.

Figure 5-12 Wireless SSO—Network Access



The following sequence takes place in Figure 5-12:

Step 1 After accepting the AUP, the NAC appliance switches the user to an online (authorized) role.

Step 2 The SSO functionality populates the online user list with the client IP address. After remediation, an entry for the host is added to the certified list. Both these tables (together with the discovered clients table) are maintained by the CAM.

Step 3 The end user is now able to communicate through the network.

As seen above, the most transparent method to facilitate wireless user authentication is to enable SSO authentication on the NAC appliance.

Note If VPN-SSO authentication is enabled without the Clean Access agent being installed on the client PC, the user is still automatically authenticated. However, they are not automatically connected through the NAC appliance until their web browser is opened and a connection attempt is made. In this case, when the user opens their web browser, they are momentarily redirected (without a logon prompt) during the "agent-less" posture assessment phase. If the client passes, they are connected to their originally requested URL. If not, they are directed to the necessary links/sites for remediation. The previously-mentioned behavior assumes that a network administrator has configured the NAC appliance to permit non-agent-based PCs to connect to the network in this manner (see Vulnerability Assessment and Remediation, page 5-16).

Vulnerability Assessment and Remediation

Detecting and correcting client device vulnerabilities before users are allowed access to the network is the core function of the Cisco NAC appliance solution. For configuring vulnerability assessment and remediation policies, see Chapters 9 and 10 of the Cisco *NAC Appliance—Clean Access Manager*

Installation and Administration Guide at the following URL:
http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

To briefly summarize, clients can be checked for vulnerabilities by the following two methods:

- Network scan—This method provides network-based vulnerability assessment and web-based remediation. The network scanner function, which is resident in the NAC appliance, performs the actual scanning and checks for well-known port vulnerabilities to which a particular host may be prone. If vulnerabilities are found, web pages configured in the Clean Access Manager can be pushed to users to distribute links to websites or information instructing users how to fix their systems.
- Clean Access Agent—This method uses a resident, machine-based software agent for vulnerability assessment and remediation. Users must download and install the Cisco Clean Access Agent, which offers administrators better visibility of the host registry, processes, installed applications, and services of a system. The Agent can be used to perform anti-virus/anti-spyware definition updates, to distribute files uploaded to the Clean Access Manager, or distribute links to websites for users to fix their systems.

There are no restrictions as to which method can be used in a Unified Wireless network. Depending on the deployment, both methods can be used concurrently. However, between the two options available, agent-based assessment and remediation is preferred whenever possible for the following reasons:

- It offers the best user experience for wireless clients from an authentication standpoint.
- Vulnerability assessment and remediation are performed locally on the client PC and not by the NAC appliance/manager, thereby improving the performance of the overall solution.

Roaming Considerations

For more details, see the "Roaming" section in Chapter 2 of the *Enterprise Mobility 3.0 Design Guide* at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/emob30dg-Book.html

The Cisco Unified Wireless solution supports the following roaming scenarios:

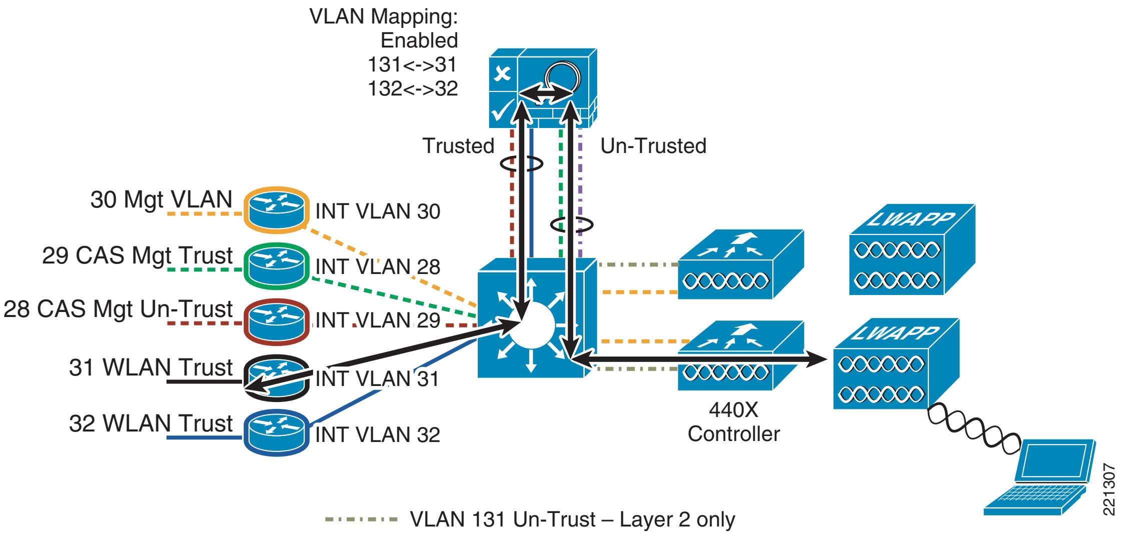
1. Layer 2 client roaming between two APs joined to same WLC.
2. Layer 2 client roaming between two APs joined to different WLCs.
3. Layer 3 client roaming between two APs joined to different WLCs, where each WLC maps the WLAN to a different VLAN/subnet

As outlined previously in NAC Appliance Modes and Positioning within the Unified Wireless Network, page 5-3, the NAC appliance needs to be in-band and Layer 2-adjacent to the WLCs. This means that the VLAN/subnet associated with a given user WLAN is trunked directly to the untrusted interface of the NAC appliance. The roaming behavior discussed below is the same regardless of whether the NAC appliance is configured for virtual or real IP gateway functionality.

Layer 2 Roaming with NAC Appliance

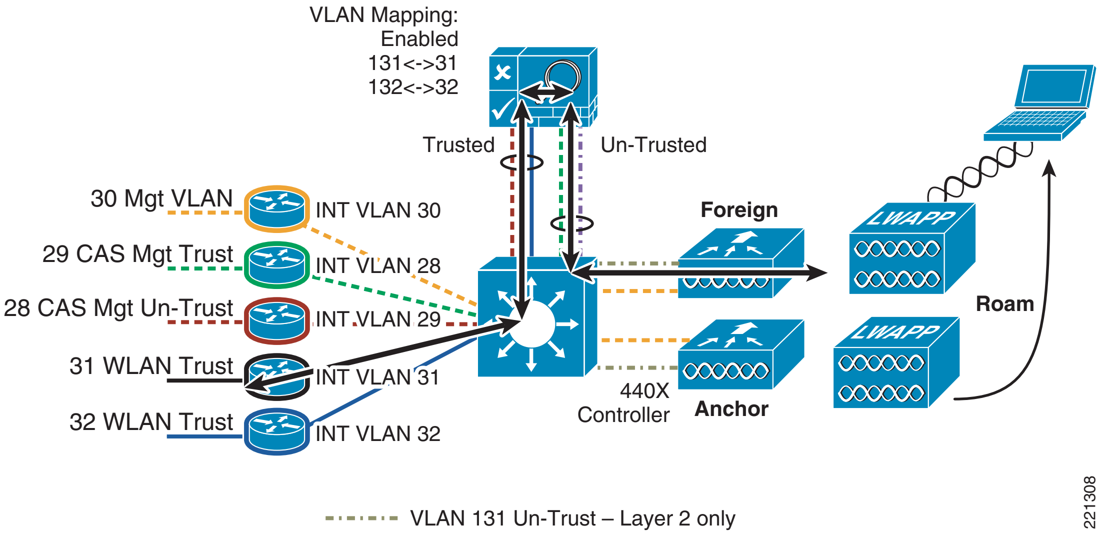
When a client roams between APs in scenarios 1 and 2 above, the user traffic remains on the same VLAN/subnet, and is thereby forwarded through the same VLAN into the NAC appliance. Thus, roaming is supported in both scenarios 1 and 2 above. See Figure 5-13 and Figure 5-14 for an example of a client roaming based on scenario 2.

Figure 5-13 Inter-WLC Layer 2 Roam —Initial Client/NAC Connectivity



In Figure 5-12, the client authenticates, associates to the WLAN, and is auto-connected through the NAC through VPN SSO and Clean Access Agent client software. Refer to Enabling Wireless Single Sign-On, page 5-62, for details regarding wireless SSO.

Figure 5-14 Inter-WLC Layer 2 Roam—Client Roams



When the client in Figure 5-14 roams to an AP joined to a different WLC, connectivity is preserved because the WLAN on the foreign controller is mapped to the same (untrusted) VLAN as the anchor WLC.

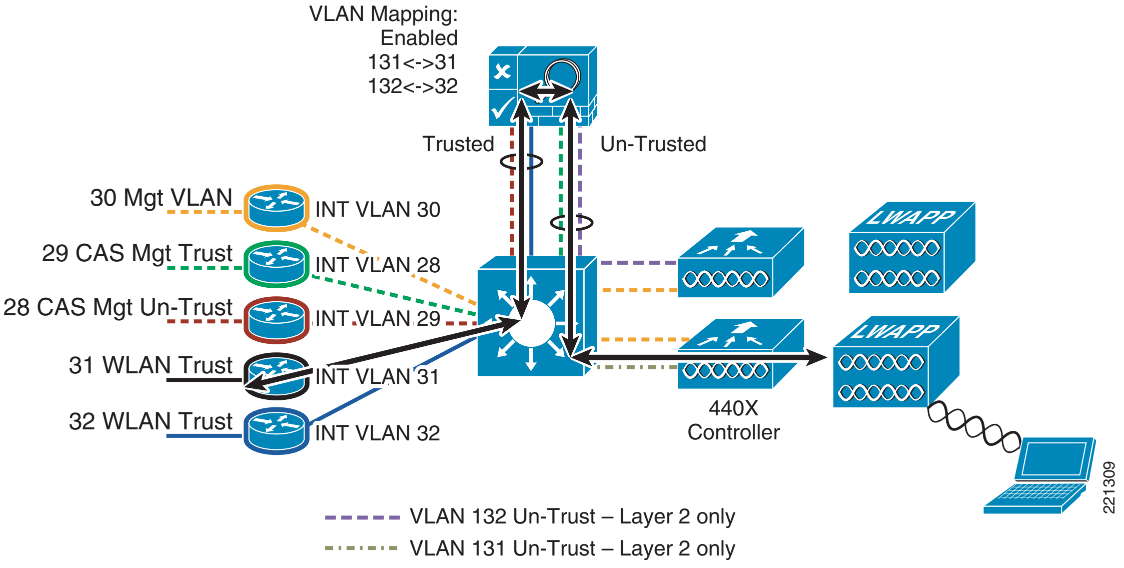
Layer 3 Roaming with NAC Appliance—WLC Images 4.0 and Earlier

Roaming based on scenario 3 above presents a problem when a WLAN is supported by two or more VLAN/subnets between controllers. The issue is not that different subnets are used, but rather the asymmetrical behavior of the mobility tunnel. When a wireless client authenticates and connects through the NAC appliance, traffic arrives at the untrusted interface of the NAC appliance on the VLAN to which the WLAN is mapped at the anchor (home) controller. When the client roams, their status with the NAC appliance remains authenticated as long as VPN SSO and Clean Access Agent are being used.

In the case of scenario 3, the mobility tunnel that is established between controllers (to facilitate inter-controller roaming) is not impacted because the management VLAN (through which mobility tunnels are established) is not trunked to the untrusted interface of the NAC appliance. When the client completes roaming to the foreign (roamed-to) controller, client traffic from the WLAN is now forwarded through a different VLAN/subnet into the untrusted interface of the NAC appliance. The roaming event succeeds from the perspective of the Unified Wireless network, but the NAC appliance blocks the client traffic because it does not switch the traffic of the user concurrently through two different untrusted VLAN/subnets.

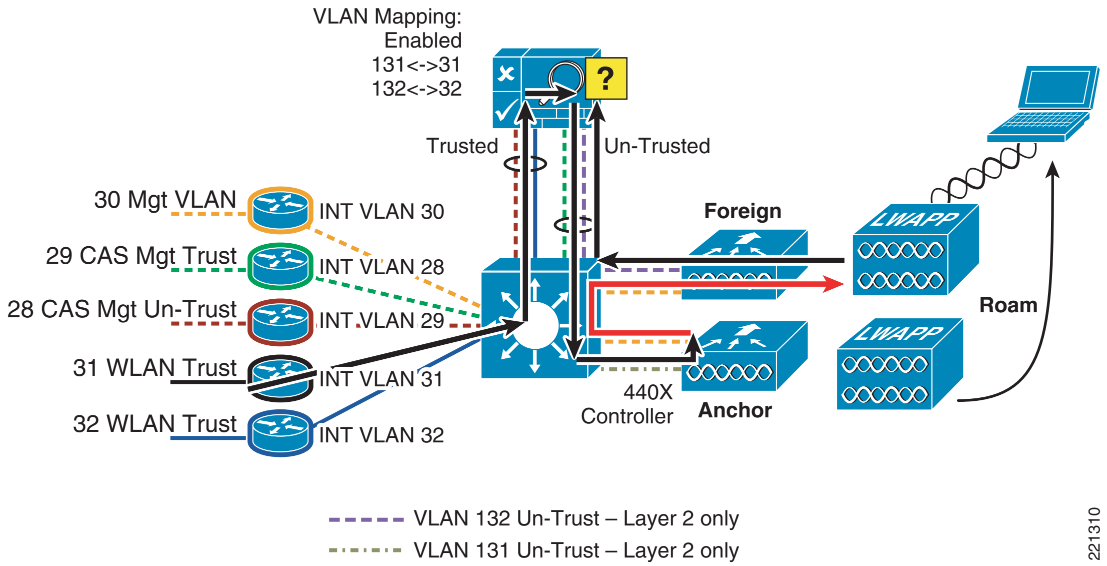
The NAC appliance switches user traffic only via the original VLAN through which the user authenticated. See Figure 5-15 and Figure 5-16 for examples of a client attempting to roam across a Layer 3 boundary.

Figure 5-15 Inter-WLC Layer 3 Roam—Initial WLAN/NAC Connectivity



The client in Figure 5-15 authenticates, associates to the WLAN, and is auto-connected through the NAC via VPN SSO and Clean Access Agent client software. Note that the other controller is using a different VLAN (132).

Figure 5-16 Inter-WLC Layer 3 Roam—Client Roams



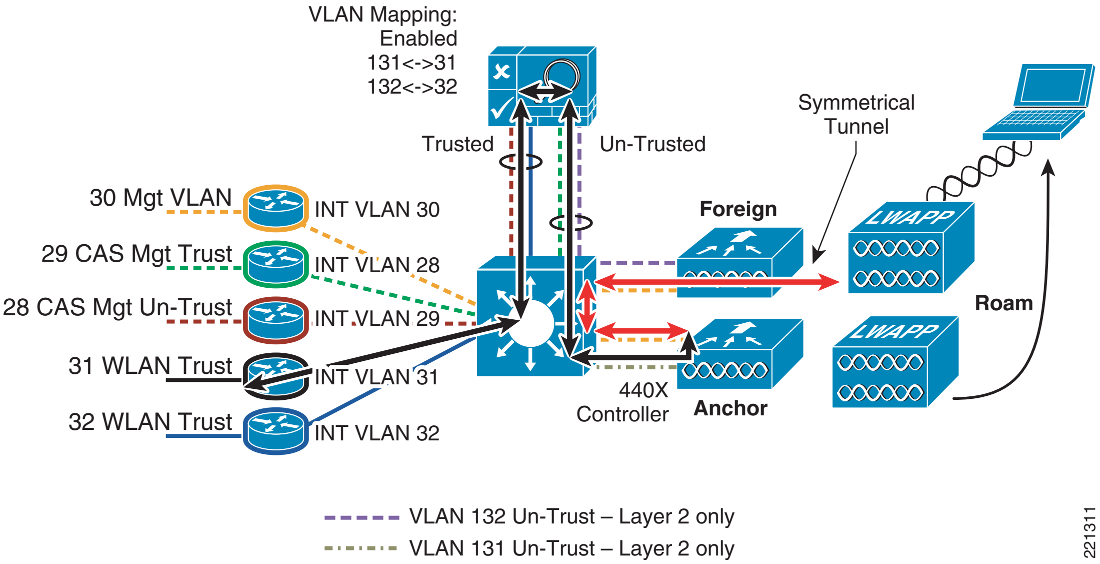
When the client in Figure 5-16 roams to an AP on the other controller, connectivity is interrupted because the foreign (roamed-to) controller forwards traffic via a different untrusted VLAN into the NAC appliance.

There is no workaround to facilitate Layer 3 roaming with NAC services when using controller Releases 4.0 and earlier.

Layer 3 Roaming with NAC Appliance—WLC Images 4.1 and Later

The asymmetrical behavior of the WLC mobility tunnel is not only problematic for NAC appliance deployments, but also creates problems in deployments where a Cisco Firewall Services Module (FWSM) is used in conjunction with a Unified Wireless deployment, or where unicast reverse path forwarding (uRPF) checking is enabled on router interfaces or SVIs. Beginning with WLC Release 4.1 and later, the mobility tunnel can be configured to operate symmetrically, thereby allowing client traffic to flow bi-directionally through the anchor controller. Client traffic remains on the original VLAN/subnet through which the user authenticated, regardless of whether the WLAN is mapped to a different VLAN/subnet at the foreign (roamed-to) controller (see Figure 5-17).

Figure 5-17 Inter-WLC Layer 3 Roam with Symmetrical Mobility Tunnel



When the client in Figure 5-17 undergoes what would otherwise be a Layer 3 roam, the symmetrical mobility tunnel forwards return traffic back to the anchor controller, which keeps the user traffic on the original NAC VLAN through which they authenticated. Client connectivity through the NAC appliance is preserved. This symmetrical tunneling behavior will become a default for software Releases 5.2 and later.

Roaming with NAC Appliance and AP Groups

In typical deployments, a WLAN is mapped to a single dynamic interface per WLC. However, consider a deployment scenario where there is a 4404-100 WLC supporting its maximum number of APs (100). Now consider a scenario where 25 users are associated to each AP. This would result in 2500 users sharing a single VLAN. For performance reasons, some customer designs may require substantially smaller subnet sizes. One way to deal with this is to break up the WLAN into multiple segments. The WLC AP grouping feature allows a single WLAN to be supported across multiple dynamic interfaces (VLANs) on the controller. This is done by taking a group of APs and mapping them to a specific dynamic interface. APs can be grouped logically by employee workgroup or physically by location.

Because a WLAN SSID can be implemented across multiple AP groups, which are in turn mapped to different VLANs/subnets, a possibility exists where a user could roam within the WLAN but cross an AP group boundary. The following scenarios are possible:

- A client roams between two APs that are members of different AP groups but joined to the same controller. This roaming scenario is not impacted when a NAC appliance is implemented with a Unified Wireless topology. Although the client roams to an AP in a different AP group, the client remains on the same dynamic interface (VLAN) through which they originally connected. This roaming behavior is no different than an Layer 2 roam, as described in Layer 2 Roaming with NAC Appliance, page 5-17. A client roams between two APs, joined to different controllers that are members of different AP groups. This scenario is similar to scenario 3 in Roaming Considerations, page 5-17, where a multi-controller deployment makes uses of different dynamic interfaces (VLAN/subnets) to support a common WLAN across a campus deployment. The only difference is that AP grouping is not configured on the WLCs. If a roaming event occurs based on the example above, the result is the same as a Layer 3 roaming event described in Layer 3 Roaming with NAC

Appliance—WLC Images 4.1 and Later, page 5-20. The client hangs at the NAC when the foreign controller attempts to forward client traffic via a different AP group VLAN than the AP group VLAN through which the client originally authenticated at the anchor controller.

Note If the symmetrical mobility tunnel feature of the WLAN controller is used (see Layer 3 Roaming with NAC Appliance—WLC Images 4.1 and Later, page 5-20), roaming between AP group boundaries is supported.

Implementing NAC Appliance High Availability with Unified Wireless

In deployments where high availability is necessary, the NAC appliance can be deployed in a 1:1, hot standby configuration. In this scenario, one NAC appliance is active while the other is in standby mode. The two servers communicate with each other via in-band or out-of-band communication. An inter-appliance communication "link" is used to determine the state of each server. When configuration changes are made to the NAC appliance configuration, the CAM pushes these changes to both active and standby appliances concurrently. Failover from an active to standby server is stateful. For more information, see Chapter 13 of the *Cisco NAC Appliance—Clean Access Server Installation and Administration Guide* at the following URL: http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

In addition, see Figure 5-18 for an example of a high-level Unified Wireless topology with NAC appliance high availability.

Figure 5-18 Unified Wireless Deployment with NAC Appliance High Availability

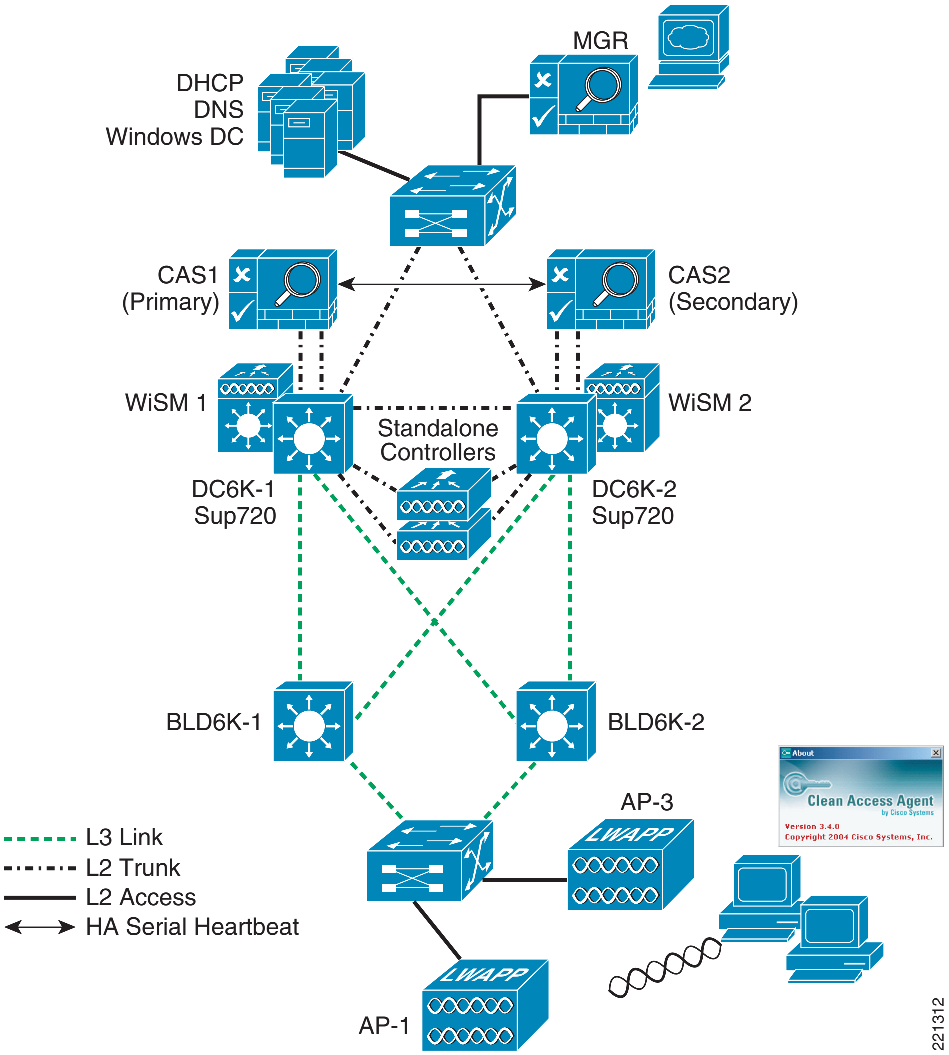


Figure 5-18 shows a fully redundant campus topology with active/standby NAC appliances.

As discussed in In-Band Modes, page 5-4, the NAC appliance can be configured either as a virtual or real IP gateway. Regardless of the gateway method, the physical interconnection between the appliance and the WLAN controller remain the same. Logical configuration differences are discussed when applicable in the following sections.

High Availability NAC Appliance/WLC Building Block

Figure 5-19 and Figure 5-20 provide a detailed diagram of the WLC and NAC appliance interconnection as part of an overall switching block in the data center. The following switching block examples should be standalone and not part of an existing data center server farm switch block.

Figure 5-19 High Availability NAC/WLC Switch Block—Virtual Gateway Mode

╌╌╌	30	Mgt VLAN	10.20.30.0/24
╌╌╌	29	CAS Mgt Trust – Eth0	10.20.29.0/24
╌╌╌	28	CAS Mgt Un-Trust – Eth1	10.20.28.0/24
━━━	31	CAS WLAN1 Trust – Eth0	10.20.31.0/24
━━━	32	CAS WLAN2 Trust – Eth0	10.20.32.0/24
-·-·-	131	CAS WLAN1 Un-Trust – Eth1	Layer 2 only
-·-·-	132	CAS WLAN2 Un-Trust – Eth1	Layer 2 only

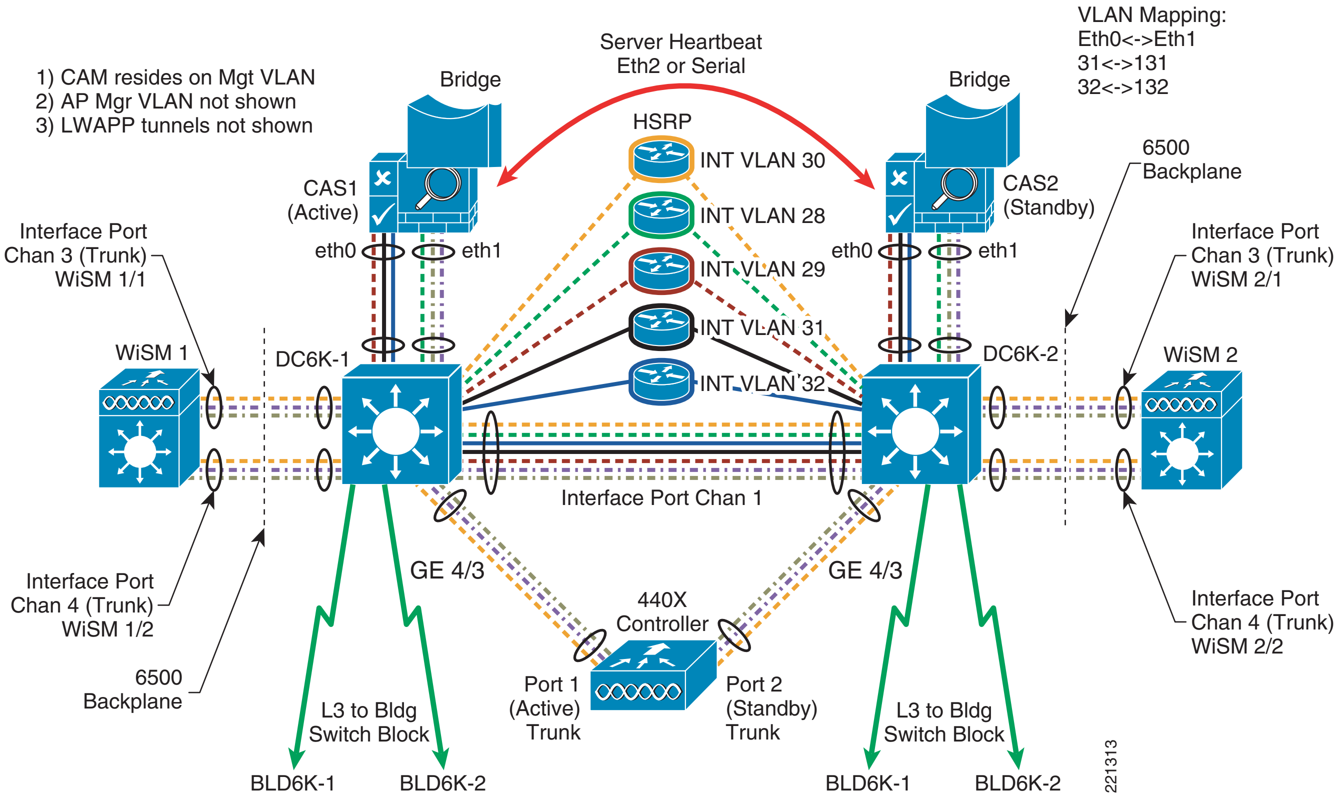
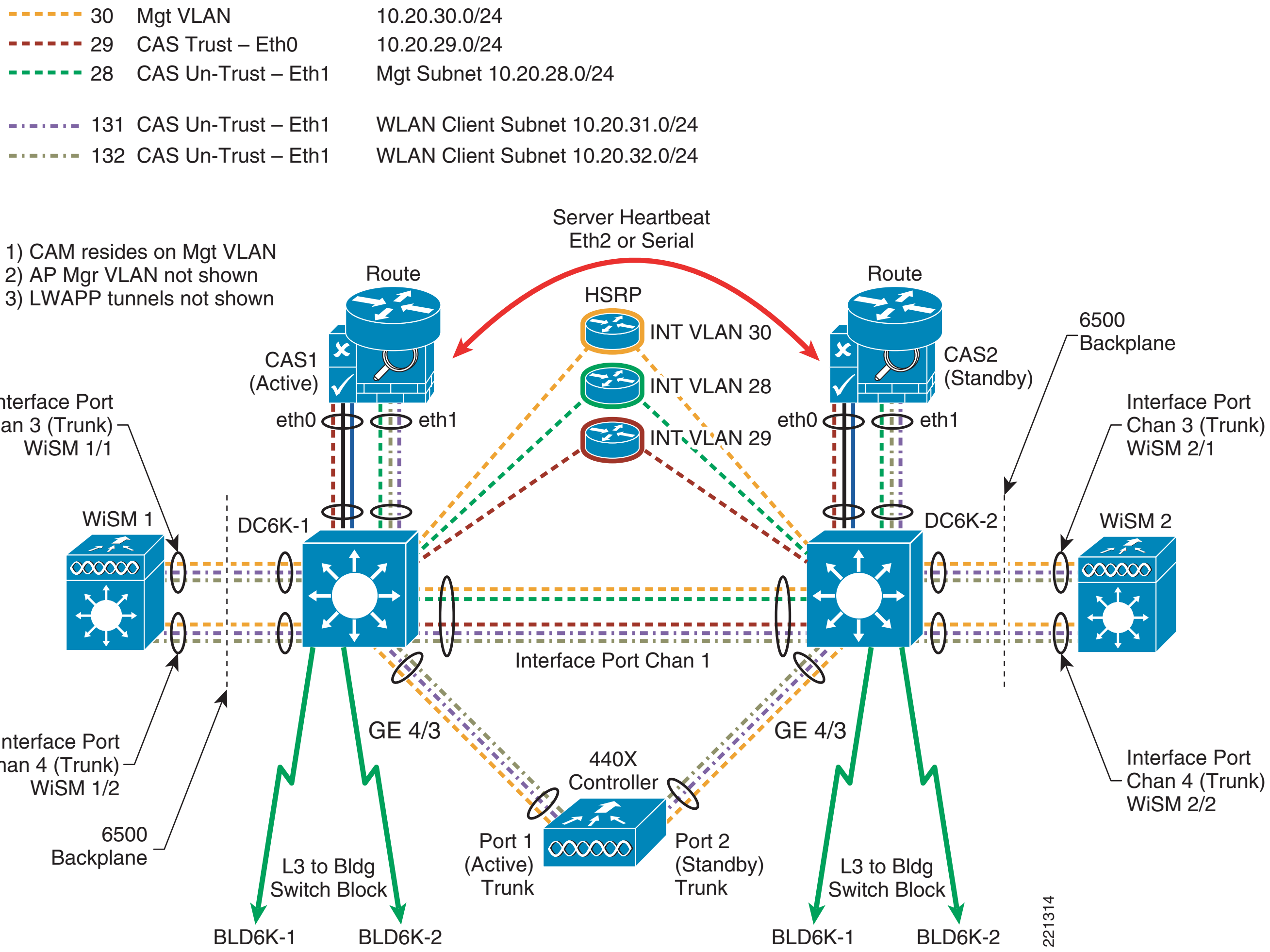


Figure 5-20 High Availability NAC/WLC Switch Block—Real IP Gateway Mode



The primary difference between the two topology examples shown pertains to where the wireless user VLANs terminate. In the case of the virtual gateway example, each user VLAN is bridged (using VLAN mapping) through the NAC appliance and terminates on its own SVI on the Catalyst switch. In the real IP gateway example, the user VLANs terminate on the untrusted interface of the NAC appliance. The appliance then forwards (routes) traffic via the trusted interface Eth0 (VLAN 29) into the network. Figure 5-21 and Figure 5-22 are simplified versions of Figure 5-19 and Figure 5-20.

Figure 5-21 Simplified Virtual Gateway Topology Example

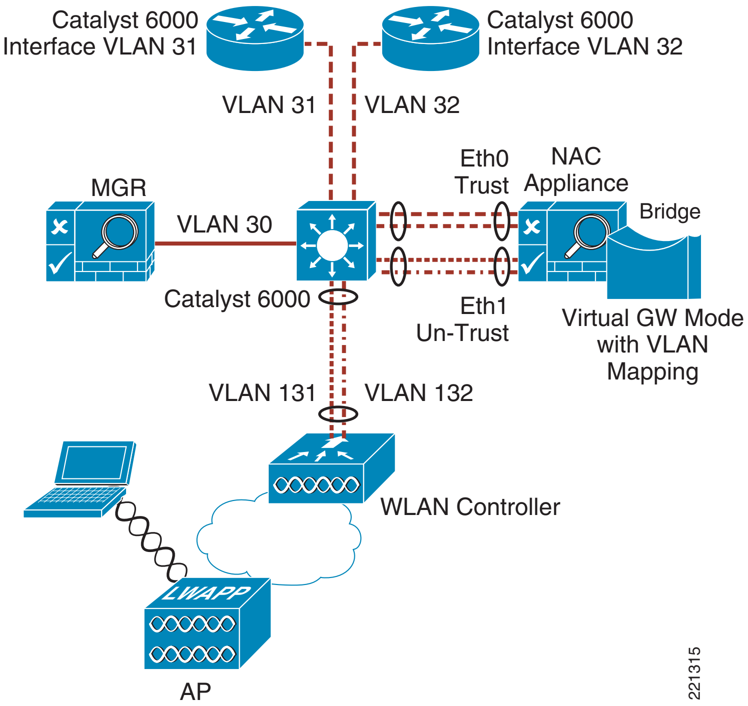
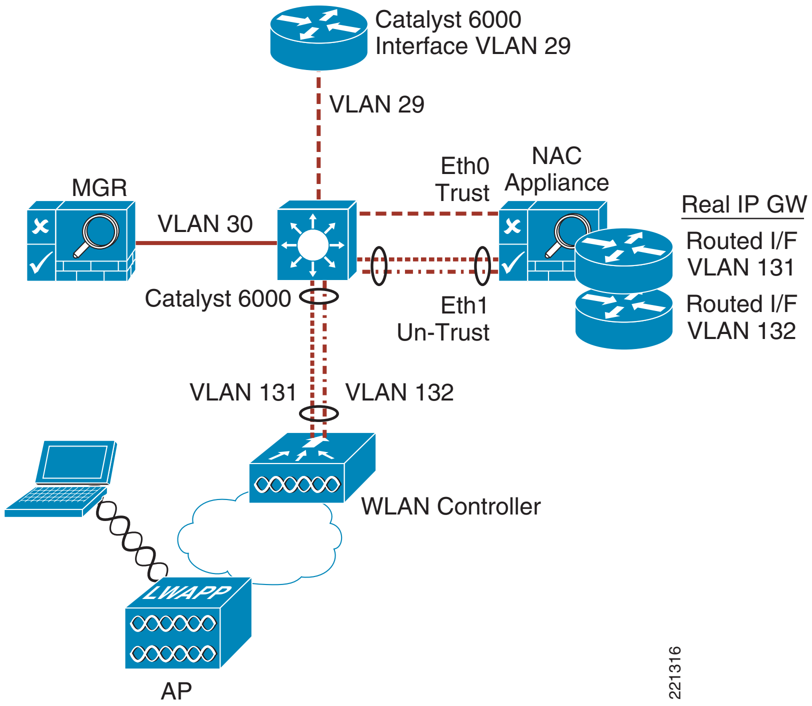


Figure 5-22 Simplified Real IP Gateway Topology Example



WLC Connectivity

Each WLC, whether standalone or a WiSM module, is connected to the switch block via 802.1q trunk(s). The WLC management and AP management interface VLANs are not trunked to the NAC appliance. These VLANs should map directly to SVIs configured for HSRP operation on the Catalyst 6000s. This allows management, RADIUS, LWAPP, and mobility tunnel traffic to avoid having to traverse through the NAC appliance.

WLC Dynamic Interface VLANs

Regardless of the gateway method of the NAC appliance, any dynamic interface (VLAN) associated with a WLAN that requires NAC services should be trunked directly to the untrusted interface (Eth1) of the NAC appliance. There should be no corresponding SVI configured on the Catalyst 6000 for those VLANs.

NAC Appliance Connectivity

Each NAC appliance is connected to the switch block via 802.1q trunks.

NAC Management VLANs

Eth0 (trusted) and Eth1 (untrusted) interfaces use a VLAN dedicated for management purposes. The Eth0 management VLAN is used for CAM/NAC communication as well as link status awareness for HA operation. The Eth1 management VLAN is used strictly for link status awareness when the NAC appliance is deployed in an HA topology.

Both Eth0 and Eth1 management VLANs should map to a SVI configured for HSRP operation on the Catalyst 6000s. The trusted-side management VLAN (Eth0) must reside on a different subnet than the CAM. If the NAC appliance is not being deployed in an HA topology, the untrusted side management VLAN/interface (Eth1) can be configured with the same IP address as the Eth0 management interface.

NAC-Wireless User VLANs

In the context of a Unified Wireless LAN deployment, the end-user VLANs are those VLANs associated with the WLC dynamic interfaces. These VLANs should be trunked directly from the WLC to the untrusted interface (Eth1) of the NAC appliance.

Virtual Gateway Mode

For each end-user VLAN that is trunked to the untrusted interface of the NAC appliance, there needs to be an associated VLAN on the trusted interface (Eth0) of the appliance (see In-Band Virtual Gateway, page 5-6). There is a 1:1 relationship between the trusted VLAN and the untrusted VLAN for a given WLAN. Each trusted-side VLAN is mapped to an SVI configured for HSRP operation on the Catalyst 6000.

Real IP Gateway Mode

In real IP gateway mode, the NAC appliance functions as a router; therefore, each end-user VLAN terminates as a routed sub-interface on the untrusted interface (Eth1) of the NAC appliance.

Inter-Switch Connectivity

For the high availability topology to work correctly, an 802.1q trunk must be established between the two "building block" Catalyst 6000s. All VLANs associated with WLC/NAC management, both untrusted and trusted traffic, must be permitted through the trunk.

Note Cisco strongly recommends that the inter-switch trunk consist of an interface port channel (representing multiple physical links between switches), not only for performance reasons, but also for reliability/resiliency of the inter-NAC appliance heartbeat link (see Inter-NAC Appliance Connectivity, page 5-28).

Inter-NAC Appliance Connectivity

Either an in-band or an out-of-band link must be established between the two appliances to facilitate stateful failover. This link is used to forward status, configuration, and synchronization information between the two platforms.

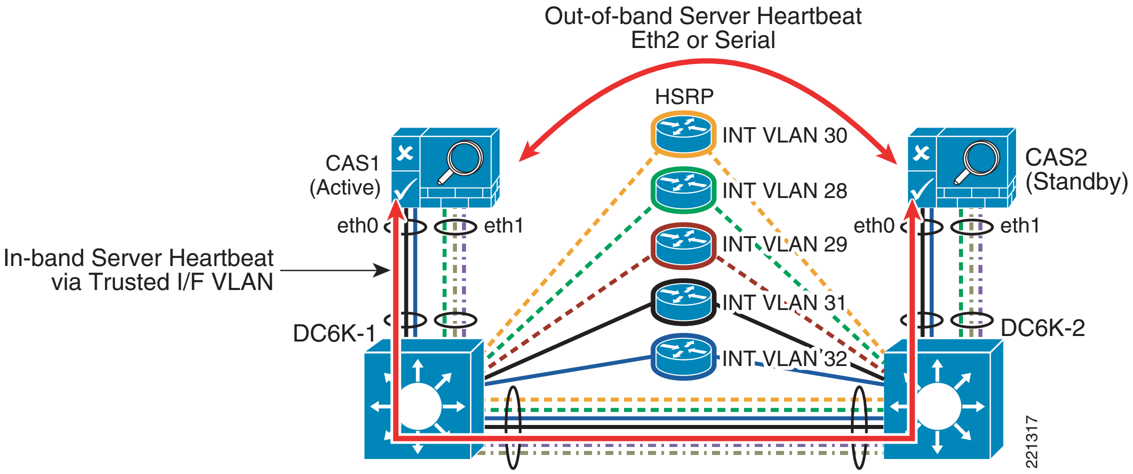
The two out-of-band options are as follows:

- Point-to-point serial connection using the console port or secondary serial port on each NAC appliance
- Point-to-point crossover Ethernet connection using a third Ethernet interface on each NAC appliance

Alternatively, a Layer 2 in-band connection can be established via the trusted management (VLAN) interface of each NAC appliance.

Note Cisco *strongly recommends* that the in-band server heartbeat method be used to eliminate the potential for a looped topology to form. See Looped Topology Prevention—Virtual Gateway Mode, page 5-29

Figure 5-23 NAC Appliance Server Heartbeat Links



Looped Topology Prevention—Virtual Gateway Mode

If an out-of-band link is used for inter-appliance communication, and for any reason that link is broken, each NAC appliance assumes an active on-line state. This in turn creates a looped Layer-2 topology across the user VLANs because per-VLAN spanning tree (PVST) BPDUs are not forwarded when the NAC appliances are bridging using the VLAN mapping method. Broadcasts originating on one or more untrusted client VLANs are forwarded through the NAC to the trusted-side VLAN and vice versa, thereby creating a broadcast storm if both NAC appliances become active at the same time.

For this reason, the in-band heartbeat method should be used. In this case, a logical IP/UDP server-to-server connection is established via the trusted management interfaces. A failure within the topology that breaks the logical server-to-server link also breaks any potential loop that would otherwise be formed as a result of both NAC appliances going into an active state at the same time.

Finally, both an in-band and out-of-band link can be used to ensure "non-revertive" behavior if the primary NAC appliance goes inactive and then becomes active again. User sessions remain on the backup NAC appliance until that server is shut down (scheduled or unscheduled), or a failure is detected on either its trusted or untrusted interface.

Note The above "looped topology" vulnerability is not applicable when the NAC appliance is deployed as a real IP gateway. However, Cisco still recommends that the same inter-appliance communication methods described above be used for real IP gateway deployments as well.

High Availability Failover Considerations

Stateful failover from an active to a standby appliance occurs if any of the following happens:

- The active appliance is re-booted.
- The active appliance fails to respond to the standby appliance heartbeat messages (application failure).
- Active appliance—Trusted interface (Eth0) physical link goes down.
- Active appliance—Trusted interface (Eth0) logical link heartbeat (ping) fails.
- Active appliance—Untrusted interface (Eth1) physical link goes down.
- Active appliance—Untrusted interface (Eth1) logical link heartbeat (ping) fails.

If any of the above occurs, the standby NAC appliance becomes active within approximately 30 seconds or less. Assuming WLAN controller SSO (VPN-SSO) has been configured and the client machines are running the Clean Access Agent software, end-user sessions are automatically restored through the backup NAC appliance. The time it takes for the solution to recover from one of the above conditions is based on two configurable timers:

- Link heartbeat timer—Monitors the link status of the trusted and untrusted interfaces. Recommended setting is 25 seconds or longer.
- Server heartbeat timer—Monitors the in-band/out-of-band server heartbeat link. Recommended setting is 15 seconds or longer.

If the NAC appliances are configured as real IP gateways, and a failure based on scenario 3 or 4 above occurs, the NAC appliances successfully failover, but clients hang. Workarounds include the following:

- Manually clear the client ARP cache (**arp -d** from Windows command line).
- Momentarily disable/enable the client WLAN adapter.

- Wait for the client default gateway ARP cache entry to time out and refresh.
- Configure the NAC appliance pair for virtual gateway operation.

Implementing Non-Redundant NAC with Unified Wireless

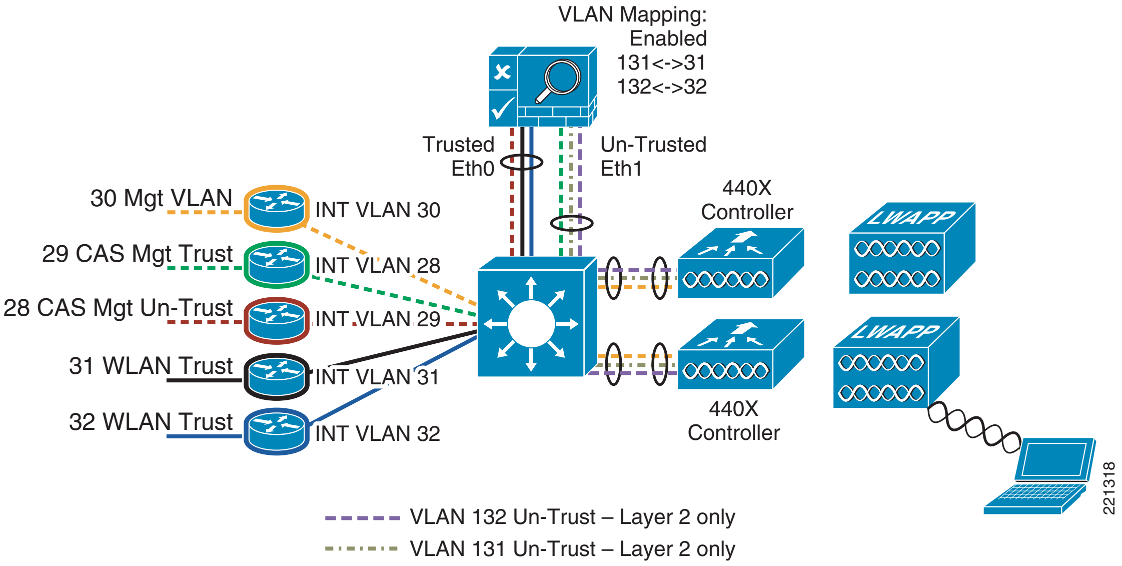
Most all of the guidelines discussed in Implementing NAC Appliance High Availability with Unified Wireless, page 5-22 also apply to implementations where only one NAC appliance is being installed. A single NAC appliance, configured for standalone operation, can be integrated into a topology that consists of a single or redundant multilayer switches:

- If a single NAC appliance is deployed as part of a redundant multilayer switch topology, all the deployment guidelines above apply except for inter-NAC appliance connectivity. This approach is not particularly desirable because there are single points of failure within the topology, but may be valid if an enterprise is looking to introduce NAC services into an existing unified wireless deployment with the intent of implementing HA in the future.
- If a single NAC appliance is deployed in conjunction with a single multilayer switch, all the deployment guidelines apply except for the following:
  - Inter-switch guidelines (see Inter-Switch Connectivity, page 5-28)
  - Inter-NAC guidelines (see Inter-NAC Appliance Connectivity, page 5-28)

All the SVIs associated with the management VLANs and end-user VLANs (virtual gateway mode) would be configured without implementing HSRP.

Figure 5-24 shows an example of a single NAC/multilayer switch topology.

Figure 5-24 Non-Redundant NAC Implementation—Virtual Gateway



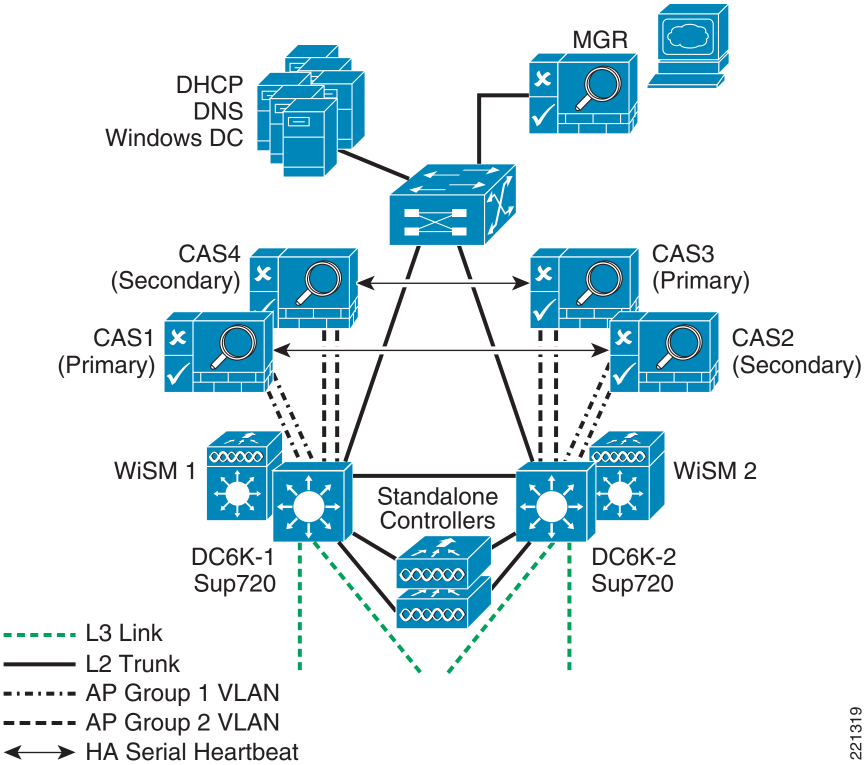
Implementing CAM High Availability

It is beyond the scope of this design guide to discuss how to implement CAM in a high availability configuration. For further details, see Chapter 16 of the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following:
http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Scaling Considerations

A single NAC appliance, assuming that it is deployed using Cisco-specified hardware (HP DL350 or equivalent), is currently capable of supporting up to 2500 concurrent users. If an enterprise anticipates having more than 2500 concurrent users, or an administrator would rather distribute users across more than one NAC appliance for performance reasons, an additional NAC appliance may be added to the switch building block in parallel with an existing deployment. Figure 5-25 shows a high-level topology example of a fully redundant, multi-NAC deployment.

Figure 5-25 Scaling NAC Appliance with Unified Wireless Deployment



Assuming that a deployment is based on the recommendations established in this design guide, the most viable method for distributing wireless users across two or more active NAC appliances is to make use of multiple dynamic interfaces in conjunction with using the WLC AP grouping feature (see Roaming with NAC Appliance and AP Groups, page 5-21). In this way, a single WLAN can be implemented across an enterprise-wide deployment while at the same time distributing user traffic (based on AP group/VLAN relationships) to a particular NAC appliance through the 802.1q trunks. This technique is applicable for either virtual or real IP gateway mode of operation.

Attention should be given to defining the AP group relationships so as to avoid situations where client roaming may involve crossing an AP group boundary between two WLCs (seeRoaming with NAC Appliance and AP Groups, page 5-21).

Integrated Wired/Wireless NAC Appliance Deployments

Because of architectural differences between Cisco WLAN Controllers and Catalyst switches, separate NAC appliances must be implemented to support an integrated wired/wireless deployment. However, a single CAM or HA CAM pair can be used to manage the NAC appliances of both networks.

NAC Appliance with Voice over WLAN Deployments

Because the NAC appliance resides "inline" to all user traffic in this design guide , WLANs that are used to support voice over WLAN (VoWLAN) applications should not be switched through the NAC appliance for the following reasons:

- The NAC appliance has no ability to prioritize VoWLAN traffic (via QoS) over other non-latency sensitive traffic.
- Multicast-based IP telephony applications cannot be supported if the NAC appliance is configured as a real IP gateway.
- Most VoWLAN handsets currently employ some form of EAP authentication for access control, and therefore do not need the authentication and access control services offered by NAC. In addition, in most cases, VoWLAN devices typically do not pose the same threat as other wireless computing devices that require endpoint security.

Therefore, Cisco recommends that separate WLANs and VLANs be dedicated to VoWLAN applications, and that the VLANs associated with a given VoWLAN do not trunk through the NAC appliance.

Multilayer Switch Building Block Considerations

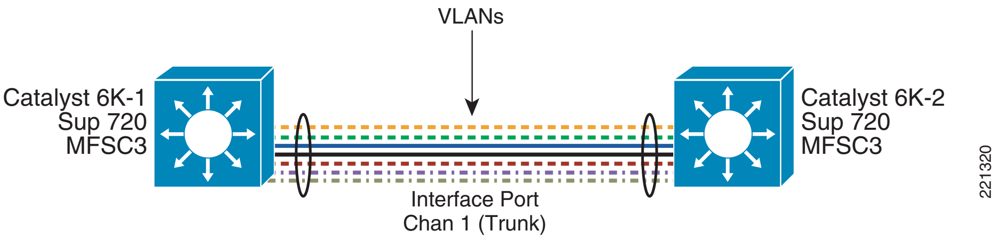
This section addresses some of the more pertinent implementation details associated with implementing a Cisco NAC appliance with the Cisco Unified Wireless solution. This section does not provide a step-by-step guide for configuring every aspect of the solution. It is assumed that the reader has a reasonably good understanding of both the Cisco Clean Access NAC appliance solution as well as the Cisco Unified Wireless solution coupled with the information offered earlier in this chapter.

The following configuration guidelines are based on the high availability NAC/Unified Wireless topology shown in Figure 5-18 and Figure 5-19. The high availability topology example is being used because it represents the recommended deployment scenario. Because of the caveats noted in Gateway Method to Use with Unified Wireless Deployments, Cisco strongly recommends that the virtual gateway method be used rather than deploying the appliances as real IP gateways. A single NAC appliance deployment is essentially identical in all aspects except where noted.

The configuration examples and screenshots are based on version 5.0.148.2 firmware image for Cisco Unified Wireless WLAN Controllers and Version 4.1.3.1 software for the Cisco NAC Appliance and Manager. The configuration sub-sections that follow are laid out in a logical progression, beginning with Layer 1 and Layer 2 device interconnect, to Layer 3 device configuration, and so on.

Figure 5-26 shows an example of a multilayer switch block.

Figure 5-26 Multilayer Switch Block



The redundant switch block in Figure 5-26 comprises two Catalyst 6500s that include Sup720/MSFC3 modules in addition to fiber and copper Gigabit port modules.

Note the following:

- The copper GigE modules are used to support connectivity to the NAC appliance servers.
- The fiber GigE modules are used for standalone controller connectivity. If only Cisco Wireless Services Modules (WiSMs) are being deployed, the fiber modules are optional
- Either fiber or copper GigE modules can be used for the inter-switch trunk.

Inter-Switch Trunk Configuration

As discussed Inter-Switch Connectivity, page 5-28, Cisco strongly recommends that the inter-switch trunk consist of two or more physical links bundled together into a port channel. Cisco also recommends that these links be established using more than one interface module in each switch, thereby ensuring that if there is a failure of an entire port module, the trunk and subsequently the heartbeat link between NAC appliances are preserved.

A port channel configuration similar to the following is defined on each Catalyst 6000:

```
interface Port-channel1

 description Channel Between C6Ks

 switchport

 switchport trunk encapsulation dot1q

 switchport trunk allowed VLAN 1-156

 switchport mode trunk

 no ip address

 !

----------------------------------snip--------------------------------

!

interface GigabitEthernet5/1

 description To DC-6K-2

 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 1-156
 switchport mode trunk
 no ip address
 channel-group 1 mode desirable
!
interface GigabitEthernet6/2
 description to DC-6K-2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 1-156
 no ip address
 channel-group 1 mode desirable
```

Note above that the port channel consists of two ports on two different modules. If restricting VLANs across the trunk, be sure to allow all VLANs associated with the NAC deployment, including but not limited to the following:

- WLC management VLAN
- WLC AP management VLAN(s)
- NAC trusted interface management VLAN
- NAC untrusted interface management VLAN
- One or more NAC untrusted-side client VLANs
- One or more NAC trusted-side client VLANs (virtual gateway mode only)

Note The port channel configuration above is not required for single appliance deployments unless it is already configured as part of an existing redundant switch block.

VLAN Configuration

The VLANs listed above must be configured on each Catalyst 6000. The WLC management and AP manager VLANs may already be configured as part of an existing Unified Wireless deployment.

Following is a sample VLAN configuration:

```
VLAN 9
 name ap-mgt !This supports AP-to-WLC LWAPP Tunnels!
!
VLAN 28
```

```
 name cas-mgt-untrust

!

VLAN 29

 name CAS-mgt-trusted

!

VLAN 30

 name DC-Mgt !This is the datacenter wide mgt VLAN - includes WLCs!

!

VLAN 31

 name client-VLAN1 !WLAN1 Client VLAN on trusted side of NAC!

!

VLAN 32

 name client-VLAN2 !WLAN2 Client VLAN on trusted side of NAC!

!

VLAN 131

 name WLAN1-CAS-Untrust !This VLAN exists between WLC's and NAC Untrusted i/f!

!

VLAN 132

 name WLAN2-CAS-Untrust !This VLAN exists between WLC's and NAC untrusted i/f!

!
```

VLANs 31 and 32 above represent trusted-side VLANs that are mapped to VLAN 131 and 132 respectively when the NAC appliance is configured as a virtual gateway with VLAN mapping.

SVI Configuration

It is assumed that before deployment, a network administrator has identified the subnets and addressing scheme needed to configure the switched virtual interfaces (SVIs) on each of the Catalyst 6000s. (See Figure 5-27.)

Figure 5-27 Switching Block—SVIs

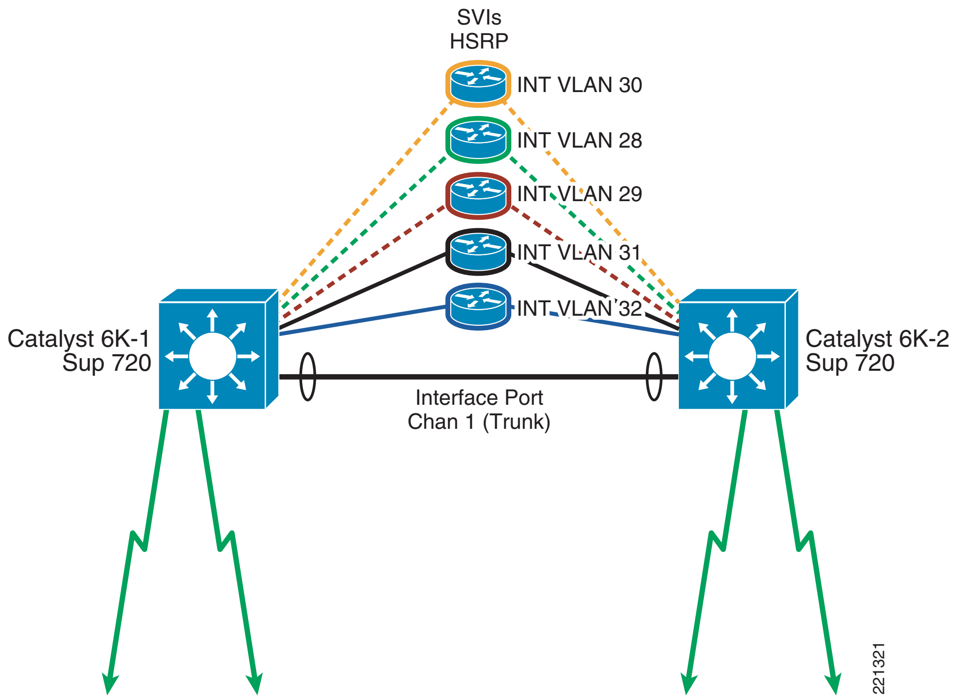


Figure 5-27 represents only a subset of the total number of SVIs that may actually exist in a campus deployment. The SVIs shown are an example of what is required to support a high availability (HA) NAC deployment.

Note AP Manager SVI is not shown in Figure 5-27.

The following is a sample SVI configuration for the following items:

- AP management VLAN 9
- Data center management VLAN 30
- NAC trusted management VLAN 29
- NAC untrusted management VLAN 28
- WLAN1 client trusted VLAN 31 (virtual gateway mode only)
- WLAN2 client trusted VLAN 32 (virtual gateway mode only)

```
interface VLAN9

 description Datacenter Controller AP Management VLAN

 ip address 10.15.9.2 255.255.255.0
 standby 121 ip 10.15.9.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN28
 description CAS-MGT-Untrust
 ip address 10.20.28.253 255.255.255.0
 standby 121 ip 10.20.28.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN29
 description CAS-MGT-Trust
 ip address 10.20.29.253 255.255.255.0
 standby 121 ip 10.20.29.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN30
 description DC Management Subnet
 ip address 10.20.30.4 255.255.255.0
 ip helper-address 10.20.30.11
 standby 121 ip 10.20.30.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN31
 description WLAN1 Client Subnet
 ip address 10.20.31.2 255.255.255.0

 standby 121 ip 10.20.31.1

 standby 121 timers msec 250 msec 750

 standby 121 priority 105

 standby 121 preempt delay minimum 180

!

interface VLAN32

 description WLAN2 Client Subnet

 ip address 10.20.32.2 255.255.255.0

 standby 121 ip 10.20.32.1

 standby 121 timers msec 250 msec 750

 standby 121 priority 105

 standby 121 preempt delay minimum 180
```

The following is the reciprocal configuration for Cat6K-2:

```
interface VLAN9

 description Datacenter Controller AP Management VLAN

 ip address 10.15.9.3 255.255.255.0

 standby 121 ip 10.15.9.1

 standby 121 timers msec 250 msec 750

!

interface VLAN28

 description CAS-MGT-Untrust

 ip address 10.20.28.254 255.255.255.0

 standby 121 ip 10.20.28.1

 standby 121 timers msec 250 msec 750

!

interface VLAN29

 description CAS-MGT-Trust

 ip address 10.20.29.254 255.255.255.0

 standby 121 ip 10.20.29.1

 standby 121 timers msec 250 msec 750

!
```

```
interface VLAN30

 description DC Management Subnet

 ip address 10.20.30.5 255.255.255.0

 ip helper-address 10.20.30.11

 standby 121 ip 10.20.30.1

 standby 121 timers msec 250 msec 750

!

interface VLAN31

 description WLAN1 Client VLAN

 ip address 10.20.31.3 255.255.255.0

 standby 121 ip 10.20.31.1

 standby 121 timers msec 250 msec 750

!

interface VLAN32

 description WLAN2 Client VLAN

 ip address 10.20.32.3 255.255.255.0

 standby 121 ip 10.20.32.1

 standby 121 timers msec 250 msec 750
```

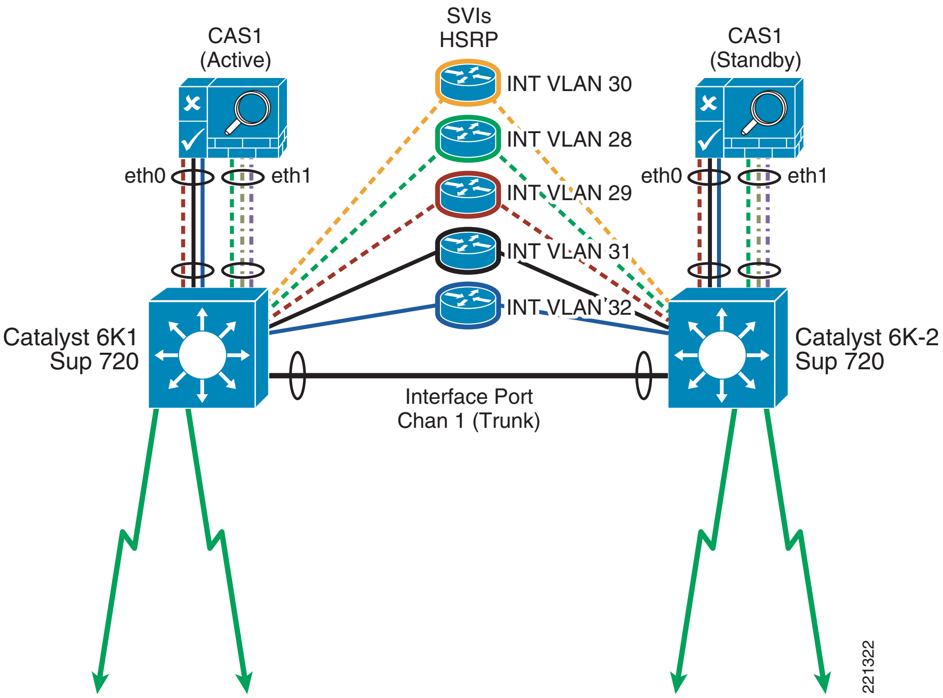
Note There are no SVIs created for the untrusted client VLANs (131 and 132).

Note If the NAC appliance deployment is non-redundant but the switch block is, HSRP is still required. Otherwise, if the switch block is non-redundant, the HSRP configuration parameters are not required.

NAC Appliance Configuration Considerations

When deploying the NAC appliances as a high availability (HA) pair, Cisco strongly recommends that you do not connect the untrusted interfaces to the network until you have completely finished configuration (see Figure 5-28). This is to prevent loops from forming in the topology during the configuration process.

Figure 5-28 NAC Appliance HA Pair



NAC Appliance Initial Configuration

For initial configuration guidelines, see Chapter 4 of the *Cisco NAC Appliance—Clean Access Server Installation and Administration Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Among other things, the NAC appliance configuration script utility guides you through the configuration of the trusted and untrusted interfaces for each appliance. Remember the following points:

- The management IP address used for the trusted interface Eth0 of each appliance must be on a different subnet than the IP address of the NAC appliance manager (CAM).
- When you are deploying the NAC appliance in an HA configuration, you need to configure a management IP address (on a different subnet) for the untrusted interface Eth1. If you are deploying only one NAC appliance, the IP address of the Eth1 can be the same as Eth0.
- Remember that if either management interface is associated with a particular VLAN ID, be sure you enable Management VLAN Tagging (when prompted during the setup script process), and set the VLAN ID during the configuration script process. Otherwise, you will not be able to access the appliance through its web interface or the CAM.

- When deploying the NAC appliance in an HA configuration, service addresses or virtual IPs are configured to represent the HA pair as a single logical appliance. During the address planning phase of a deployment, network administrators should keep in mind that three IP addresses are required for the trusted interface pair between NAC appliances and three IP addresses are also needed for the untrusted interface pair. The Service IPs are configured later after the appliances are connected to the network.
- A shared secret is used to protect communication between the CAM and the NAC appliance. It must be configured exactly the same, or the CAM is not able to communicate with the appliance.
- A temporary certificate based on the trusted IP address of Eth0 or hostname for Eth0 must be created. This is changed later to represent the service IP address/hostname of the H/A pair.

NAC Appliance Switch Connectivity

When an initial configuration is established, the appliances can be connected to the switch block. Only Eth0 (trusted interface) should be connected until the NAC appliances have been completely configured. The switch ports to which the appliances connect need to be configured as trunk ports. Following is a sample switch port configuration for the Eth0 and Eth1 appliance interfaces, and is applied to both switches:

```
interface FastEthernet1/1

 description CAS-Trusted

 switchport

 switchport trunk encapsulation dot1q

 switchport trunk native VLAN 999

 switchport trunk allowed VLAN 29,31,32

 switchport mode trunk

 no ip address

!

interface FastEthernet1/2

 description CAS-Untrusted

 switchport

 switchport trunk encapsulation dot1q

 switchport trunk native VLAN 998

 switchport trunk allowed VLAN 28,131,132

 switchport mode trunk

 no ip address
```

In the configuration above, each trunk is configured to allow only those VLANs necessary to support the NAC deployment. FastEthernet 1/1 supports the NAC appliance trusted interface, which includes the management VLAN, and two trusted-side client VLANs (see VLAN Configuration, page 5-34). FastEthernet 1/2 supports the NAC appliance untrusted management VLAN in addition to the two untrusted-side client VLANs.

Note The examples above are FastEthernet interfaces; however, in an actual NAC appliance deployment, these would be Gigabit Ethernet interfaces.

NAC Appliance HA Server Configuration

After the appliances are connected, and assuming that logical connectivity exists to the trusted management interfaces, you can open a web browser and connect directly to the web management interface of each server, from which you can configure the advanced options needed to support an HA deployment.

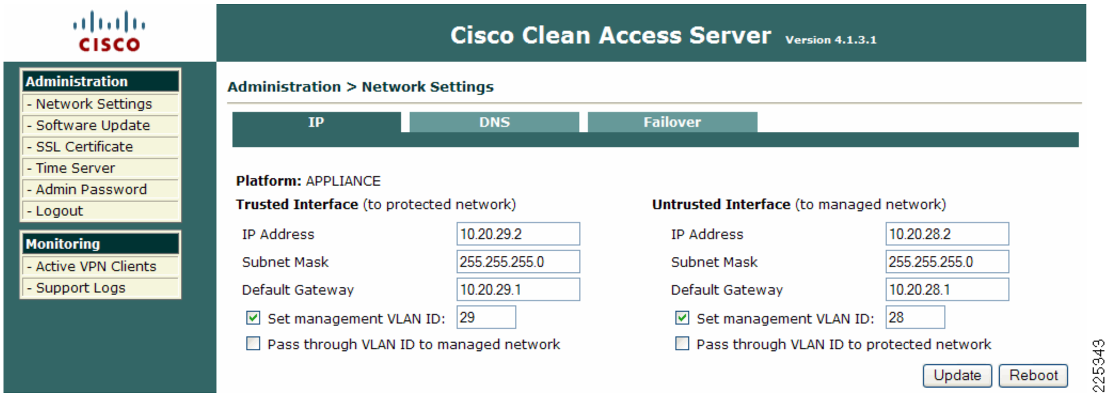
Note The following steps are not required for single appliance deployments.

Step 1 Connect to the appliance by opening a web browser and then entering the trusted interface management IP or host name as follows:

```
https://<trusted mgt IP>/admin/
```

The Network Settings screen appears, as shown in Figure 5-29, and shows a summary of the appliance interface configuration.

Figure 5-29 NAC Appliance Network Settings



Platform: APPLIANCE

Trusted Interface (to protected network)

IP Address: 10.20.29.2
Subnet Mask: 255.255.255.0
Default Gateway: 10.20.29.1
☑ Set management VLAN ID: 29
☐ Pass through VLAN ID to managed network

Untrusted Interface (to managed network)

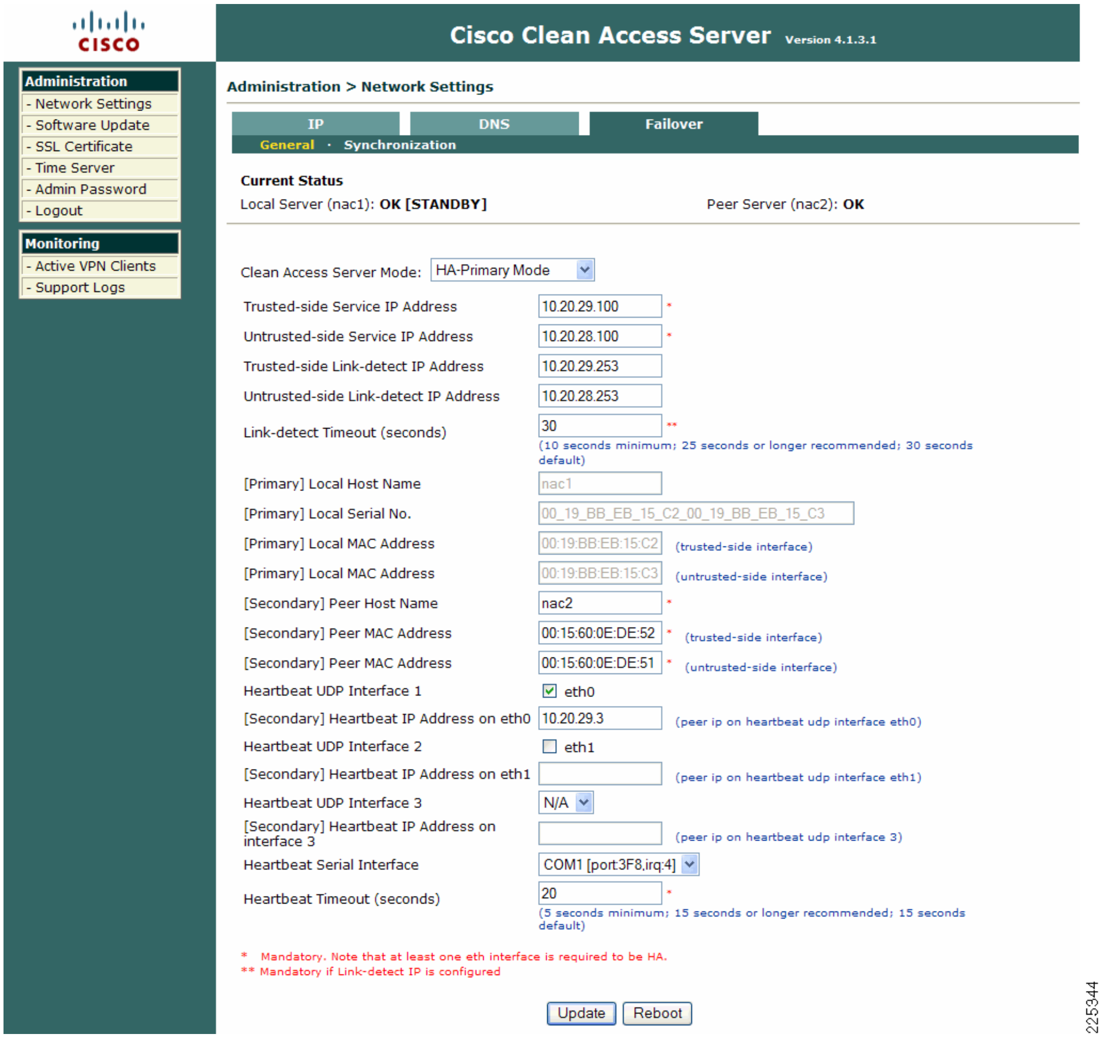
IP Address: 10.20.28.2
Subnet Mask: 255.255.255.0
Default Gateway: 10.20.28.1
☑ Set management VLAN ID: 28
☐ Pass through VLAN ID to protected network

Step 2 Click the **Failover** tab to navigate to the HA settings of the appliance. The appliance initially starts up in standalone mode.

Step 3 Select **HA Primary Mode**, click **Update**, and then click **Reboot**.

Step 4 After the appliance reboots, reconnect and navigate to the **Failover** tab, where the HA configuration settings are displayed, as shown in Figure 5-30.

Figure 5-30 NAC Appliance HA—Primary Configuration Settings



Cisco Clean Access Server Version 4.1.3.1

Administration
- Network Settings
- Software Update
- SSL Certificate
- Time Server
- Admin Password
- Logout

Monitoring
- Active VPN Clients
- Support Logs

Administration > Network Settings

IP | DNS | Failover

General · Synchronization

Current Status

Local Server (nac1): **OK [STANDBY]** Peer Server (nac2): **OK**

Clean Access Server Mode:	HA-Primary Mode
Trusted-side Service IP Address	10.20.29.100 *
Untrusted-side Service IP Address	10.20.28.100 *
Trusted-side Link-detect IP Address	10.20.29.253
Untrusted-side Link-detect IP Address	10.20.28.253
Link-detect Timeout (seconds)	30 ** (10 seconds minimum; 25 seconds or longer recommended; 30 seconds default)
[Primary] Local Host Name	nac1
[Primary] Local Serial No.	00_19_BB_EB_15_C2_00_19_BB_EB_15_C3
[Primary] Local MAC Address	00:19:BB:EB:15:C2 (trusted-side interface)
[Primary] Local MAC Address	00:19:BB:EB:15:C3 (untrusted-side interface)
[Secondary] Peer Host Name	nac2 *
[Secondary] Peer MAC Address	00:15:60:0E:DE:52 * (trusted-side interface)
[Secondary] Peer MAC Address	00:15:60:0E:DE:51 * (untrusted-side interface)
Heartbeat UDP Interface 1	☑ eth0
[Secondary] Heartbeat IP Address on eth0	10.20.29.3 (peer ip on heartbeat udp interface eth0)
Heartbeat UDP Interface 2	☐ eth1
[Secondary] Heartbeat IP Address on eth1	(peer ip on heartbeat udp interface eth1)
Heartbeat UDP Interface 3	N/A
[Secondary] Heartbeat IP Address on interface 3	(peer ip on heartbeat udp interface 3)
Heartbeat Serial Interface	COM1 [port:3F8,irq:4]
Heartbeat Timeout (seconds)	20 * (5 seconds minimum; 15 seconds or longer recommended; 15 seconds default)

* Mandatory. Note that at least one eth interface is required to be HA.
** Mandatory if Link-detect IP is configured

Step 5 Repeat the steps above to configure the other NAC appliance for HA-secondary mode. Figure 5-30 shows a list of configuration parameters associated with enabling HA failover between the NAC appliances. Following is a summary of the parameters and considerations to make when configuring HA:

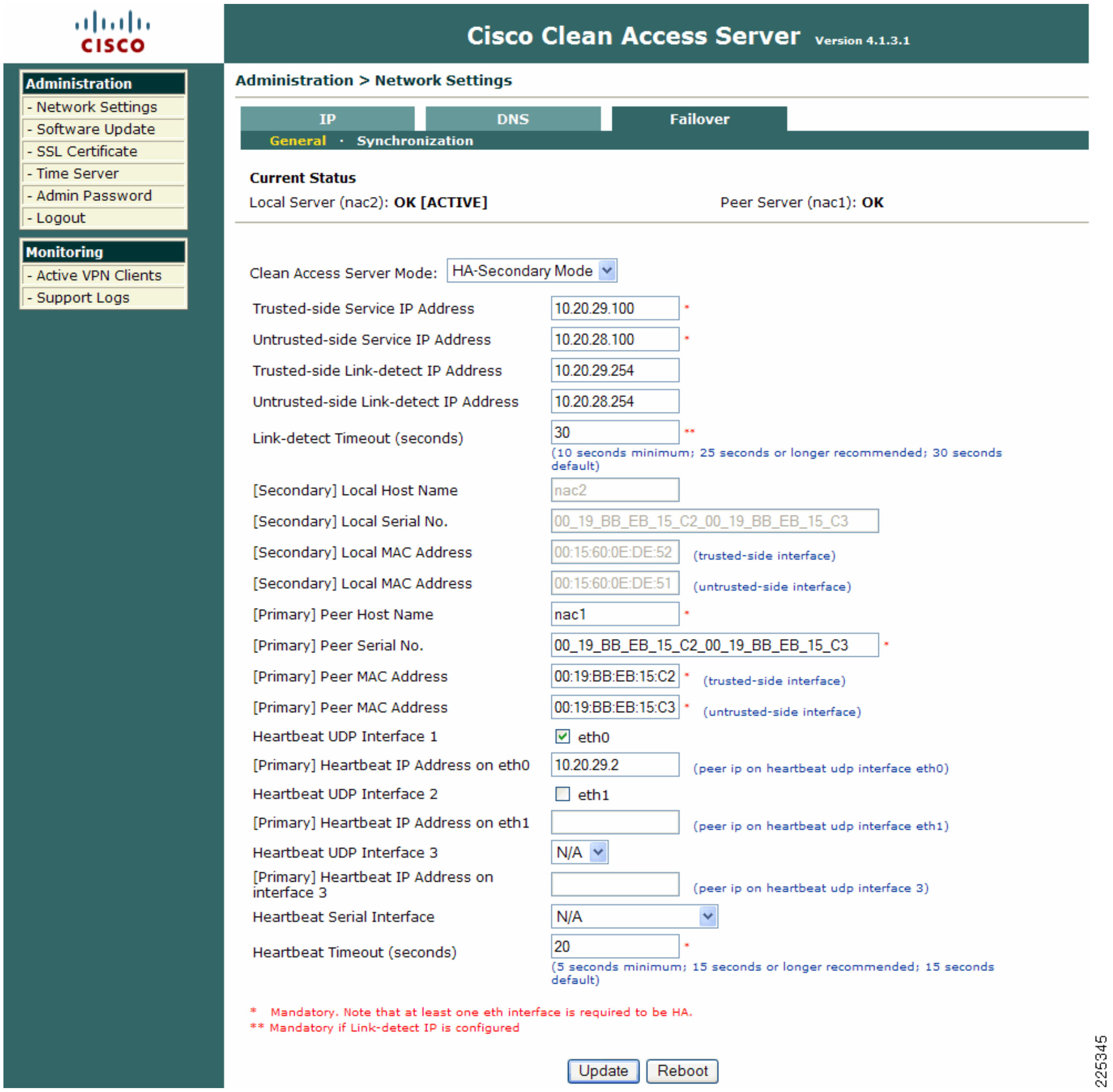
- Server mode—One server is configured as HA-primary mode and the other is configured as HA-secondary mode.
- Trusted-side service IP address—Virtual IP address that represents the logical NAC pair when in HA mode of operation. It is analogous to a standby IP in HSRP configurations.
- Untrusted-side service IP address—Virtual IP address that represents the logical NAC pair on the untrusted side of the appliance.
- Trusted-side link detect IP address—IP address that the appliance pings to verify the link status of the trusted port. The IP address used should be the HSRP standby IP address of the trusted management subnet. See interface VLAN 29 configuration in SVI Configuration, page 5-36.
- Untrusted-side link detect IP address—This is an IP address that the appliance pings to verify the link status of the untrusted port. The IP address used should be the HSRP standby IP address of the untrusted management subnet. See interface VLAN 28 configuration in SVI Configuration, page 5-36.

- Link detect timeout
- [Primary] Local Host Name, Local Serial Number, Local MAC Untrusted, and Local MAC Trusted—These fields are pre-populated.
- [Secondary] Peer Host Name, Peer Serial Number, Peer MAC Untrusted, and Peer MAC Trusted—This information can be obtained from the other NAC appliance HA-secondary mode configuration settings.
- Heartbeat UDP interface—This is the interface through which the appliance checks for the status/health of the peer server. Cisco strongly recommends that this be set to Eth0 (trusted interface).
- Secondary heartbeat address—IP address of the trusted management interface (not the service IP) of the peer appliance.
- Heartbeat serial interface—This interface should be used in addition to the heartbeat UDP interface, but not by itself. A crossover (null) modem cable is connected to the applicable serial interface of each appliance.
- Heartbeat timeout

Step 6 After all settings have been made, click **Update** and then **Reboot**.

Step 7 Repeat the configuration above for the NAC appliance that serves as the secondary (standby) server. See Figure 5-31 for a reciprocal HA configuration example used for the secondary NAC appliance.

Figure 5-31 NAC Appliance HA-Secondary Configuration



Current Status

Local Server (nac2): **OK [ACTIVE]** Peer Server (nac1): **OK**

Clean Access Server Mode:	HA-Secondary Mode	
Trusted-side Service IP Address	10.20.29.100	*
Untrusted-side Service IP Address	10.20.28.100	*
Trusted-side Link-detect IP Address	10.20.29.254	
Untrusted-side Link-detect IP Address	10.20.28.254	
Link-detect Timeout (seconds)	30	** (10 seconds minimum; 25 seconds or longer recommended; 30 seconds default)
[Secondary] Local Host Name	nac2	
[Secondary] Local Serial No.	00_19_BB_EB_15_C2_00_19_BB_EB_15_C3	
[Secondary] Local MAC Address	00:15:60:0E:DE:52	(trusted-side interface)
[Secondary] Local MAC Address	00:15:60:0E:DE:51	(untrusted-side interface)
[Primary] Peer Host Name	nac1	*
[Primary] Peer Serial No.	00_19_BB_EB_15_C2_00_19_BB_EB_15_C3	*
[Primary] Peer MAC Address	00:19:BB:EB:15:C2	* (trusted-side interface)
[Primary] Peer MAC Address	00:19:BB:EB:15:C3	* (untrusted-side interface)
Heartbeat UDP Interface 1	☑ eth0	
[Primary] Heartbeat IP Address on eth0	10.20.29.2	(peer ip on heartbeat udp interface eth0)
Heartbeat UDP Interface 2	☐ eth1	
[Primary] Heartbeat IP Address on eth1		(peer ip on heartbeat udp interface eth1)
Heartbeat UDP Interface 3	N/A	
[Primary] Heartbeat IP Address on interface 3		(peer ip on heartbeat udp interface 3)
Heartbeat Serial Interface	N/A	
Heartbeat Timeout (seconds)	20	* (5 seconds minimum; 15 seconds or longer recommended; 15 seconds default)

* Mandatory. Note that at least one eth interface is required to be HA.
** Mandatory if Link-detect IP is configured

Self-Signed Certificate for HA Deployment

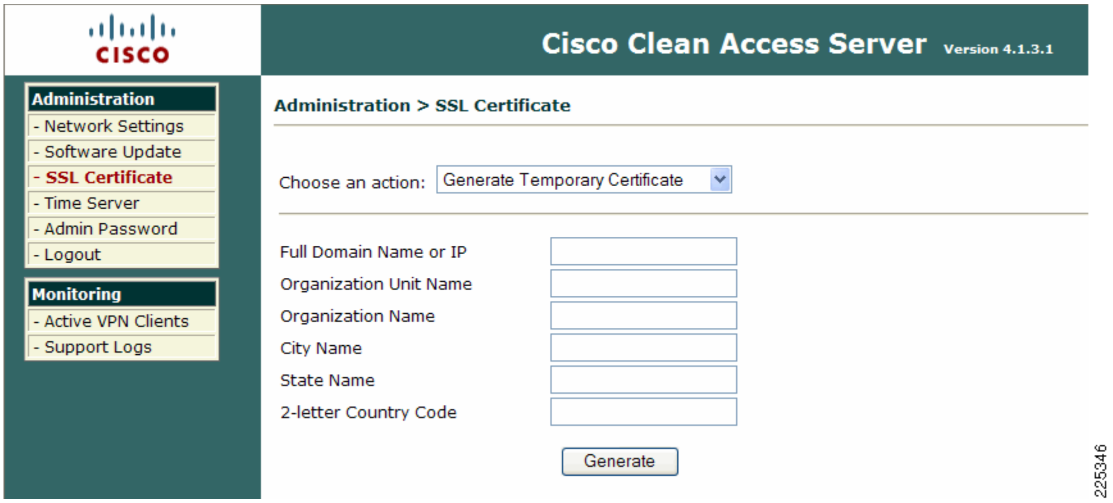
When a NAC appliance is configured for the first time, the installation script asks whether you want to create a temporary self-signed certificate. If so, the certificate is typically created using the IP address or host name of the trusted interface, Eth0. This self-signed certificate is used to establish an SSL session with end users during HTTP redirect to the NAC appliance for authentication and posture assessment or when the Clean Access desktop agent connects to the appliance for authentication and policy assessment. An imported certificate can also be installed on the appliance(s).

When a pair of NAC appliances are configured for an HA deployment, the temporary certificate may need to be re-generated to reflect the service IP address of the appliance pair. Alternatively, if using a hostname, DNS may need to be updated to reflect the service IP address.

If an IP address is used for the certificate, you can generate a new temporary certificate based on the service IP by selecting SSL certificate from the left-hand menu bar of the NAC appliance web management GUI (see Figure 5-32).

Repeat the process for the other appliance, making sure to use the same hostname or service IP address.

Figure 5-32 Temporary SSL Certificate Generation



Administration > SSL Certificate

Choose an action: Generate Temporary Certificate

Full Domain Name or IP

Organization Unit Name

Organization Name

City Name

State Name

2-letter Country Code

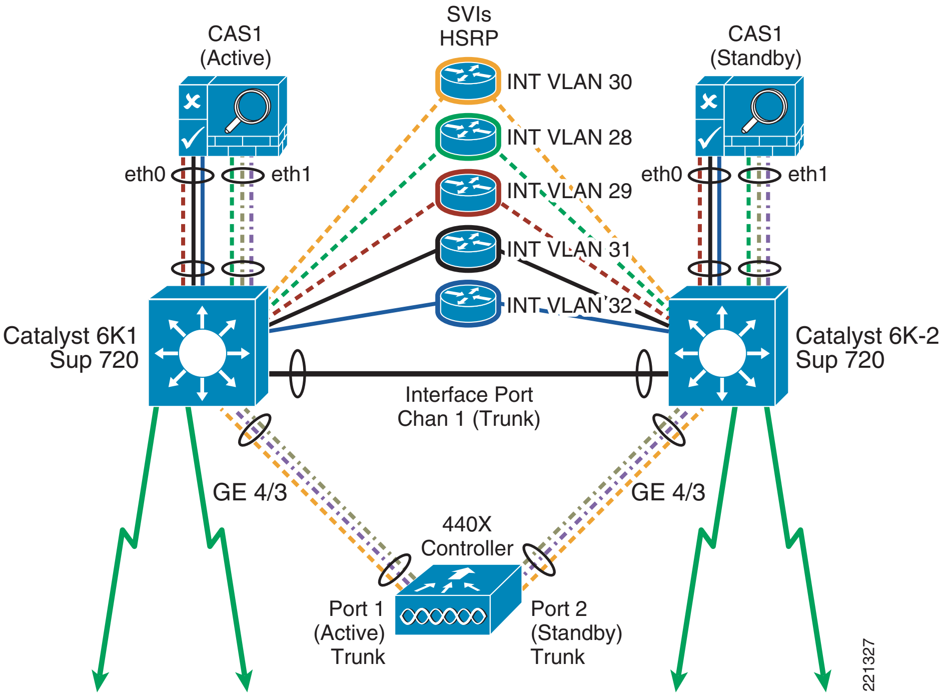
Note in Figure 5-32 that the SSL Certificate Domain is the trusted-side service IP address from the HA configuration in Figure 5-30.

Standalone WLAN Controller Deployment with NAC Appliance

For detailed configuration guidelines for the Cisco 4400 series WLAN Controllers, see the following documentation: http://www.cisco.com/en/US/partner/products/ps6366/products_configuration_guide_book09186a00806b0077.html

Two options exist when deploying standalone WLCs into the switch block (see Figure 5-33).

Figure 5-33 Standalone WLC/Switch Block



The Cisco 4402 Series WLCs offer two Gigabit Ethernet ports, whereas the 4404 Series WLCs offer four Gigabit Ethernet ports. Options include the following:

- For a Distribution Layer with a single switch, install the 4402/04 with all ports connected to one switch, and configure the WLC ports for link aggregation (LAG) mode and their associated Catalyst switch ports as a port channel. This is the best option if there is only one Catalyst switch in the WLC/NAC switching block.
- For a Distribution Layer with the recommended redundant switches, Install the 4402/04 with one port (pair of ports in the case of 4404) connected to one switch, and the other port (or pair of ports for the 4404) connected to the other switch block, in a dual-homed scenario. If this method is chosen, primary and backup ports can be designated for the management and dynamic interfaces configured on the WLC.

The controller shown in Figure 5-33 represents a 4402 that is dual-homed to a redundant switch block. The following is an example of the switch port configuration on each Catalyst 6000:

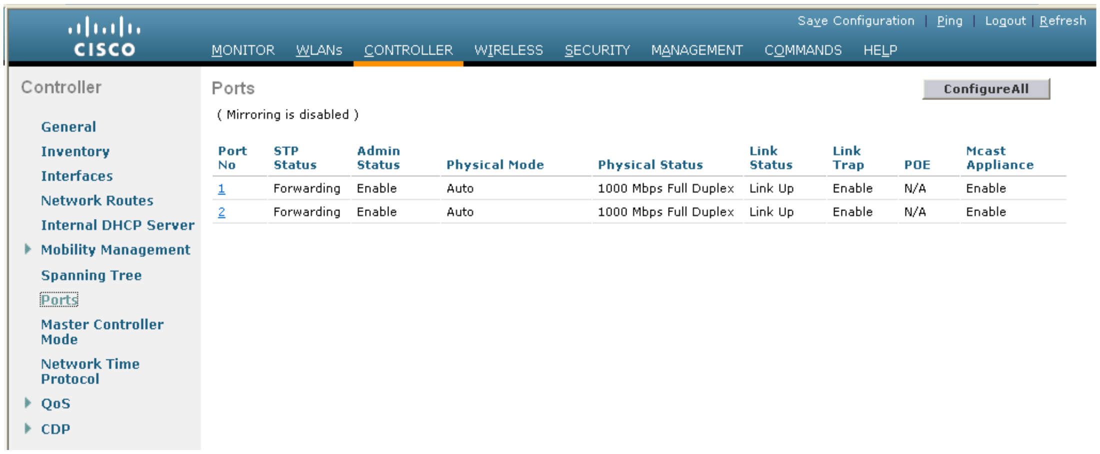
```
Cat6K-1

interface GigabitEthernet4/3

 description To WLC#3 Port 1

 switchport

 switchport trunk encapsulation dot1q

 switchport mode trunk

 no ip address
DC6K-2
```

```
interface GigabitEthernet4/3
 description To WLC#3 Port 2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
```

WLC Port and Interface Configuration

When the WLC physical ports are dual-homed, the associated management and dynamic interfaces can be mapped to one port or the other. Both physical ports can be active, supporting dynamic interfaces while at the same time serving as a backup port for a different dynamic or management interface. Figure 5-34 shows the WLC port status.

Figure 5-34 WLC Port Summary



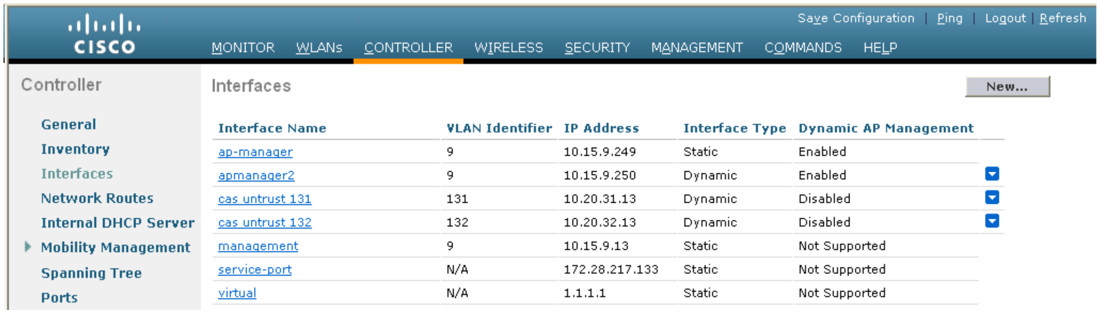
Ports

(Mirroring is disabled)

Port No	STP Status	Admin Status	Physical Mode	Physical Status	Link Status	Link Trap	POE	Mcast Appliance
1	Forwarding	Enable	Auto	1000 Mbps Full Duplex	Link Up	Enable	N/A	Enable
2	Forwarding	Enable	Auto	1000 Mbps Full Duplex	Link Up	Enable	N/A	Enable

Figure 5-35 shows a summary of management and dynamic interfaces configured on the WLC.

Figure 5-35 WLC Interface Summary



Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	9	10.15.9.249	Static	Enabled
apmanager2	9	10.15.9.250	Dynamic	Enabled
cas untrust 131	131	10.20.31.13	Dynamic	Disabled
cas untrust 132	132	10.20.32.13	Dynamic	Disabled
management	9	10.15.9.13	Static	Not Supported
service-port	N/A	172.28.217.133	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

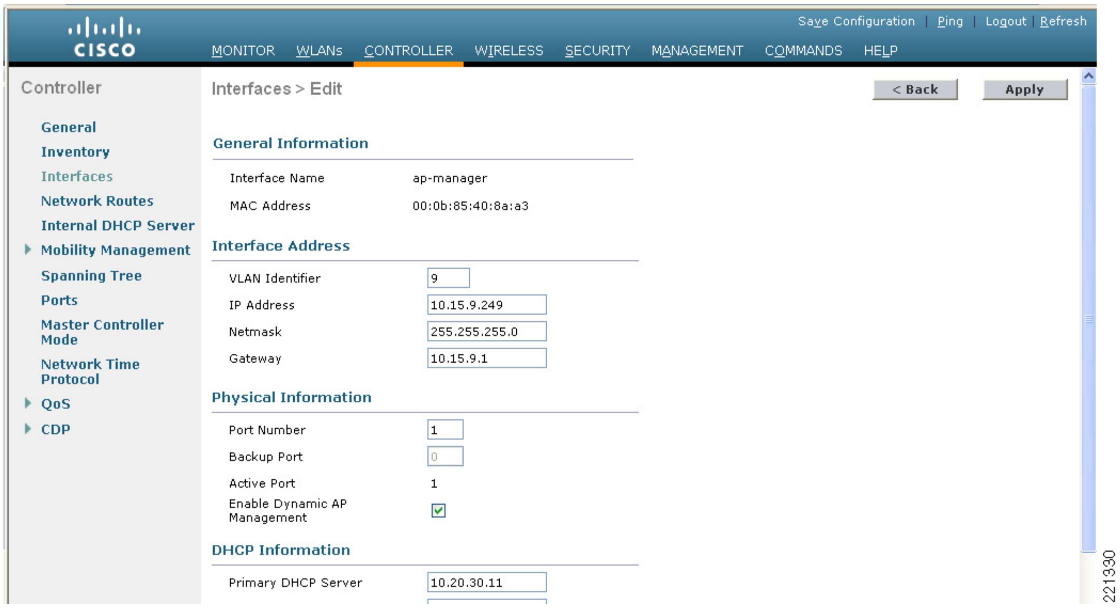
Note in Figure 5-35 that there are two AP manager interfaces; one is static and the other dynamic. The static AP manager interface represents the default AP manager interface. It cannot be deleted and is mandatory for proper operation of the Unified Wireless solution.

AP Manager Interfaces

The static AP manager interface can be assigned to only one port. It cannot be assigned a backup port. Therefore, if the WLC port or Catalyst switch interface supporting the static AP manager interface goes down, all APs joined to that controller rejoin a different controller based on their controller priority settings.

To work around this, a second dynamic interface is configured to support AP management, which is subsequently assigned to the other physical WLC port. The WLC now has an AP manager interface assigned to each physical port. If one of the ports fails, an AP manager interface is still available (see Figure 5-36 and Figure 5-37).

Figure 5-36 Static AP Manager Interface Configuration



Interfaces > Edit

General Information

Interface Name ap-manager
MAC Address 00:0b:85:40:8a:a3

Interface Address

VLAN Identifier 9
IP Address 10.15.9.249
Netmask 255.255.255.0
Gateway 10.15.9.1

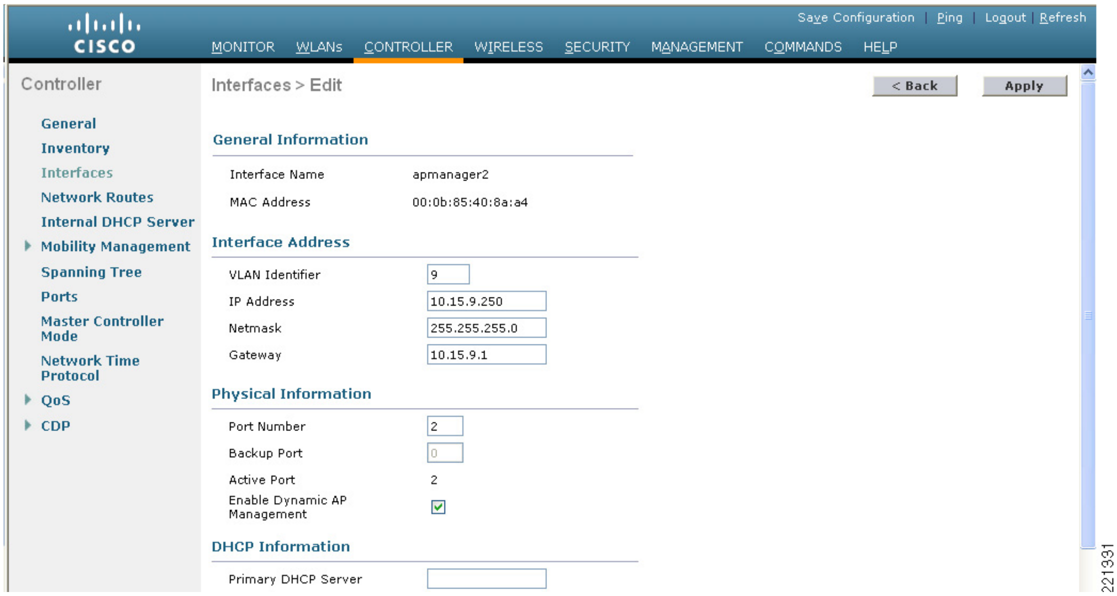
Physical Information

Port Number 1
Backup Port 0
Active Port 1
Enable Dynamic AP Management ☑

DHCP Information

Primary DHCP Server 10.20.30.11

Figure 5-37 Dynamic AP Manager Interface Configuration



Interfaces > Edit

General Information

Interface Name	apmanager2
MAC Address	00:0b:85:40:8a:a4

Interface Address

VLAN Identifier	9
IP Address	10.15.9.250
Netmask	255.255.255.0
Gateway	10.15.9.1

Physical Information

Port Number	2
Backup Port	0
Active Port	2
Enable Dynamic AP Management	☑

DHCP Information

Primary DHCP Server	

WLAN Client Interfaces

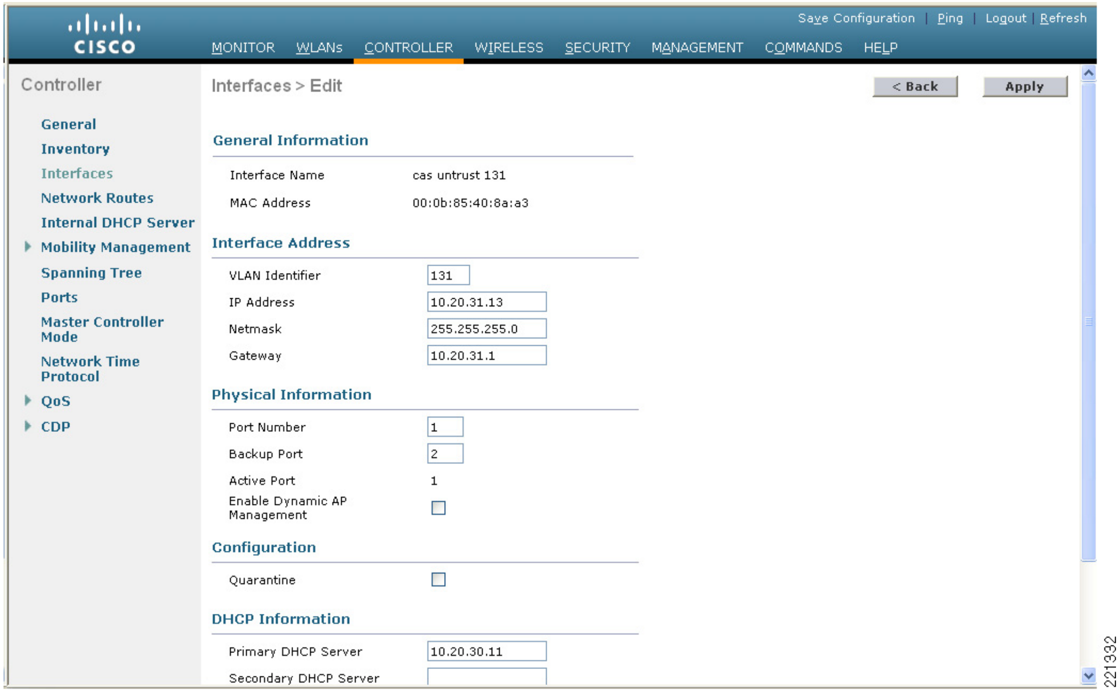
Dynamic interface/VLANs that support WLAN clients can be assigned to either physical port on the WLC. These interfaces can also have a backup port assigned to them.

In Figure 5-35, the following two WLAN client interfaces are configured:

- Clean access untrust 131
- Clean access untrust 132

Figure 5-38 and Figure 5-39 show an example configuration for each dynamic interface.

Figure 5-38 "cas untrust 131"Dynamic Interface Configuration



Interfaces > Edit

General Information

Interface Name	cas untrust 131
MAC Address	00:0b:85:40:8a:a3

Interface Address

VLAN Identifier	131
IP Address	10.20.31.13
Netmask	255.255.255.0
Gateway	10.20.31.1

Physical Information

Port Number	1
Backup Port	2
Active Port	1
Enable Dynamic AP Management	□

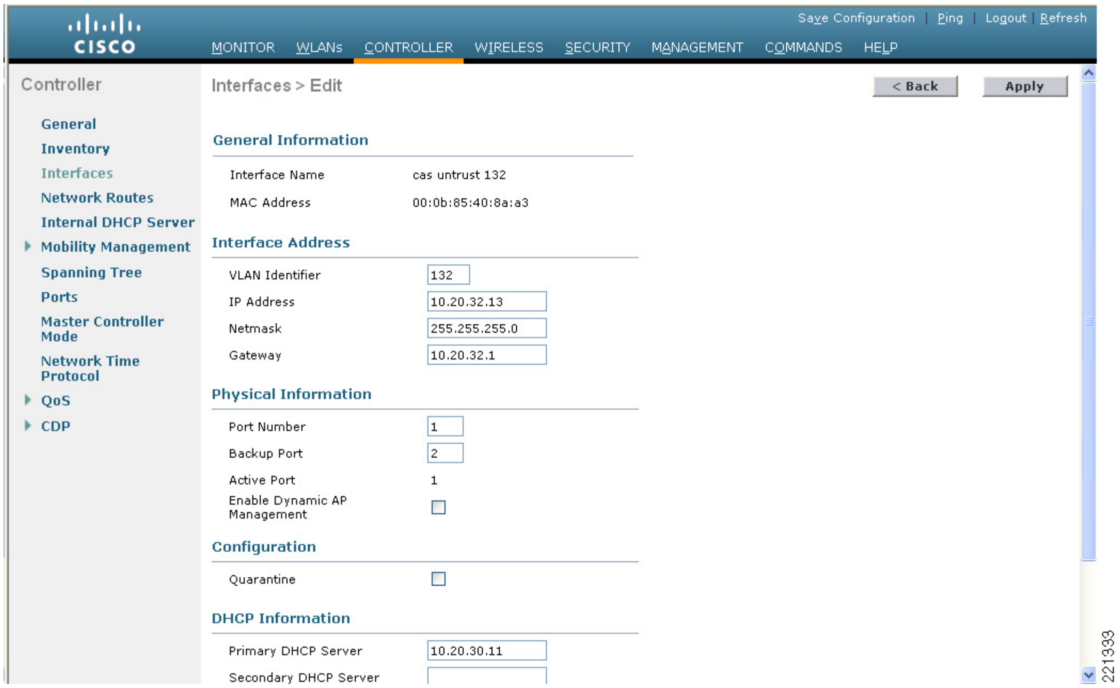
Configuration

Quarantine	□

DHCP Information

Primary DHCP Server	10.20.30.11
Secondary DHCP Server	

Figure 5-39 "Clean access untrust 132" Dynamic Interface Configuration



Interfaces > Edit

General Information

Interface Name	cas untrust 132
MAC Address	00:0b:85:40:8a:a3

Interface Address

VLAN Identifier	132
IP Address	10.20.32.13
Netmask	255.255.255.0
Gateway	10.20.32.1

Physical Information

Port Number	1
Backup Port	2
Active Port	1
Enable Dynamic AP Management	□

Configuration

Quarantine	□

DHCP Information

Primary DHCP Server	10.20.30.11
Secondary DHCP Server	

From the WLAN client interface configurations shown in Figure 5-38 and Figure 5-39, note the following points:

- Each interface is assigned to a different physical port. In addition, each interface is assigned with the other physical port as its backup.
- The IP address, subnet, and gateway parameters configured are linked to the trusted side of the NAC appliance; specifically VLANs 31 and 32, and SVIs 31 and 32 in the switch block.
- Client WLAN traffic is switched out of VLANs 131 and 132, and is trunked to the untrusted side of the NAC appliance.

Mapping WLANs to Untrusted WLC Interfaces

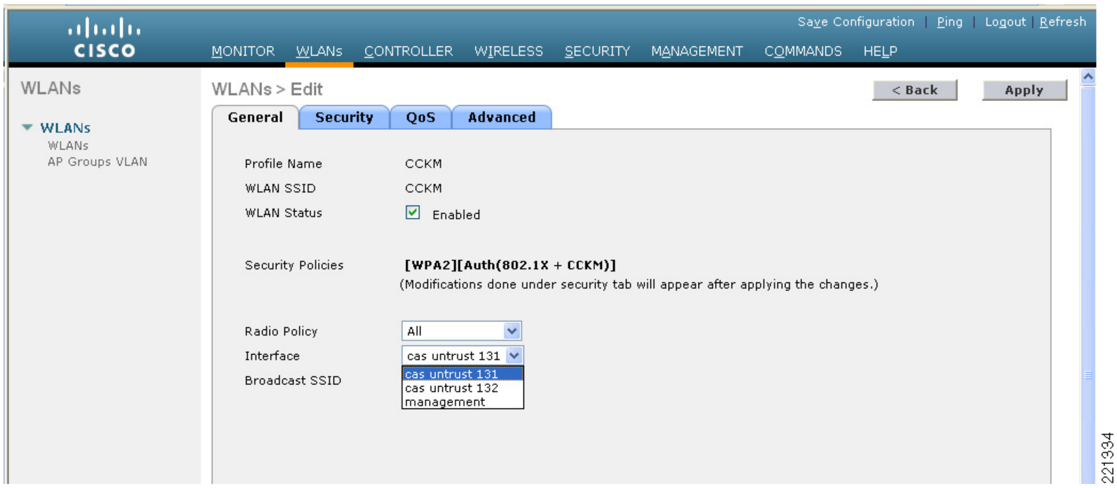
As shown in WLAN Client Interfaces, page 5-50, two dynamic interfaces are created and assigned to VLANs that trunk to the untrusted interface (Eth1) of the NAC appliance. The interface names are as follows:

- Clean access untrust 131
- Clean access untrust 132

It is a simple process to assign campus WLANs (requiring NAC services) to a controller interface that trunks to the NAC appliance.

In Figure 5-40, the WLAN CCKM is assigned to interface name **cas untrust 131**. All clients who authenticate/associate to this WLAN switch through the NAC appliance for authentication, policy/posture assessment, and remediation if necessary.

Figure 5-40 WLAN—Dynamic Interface Assignment



Profile Name CCKM

WLAN SSID CCKM

WLAN Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface cas untrust 131

Broadcast SSID

cas untrust 131
cas untrust 132
management

WiSM Deployment with NAC Appliance

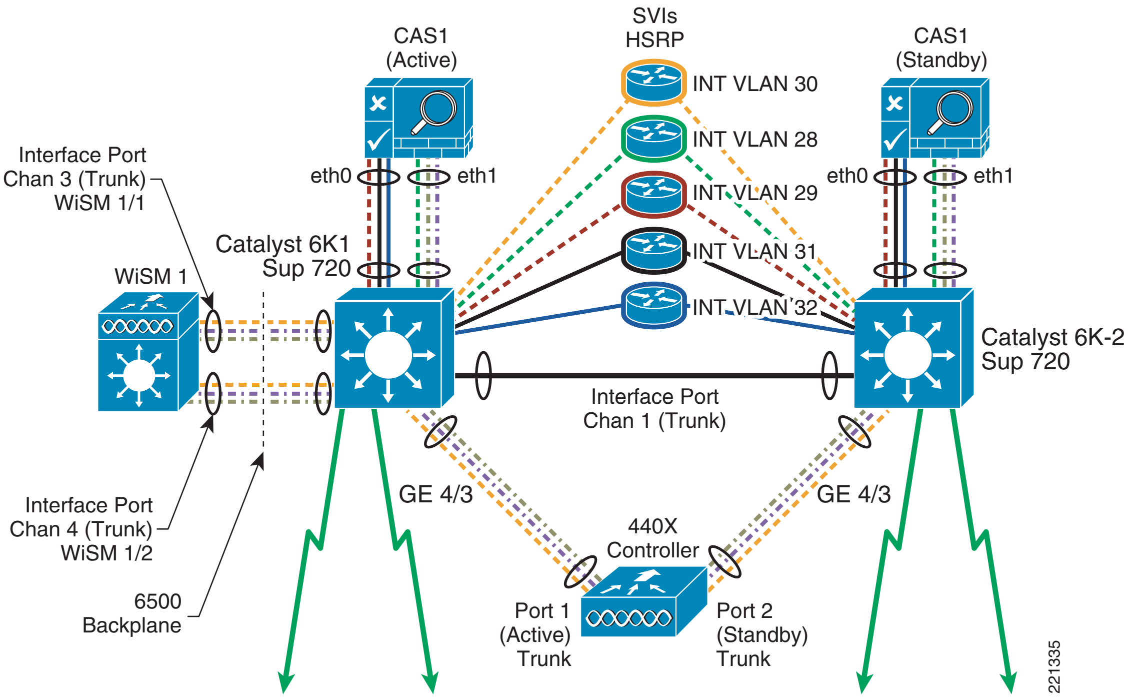
For detailed WiSM installation and configuration guidelines, see the following URLs:

http://www.cisco.com/en/US/partner/products/hw/modules/ps2706/prod_module_installation_guide09186a00807084f9.html

http://www.cisco.com/en/US/partner/products/ps6366/products_configuration_guide_book09186a00806b0077.html

Because the WiSM module is installed directly into the Catalyst 6500, the only option with regard to its deployment is the switch in which to install the module. Based on the design recommendations presented in this guide, the WiSM is Layer 2-adjacent to the NAC appliances; therefore, it can be located in either switch (assuming redundant switches make up the switch block) regardless which NAC appliance is active. This is also true for standalone controller implementations.

Figure 5-41 WiSM Module Integration



WiSM Backplane Switch Connectivity

The WiSM module connects directly to the backplane of the 6500. The module contains two WLAN controllers, each having the equivalent of four Gigabit Ethernet connections to the backplane. Each set of four Gigabit connections are grouped into a port channel. Note the following configuration example for Cat6K-1

```
:

interface Port-channel3

 description To WiSM 3/1 10.20.30.50
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
!
interface Port-channel4
 description To WiSM 3/2 10.20.30.52
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast

interface GigabitEthernet3/1
 description To WiSM 3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 3 mode on
!
interface GigabitEthernet3/2
 description To WiSM 3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp

 spanning-tree portfast

 channel-group 3 mode on

!

interface GigabitEthernet3/3

 description To WiSM 3/1

 switchport

 switchport trunk encapsulation dot1q

 switchport mode trunk

 no ip address

 mls qos trust dscp

 spanning-tree portfast

 channel-group 3 mode on

!

interface GigabitEthernet3/4

 description To WiSM 3/1

 switchport

 switchport trunk encapsulation dot1q

 switchport mode trunk

 no ip address

 mls qos trust dscp

 spanning-tree portfast

 channel-group 3 mode on

interface GigabitEthernet3/5

 description To WiSM 3/2

 switchport

 switchport trunk encapsulation dot1q

 switchport mode trunk

 no ip address

 mls qos trust dscp

 spanning-tree portfast

 channel-group 4 mode on
```

```
!
interface GigabitEthernet3/6
 description To WiSM 3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 4 mode on
!
interface GigabitEthernet3/7
 description To WiSM 3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 4 mode on
!
interface GigabitEthernet3/8
 description To WiSM 3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 4 mode on
```

WiSM Interface Configuration

The WiSM is configured and operates the same as a standalone controller. Therefore, the WiSM management and dynamic interface configurations are similar to that of the standalone controller shown in WLAN Client Interfaces except for the following:

- The WiSM controllers do not require secondary AP manager interfaces.
- The dynamic interfaces assigned to client WLANs do not support backup ports because the backplane connections of the controller operate in LAG mode.

WiSM WLAN Interface Assignment

The WLAN/interface configuration is the same as that described in Mapping WLANs to Untrusted WLC Interfaces, page 5-52.

Clean Access Manager/NAC Appliance Configuration Guidelines

This section describes the configuration aspects of the Clean Access solution that pertain to interoperability with the Cisco Unified Wireless solution. It is beyond the scope of this section to discuss policies, posture assessment techniques, and remediation methods. For detailed configuration guidelines, refer to the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following URL:

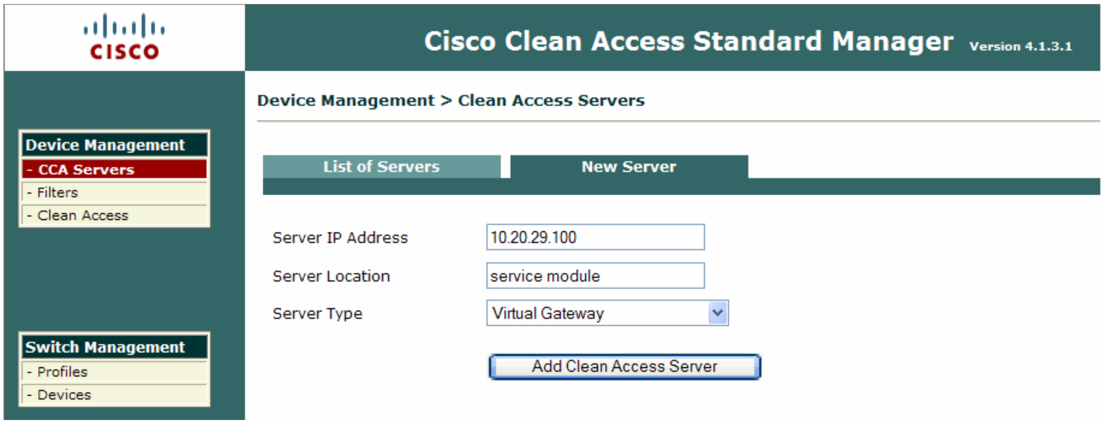
http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

The following subsections assume that a CAM has been physically installed and initially configured, appropriate appliance licenses have been installed, and there is logical connectivity to the NAC appliances.

Adding an HA NAC Pair to the CAM

When the NAC appliances are configured as an HA pair, logically they appear to the CAM as one NAC appliance. When you add the HA pair for the first time, you do so by using the trusted-side service IP address of the pair. See Figure 5-42 and Figure 5-43 for new appliance addition.

Figure 5-42 Adding HA Server Pair to CAM



Device Management > Clean Access Servers

Server IP Address: 10.20.29.100

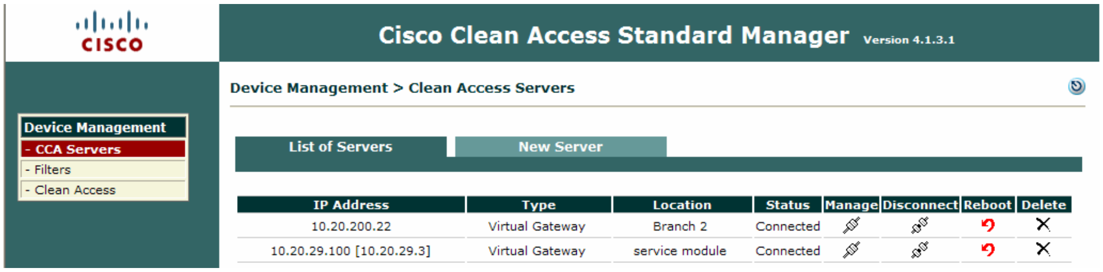
Server Location: service module

Server Type: Virtual Gateway

225347

Note in Figure 5-43 that the Server Type is set to virtual gateway.

Figure 5-43 Successful Server Addition



Device Management > Clean Access Servers

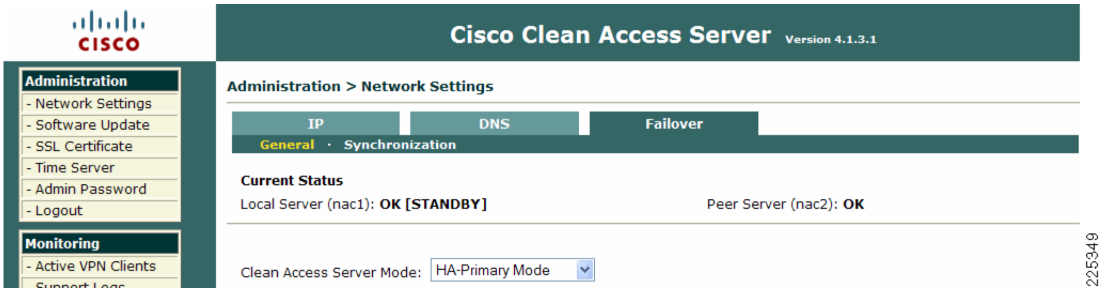
IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.20.200.22	Virtual Gateway	Branch 2	Connected	🔌	🔌	↺	✕
10.20.29.100 [10.20.29.3]	Virtual Gateway	service module	Connected	🔌	🔌	↺	✕

225248

Note the IP address field in Figure 5-43. Two IP addresses are represented. The first address is the service IP address of the appliance pair. The second address (in parentheses) represents the actual appliance that is active. If the HA pair cannot be added, do the following:

- Verify connectivity between CAM and NAC appliance interfaces. Verify that you can ping the trusted management interface addresses in addition to the service IP address.
- Ensure that a valid appliance license(s) is installed on the CAM.
- Check the appliance HA status by connecting to each appliance directly through its web management interface, as described in NAC Appliance HA Server Configuration, page 5-42. Click the **Failover** tab and check the appliance status. One appliance should show active while the other shows inactive.

Figure 5-44 Active Server

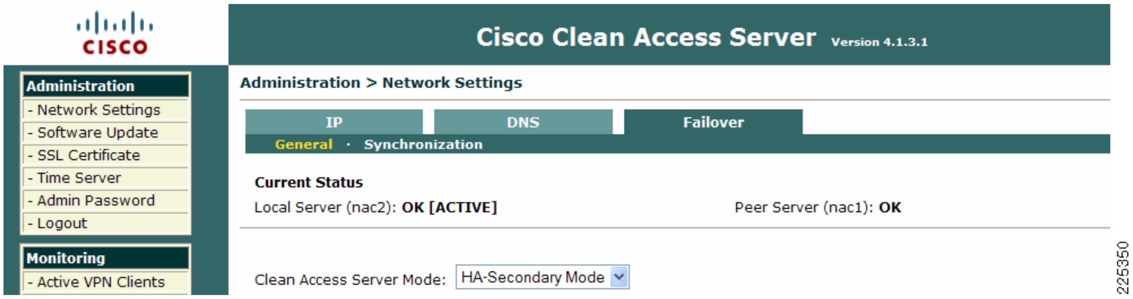


Current Status

Local Server (nac1): OK [STANDBY] Peer Server (nac2): OK

Clean Access Server Mode: HA-Primary Mode

Figure 5-45 Inactive Server



Current Status

Local Server (nac2): OK [ACTIVE] Peer Server (nac1): OK

Clean Access Server Mode: HA-Secondary Mode

Adding a Single NAC Appliance to the CAM

The process is the same as in Adding an HA NAC Pair to the CAM, page 5-57, except that the actual IP address of the trusted management interface of the appliance is used.

Connecting the Untrusted Interfaces (HA Configuration)

After the NAC appliance(s) have been added to the CAM as a virtual gateway, and the failover status of the HA pair indicates that one appliance is active and the other inactive (as shown in Figure 5-20 and Figure 5-21), the untrusted ports on each appliance can be connected to the switch block.

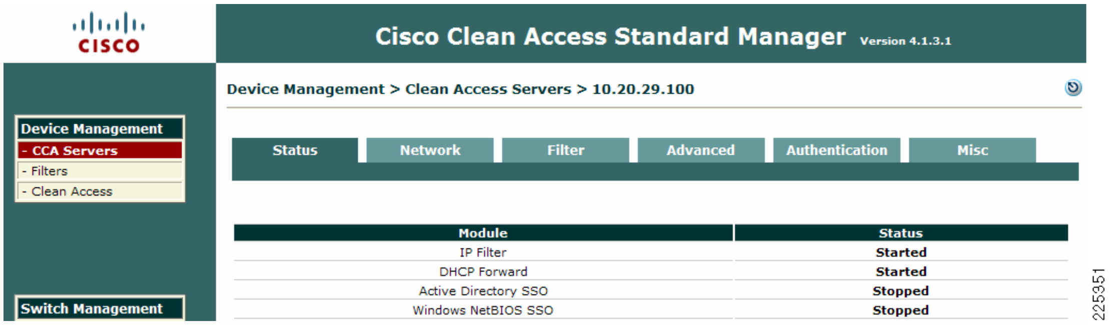
Adding Managed Networks

The CAM must be configured with those subnets that require NAC services. Using the sample NAC/Unified Wireless design in this document, the managed networks are the trusted-side subnets associated with VLANs 31 and 32 and their respective SVIs. (See Inter-Switch Trunk Configuration, page 5-33 and SVI Configuration, page 5-36.)

Step 1 From the Server List page on the CAM, click **Manage**. A server status is displayed, as shown in Figure 5-46.

Note All configuration additions or updates from this point onward are applied to both the active and inactive NAC appliances.

Figure 5-46 Server Status

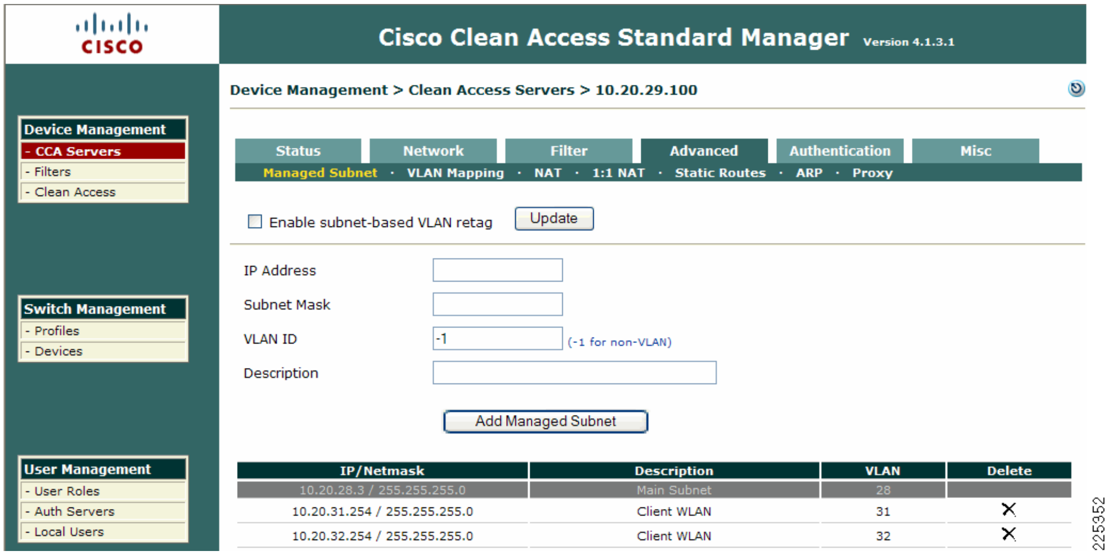


Device Management > Clean Access Servers > 10.20.29.100

Module	Status
IP Filter	Started
DHCP Forward	Started
Active Directory SSO	Stopped
Windows NetBIOS SSO	Stopped

Step 2 Click the **Advanced** tab. The Managed Subnets submenu is displayed, as shown in Figure 5-47.

Figure 5-47 Managed Subnets Configuration Sub-Menu



Device Management > Clean Access Servers > 10.20.29.100

□ Enable subnet-based VLAN retag

IP Address

Subnet Mask

VLAN ID -1 (-1 for non-VLAN)

Description

IP/Netmask	Description	VLAN	Delete
10.20.28.3 / 255.255.255.0	Main Subnet	28	
10.20.31.254 / 255.255.255.0	Client WLAN	31	✕
10.20.32.254 / 255.255.255.0	Client WLAN	32	✕

The configuration in Figure 5-47 shows two client subnets configured. These networks represent the trusted-side VLAN/subnets configured in Inter-Switch Trunk Configuration, page 5-33 and SVI Configuration, page 5-36. These are also the same subnets configured in the WLC dynamic interface configuration. See WLAN Client Interfaces, page 5-50. Note the following points in the configuration above:

- Do not enable subnet-based VLAN Retag.
- An IP address from the subnet to be managed must also be assigned to the NAC appliance. Thus, for a given managed client subnet in an HA topology with WLAN controllers and NAC, addresses must be reserved for the following:
  - Cat6K-1 SVI
  - Cat6K-2 SVI

- HSRP standby IP
- Each WLAN Controller with a dynamic interface on the VLAN/subnet
- NAC appliance managed subnet IP (above)

- Consideration must be given to planning the IP addressing scheme to be used in the deployment. It may be necessary to use VLSM masking to support enough addresses for end clients

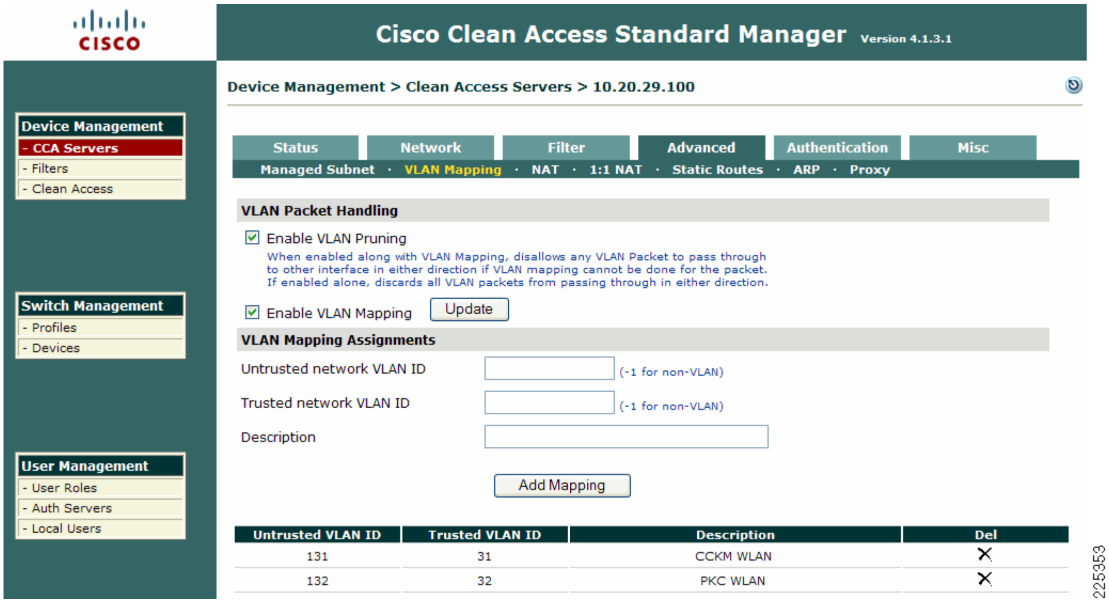
The VLANs associated with the managed subnet configuration above are the trusted-side VLANs 31 and 32. Whereas the WLAN controller configuration uses VLANs 131 and 132, respectively. See WLAN Client Interfaces, page 5-50. This is discussed further in VLAN Mapping, page 5-61.

VLAN Mapping

VLAN mapping bridges untrusted-side VLANs to their trusted-side counterparts to essentially form a single VLAN. VLAN mapping concepts are discussed in In-Band Modes, page 5-4.

From the Managed Subnets submenu, click the VLAN Mapping submenu. See Figure 5-48 for a VLAN mapping configuration example.

Figure 5-48 VLAN Mapping Sub-Menu



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
131	31	CCKM WLAN	✕
132	32	PKC WLAN	✕

The configuration in Figure 5-48 shows two VLAN mapping pairs. In summary, when a client comes in on an untrusted-side VLAN (from the WLC), the following happens:

- They are challenged for authentication.
- They are verified for policy compliance.
- If authenticated and policy compliance checks pass, they are switched out the trusted-side VLAN.

DHCP Pass-through

By default, the NAC appliance blocks all traffic between the untrusted and trusted-side VLANs until a user has authenticated and passed posture assessment. Exceptions include the following:

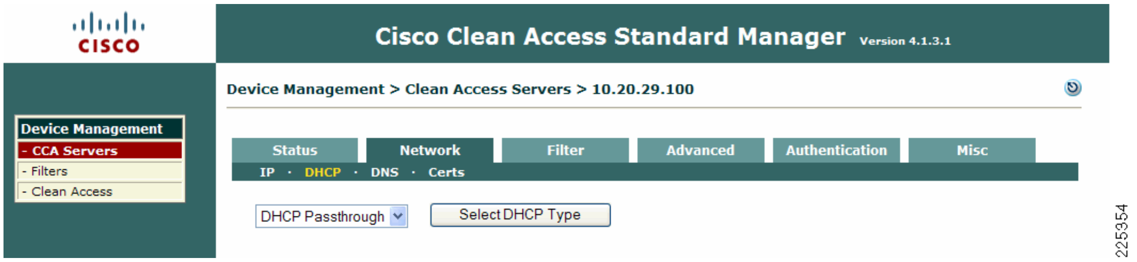
- Those devices or subnets configured in the Filters sub-menu configuration
- DNS packets (allowed by default in the unauthenticated role)
- DHCP packets

When the NAC appliance is configured as a virtual gateway, DHCP pass-through must be enabled so that the client device can obtain an IP address. This assumes the DHCP server is centralized and resides on the trusted side of the NAC appliance. DHCP pass-through is not required if the WLAN controller is acting as the DHCP server; however, this is not recommended for a large-scale campus deployment.

Step 1 From the CAM left-hand menu, under **Devices**, select **CCA Servers** and then click the **Manage** icon for the NAC appliance configured in Adding an HA NAC Pair to the CAM, page 5-57.

Step 2 From the server status page, select the **Network** tab and then the DHCP submenu. The DHCP configuration page is displayed, as shown in Figure 5-49.

Figure 5-49 NAC Appliance—Virtual Gateway/DHCP Configuration


Cisco Clean Access Standard Manager Version 4.1.3.1

Device Management > Clean Access Servers > 10.20.29.100

Step 3 Select **DHCP Passthrough** from the drop-down menu shown in Figure 5-49.

Step 4 Click the **Select DHCP Type** button to establish pass-through mode on the appliance.

Note The appliance may have to be rebooted after making the change above. If so, the appliance reboots automatically.

Enabling Wireless Single Sign-On

Wireless Single Sign On (SSO) is a critical component on a WLAN NAC deployment, because almost all enterprise level WLAN deployments will have implemented 802.1X/EAP authentication as part of the WLAN security solution. This authentication occurs prior to the the NAC appliance, but authentication and authorization are a critical component of the NAC framework. Therefore, a mechanism is needed to ensure that NAC is able to authenticate and authorize clients without forcing WLAN users to authenticate twice.

The NAC Appliance supports two different mechanisms for SSO:

- VPN SSO
- Active Directory SSO

To enable wireless SSO, the following is required:

- Enable VPN authentication on the NAC appliance—Each WLC that is configured with an 802.1x/EAP WLAN that will be subject to NAC assessment must be defined as a "VPN concentrator" in the NAC appliance.
- Enable RADIUS accounting on the WLCs—Each controller that is defined in the NAC appliance must be configured to send RADIUS accounting records to the NAC appliance for each 802.1x/EAP WLAN that is a managed subnet in the NAC.

Configuring Authentication for Wireless VPN SSO

To enable wireless SSO, the following is required:

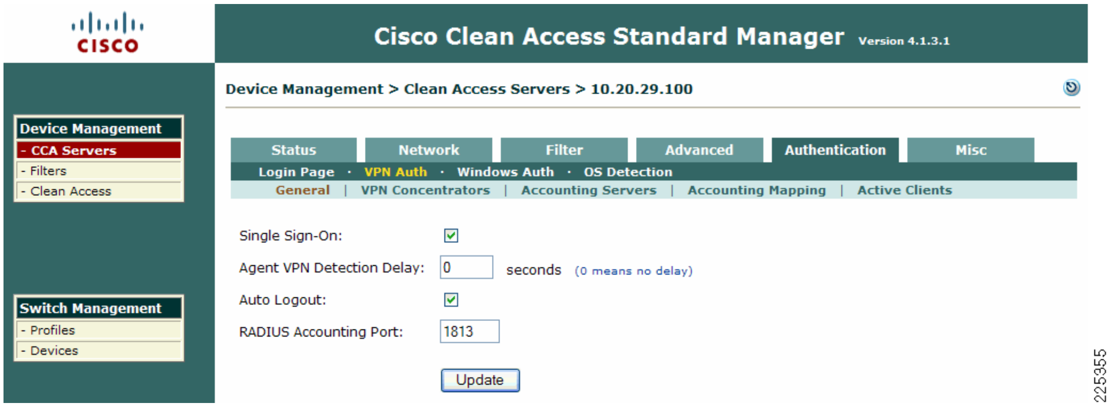
- Enable VPN authentication on the NAC appliance—Each WLC that is configured with an 802.1x/EAP WLAN that will be subject to NAC assessment must be defined as a "VPN concentrator" in the NAC appliance.
- Enable RADIUS accounting on the WLCs—Each controller that is defined in the NAC appliance must be configured to send RADIUS accounting records to the NAC appliance for each 802.1x/EAP WLAN that is a managed subnet in the NAC.

Step 1 From the CAM left-hand menu, under Devices, select CCA Servers and then click the **Manage** icon for the NAC appliance configured in Adding an HA NAC Pair to the CAM, page 5-57.

Step 2 From the server status page, select the **Authentication** tab and then the **VPN Auth** submenu.

The VPN authentication general configuration page appears, as shown in Figure 5-50.

Figure 5-50 VPN Auth—General Settings



Cisco Clean Access Standard Manager Version 4.1.3.1

Device Management > Clean Access Servers > 10.20.29.100

Single Sign-On: ☑

Agent VPN Detection Delay: 0 seconds (0 means no delay)

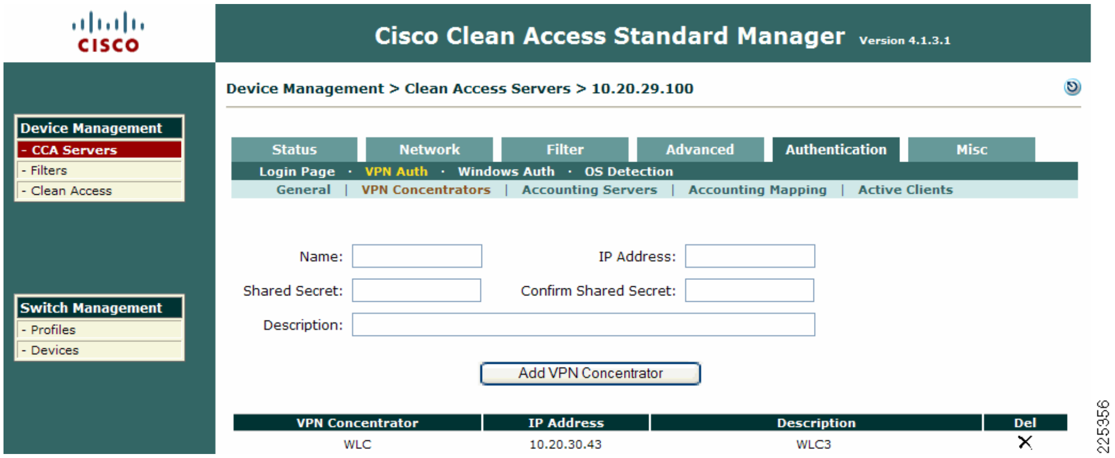
Auto Logout: ☑

RADIUS Accounting Port: 1813

The global configuration options for VPN Auth are shown in Figure 5-50. The SSO option must be selected as well as configuring a RADIUS Accounting Port number that matches what is configured on the WLAN controllers. You can optionally select **Auto Logout**, which after receipt of an accounting stop, automatically logs out the user session in the NAC appliance.

Step 3 From the VPN Auth, General settings submenu, click **VPN Concentrators**. See Figure 5-51.

Figure 5-51 VPN Auth—VPN Concentrators Configuration


cisco
Cisco Clean Access Standard Manager Version 4.1.3.1
Device Management
- CCA Servers
- Filters
- Clean Access
Switch Management
- Profiles
- Devices
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Add VPN Concentrator
225356

Device Management > Clean Access Servers > 10.20.29.100

Name:
IP Address:
Shared Secret:
Confirm Shared Secret:
Description:

VPN Concentrator	IP Address	Description	Del
WLC	10.20.30.43	WLC3	✕

The configuration screen shown in Figure 5-51 is where the WLAN controllers are configured. An entry must be made for each WLC that has 802.1x/EAP-based WLANs that are managed by the NAC appliance. All the fields above are self-explanatory.

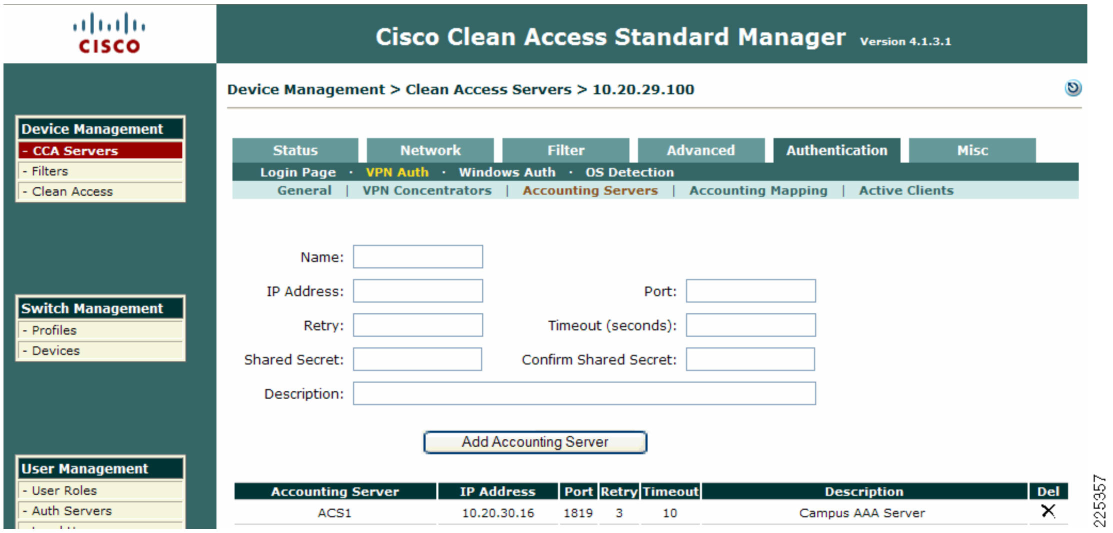
Note The IP address used in the VPN concentrator entry above must be that of the management IP address of the WLAN controller.

Radius Proxy Accounting (Optional)

If there is a requirement to forward RADIUS accounting records to AAA server(s) upstream in a campus deployment, the NAC appliance can be configured to proxy the accounting records received by the WLCs and to forward them.

Step 1 From the VPN Auth submenu, select **Accounting Servers**. (See Figure 5-52.)

Figure 5-52 Accounting Server Configuration


Cisco Clean Access Standard Manager Version 4.1.3.1
Device Management > Clean Access Servers > 10.20.29.100
Device Management
- CCA Servers
- Filters
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Add Accounting Server
225357

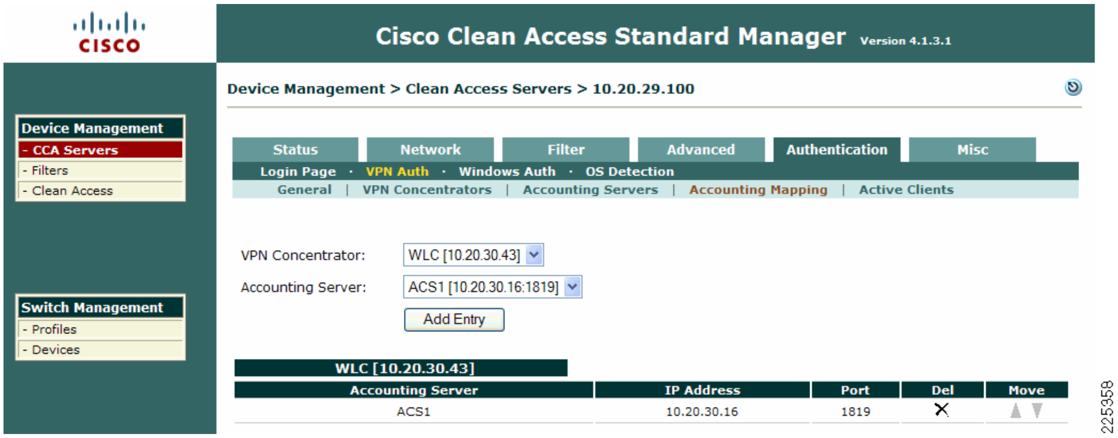
Name:
IP Address: Port:
Retry: Timeout (seconds):
Shared Secret: Confirm Shared Secret:
Description:

Accounting Server	IP Address	Port	Retry	Timeout	Description	Del
ACS1	10.20.30.16	1819	3	10	Campus AAA Server	✕

The accounting server configuration page shown in Figure 5-52 represents eligible upstream AAA or accounting servers to which the NAC appliance can proxy. The next step is to create proxy relationships between the WLAN controllers and upstream accounting servers.

Step 2 From the VPN Auth submenu, select **Accounting Mapping** (see Figure 5-53).

Figure 5-53 Accounting Mapping


Cisco Clean Access Standard Manager Version 4.1.3.1
Device Management > Clean Access Servers > 10.20.29.100
Device Management
- CCA Servers
- Filters
- Clean Access
Switch Management
- Profiles
- Devices
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Add Entry
225358

VPN Concentrator: WLC [10.20.30.43]
Accounting Server: ACS1 [10.20.30.16:1819]

WLC [10.20.30.43]

Accounting Server	IP Address	Port	Del	Move
ACS1	10.20.30.16	1819	✕	▲ ▼

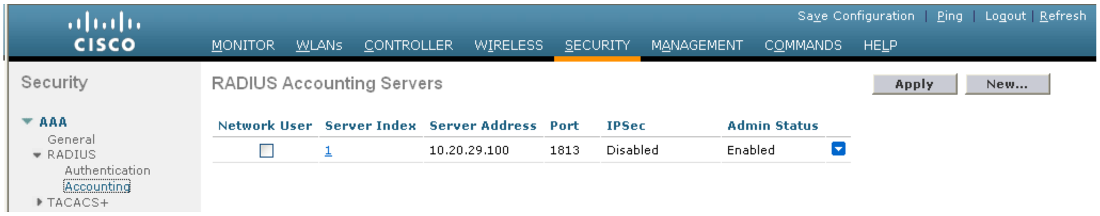
Step 1 Use the pull-down menus shown in Figure 5-53 to establish mapping (proxy) relationships between WLAN controllers and upstream accounting servers via the NAC appliance.

WLAN Controller—Configuring RADIUS Accounting for Wireless VPN SSO

The final step required to configure wireless SSO involves enabling RADIUS accounting on the WLAN controllers. The following must be accomplished for each controller with 802.1x/EAP WLANs that are being managed by the NAC appliance.

Step 1 From the controller main configuration page, select **Security** from the top menu bar and then **RADIUS Accounting** from the left-hand menu. See Figure 5-54.

Figure 5-54 WLAN Controller RADIUS Accounting Configuration



RADIUS Accounting Servers

Network User	Server Index	Server Address	Port	IPSec	Admin Status
□	1	10.20.29.100	1813	Disabled	Enabled

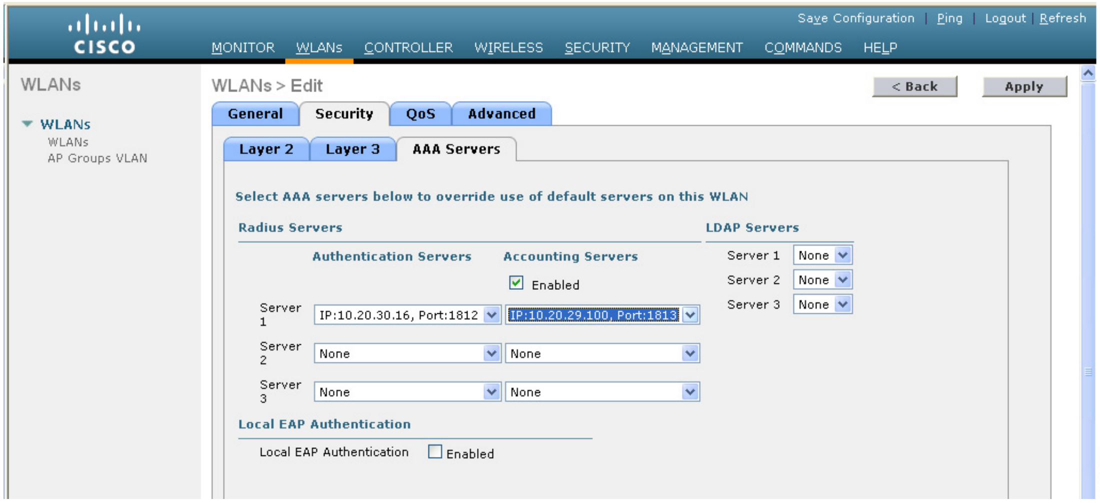
Figure 5-54 shows a RADIUS accounting server entry for the NAC appliance. Note the following:

- The accounting server IP address must be the "service IP address" of the trusted management interface of the NAC appliance.
- The **Network User box** should not be checked because this server entry is used by default for all configured WLANs unless the following applies:
  - Accounting is explicitly disabled in the WLANs RADIUS server configuration (only applicable in 4.0.206.0 MR2 WLC images and later).
  - A different accounting server has been selected in the WLANs RADIUS server configuration.
- Otherwise, if the box is checked, the NAC appliance could receive accounting records for WLANs that are not being managed by the NAC.

Step 2 The final step is to enable accounting for each 802.1x/EAP WLAN that is being managed by the NAC. From the controller main menu, select **WLANs** tab.

Step 3 Find the WLAN to configure from the list and click **Edit**. (See Figure 5-55.)

Figure 5-55 WLAN Configuration Screen



Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
		☑ Enabled
Server 1	IP:10.20.30.16, Port:1812	IP:10.20.29.100, Port:1813
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

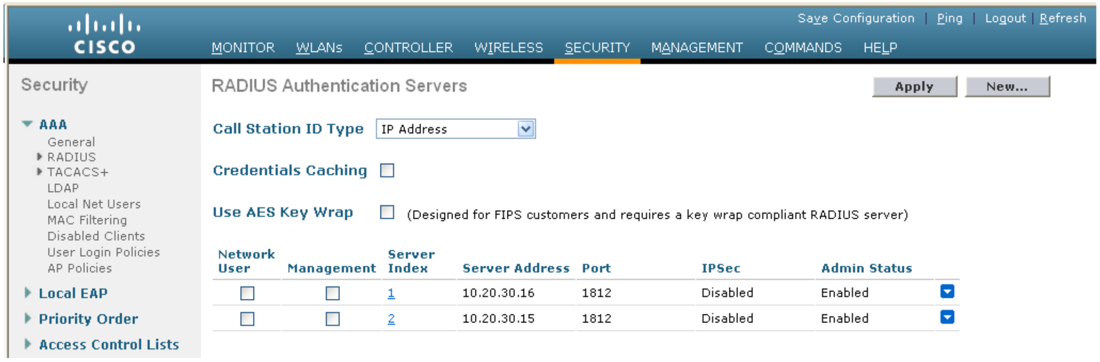
Local EAP Authentication □ Enabled

Accounting has been enabled for the WLAN in Figure 5-55, and the NAC appliance entry configured in Figure 5-54 has been selected as the RADIUS accounting server.

Note In the event of a NAC failure, wireless SSO remains operational because the accounting server (NAC) entry configured above uses the service IP of the NAC HA pair.

Note For WLC Release 4.0 and earlier, the Call Station ID Type must be set to **IP Address** in the RADIUS authentication servers configuration for Wireless SSO to work properly (see Figure 5-56). In Release 4.1 and later, the Call Station ID setting is not critical because the RADIUS accounting messages include Framed-IP-Address as a standard attribute in the record.

Figure 5-56 Call Station ID Type Setting



RADIUS Authentication Servers

Call Station ID Type: IP Address

Credentials Caching □

Use AES Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
□	□	1	10.20.30.16	1812	Disabled	Enabled
□	□	2	10.20.30.15	1812	Disabled	Enabled

Configuring Authentication for Wireless Active Directory SSO

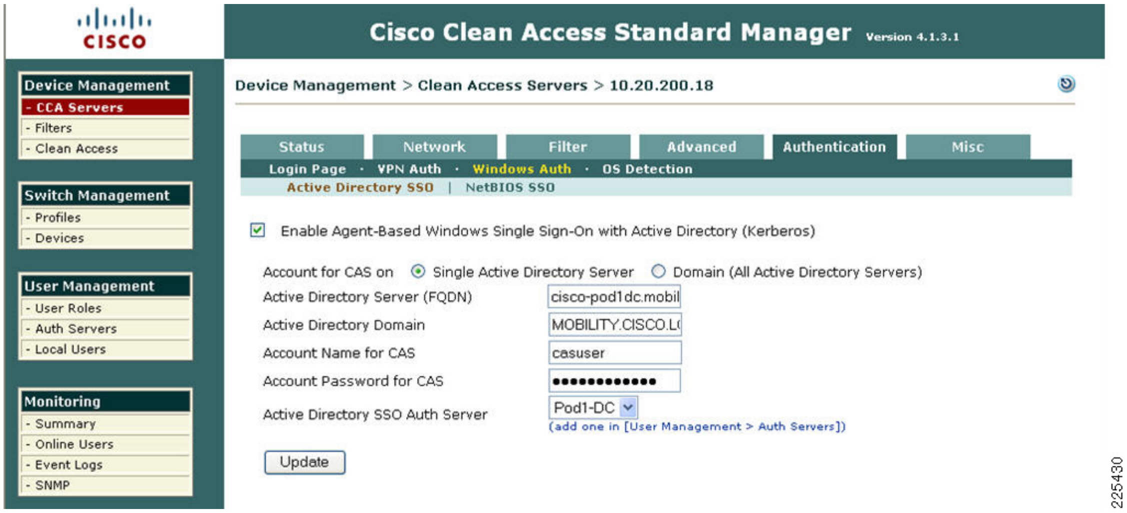
Step 1 From the CAM left-hand menu, under Devices, select CCA Servers and then click the **Manage** icon for the NAC appliance configured inAdding an HA NAC Pair to the CAM, page 5-57.

Step 2 From the server status page, select the **Authentication** tab and then the **Windows Auth** submenu.

Step 3 Configure the Submenu with the Active Directory server name, the Directory domain name, and the account details for this NAC appliance—an account for each NAC appliance must be created

An example is shown in Figure 5-57.

Figure 5-57 Windows Auth—General Settings



☑ Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

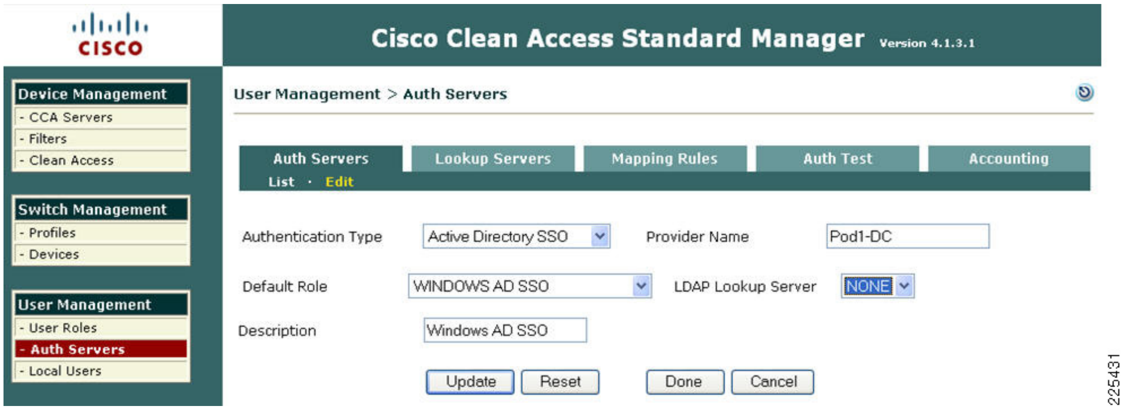
Account for CAS on ● Single Active Directory Server ○ Domain (All Active Directory Servers)

Active Directory Server (FQDN)	cisco-pod1dc.mobil
Active Directory Domain	MOBILITY.CISCO.L(
Account Name for CAS	casuser
Account Password for CAS	●●●●●●●●●●●●
Active Directory SSO Auth Server	Pod1-DC

Note You need to use **ktpass** command on Active Directory server (or domain) to force DES encryption to be used with NAC user password. Windows otherwise uses RC4, which is not supported by Linux. Example:*ktpass.exe -princ <casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM> -mapuser <casuser> -pass <Cisco123> -out <c:\casuser.keytab> -ptype KRB5_NT_PRINCIPAL -target <cca-eng-domain.cisco.com> +DesOnly*. The NAC documentation does not specify use of '-target' attribute. This may be required for **ktpass** command to work. If so, specify the fully qualified domain name for the AD server.

Step 4 From the CAM left hand menu, select the **Auth Servers** and under the **Auth Servers** select **New**, and complete the submenu, as shown in Figure 5-58, where the provider name equals the name of the Active Directory SSO Auth Server.

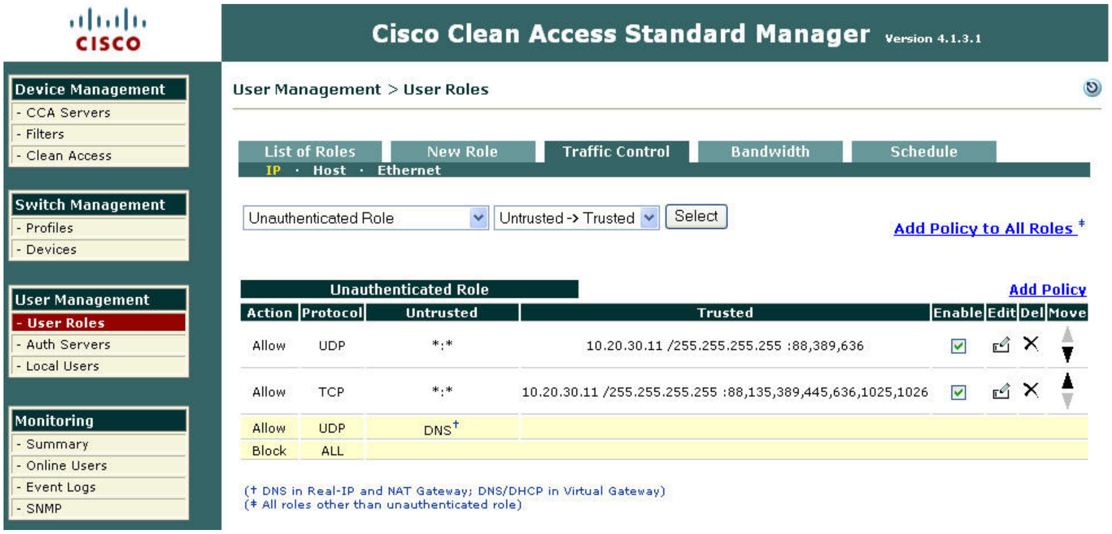
Figure 5-58 Authenciation Server Configuration



Authentication Type	Active Directory SSO	Provider Name	Pod1-DC
Default Role	WINDOWS AD SSO	LDAP Lookup Server	NONE
Description	Windows AD SSO		

Step 5 To ensure that windows client authentication can be performed to active directory the NAC appliance must allow unauthenticated clients to pass Windows client traffic to pass through the NAC appliance, as illustrated in Figure 5-59.

Figure 5-59 Allow Active Directory Authentication Traffic



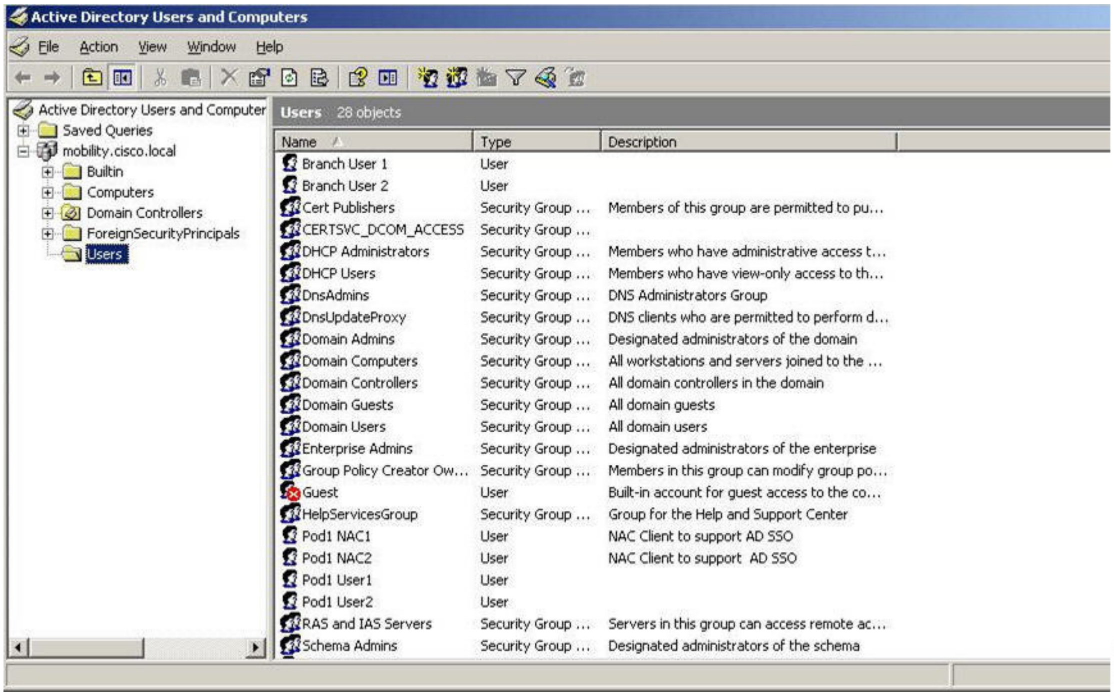
Unauthenticated Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	UDP	*:*	10.20.30.11 /255.255.255.255 :88,389,636	☑			
Allow	TCP	*:*	10.20.30.11 /255.255.255.255 :88,135,389,445,636,1025,1026	☑			
Allow	UDP	DNS†					
Block	ALL						

(† DNS in Real-IP and NAT Gateway; DNS/DHCP in Virtual Gateway)
(‡ All roles other than unauthenticated role)

Figure 5-60 shows example NAC appliance accounts (Pod1 NAC1 and Pod1 NAC2) that have been created in Active Directory to allow the NAC appliance to query Active Directory.

Figure 5-60 NAC Appliance's as Clients in AD



Name	Type	Description
Branch User 1	User	
Branch User 2	User	
Cert Publishers	Security Group ...	Members of this group are permitted to pu...
CERTSVC_DCOM_ACCESS	Security Group ...	
DHCP Administrators	Security Group ...	Members who have administrative access t...
DHCP Users	Security Group ...	Members who have view-only access to th...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permitted to perform d...
Domain Admins	Security Group ...	Designated administrators of the domain
Domain Computers	Security Group ...	All workstations and servers joined to the ...
Domain Controllers	Security Group ...	All domain controllers in the domain
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators of the enterprise
Group Policy Creator Ow...	Security Group ...	Members in this group can modify group po...
Guest	User	Built-in account for guest access to the co...
HelpServicesGroup	Security Group ...	Group for the Help and Support Center
Pod1 NAC1	User	NAC Client to support AD SSO
Pod1 NAC2	User	NAC Client to support AD SSO
Pod1 User1	User	
Pod1 User2	User	
RAS and IAS Servers	Security Group ...	Servers in this group can access remote ac...
Schema Admins	Security Group ...	Designated administrators of the schema

Creating a Wireless User Role

The following configuration examples outlined in this section through Defining User Pages represent a minimum configuration to support wireless SSO connectivity through the NAC appliance. These sections are not a comprehensive guide to enabling other authentication methods, posture assessment policies, or remediation techniques; nor do they cover all possible options that can be employed in a typical enterprise deployment. For in-depth guidance on these advanced topics, refer to the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

After initial installation, the NAC manager (CAM) has the following three default user roles:

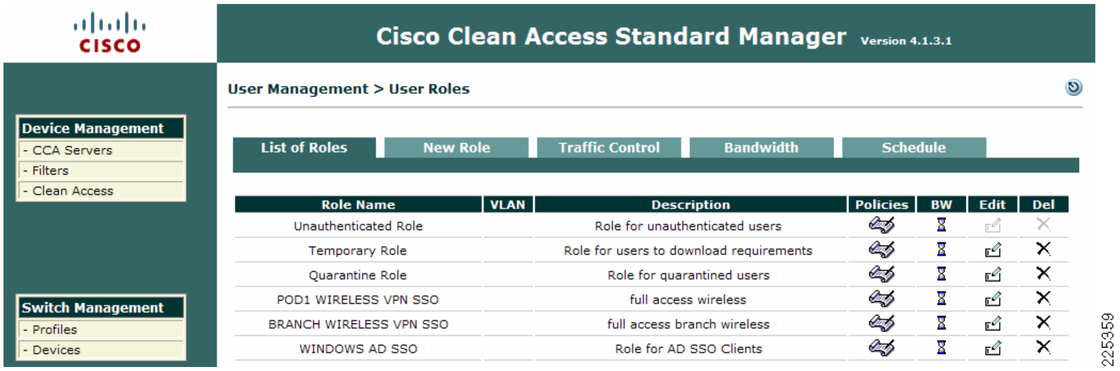
- Quarantine
- Unauthenticated
- Temporary

Users on managed subnets who have not authenticated with the NAC appliance are, by default, assigned the unauthenticated role. The temporary and quarantine roles are reserved for users who do not meet the policy requirements defined by the system administrator and that require remediation.

After a user is authenticated and passes all policy checks, they are assigned to a user logon role. User logon roles can vary between users and groups. Therefore, a user role must be configured for wireless users.

Step 1 From the CAM screen, click **User Roles** under User Management in the left-hand menu column. Figure 5-61 shows the three default roles.

Figure 5-61 User Roles Screen

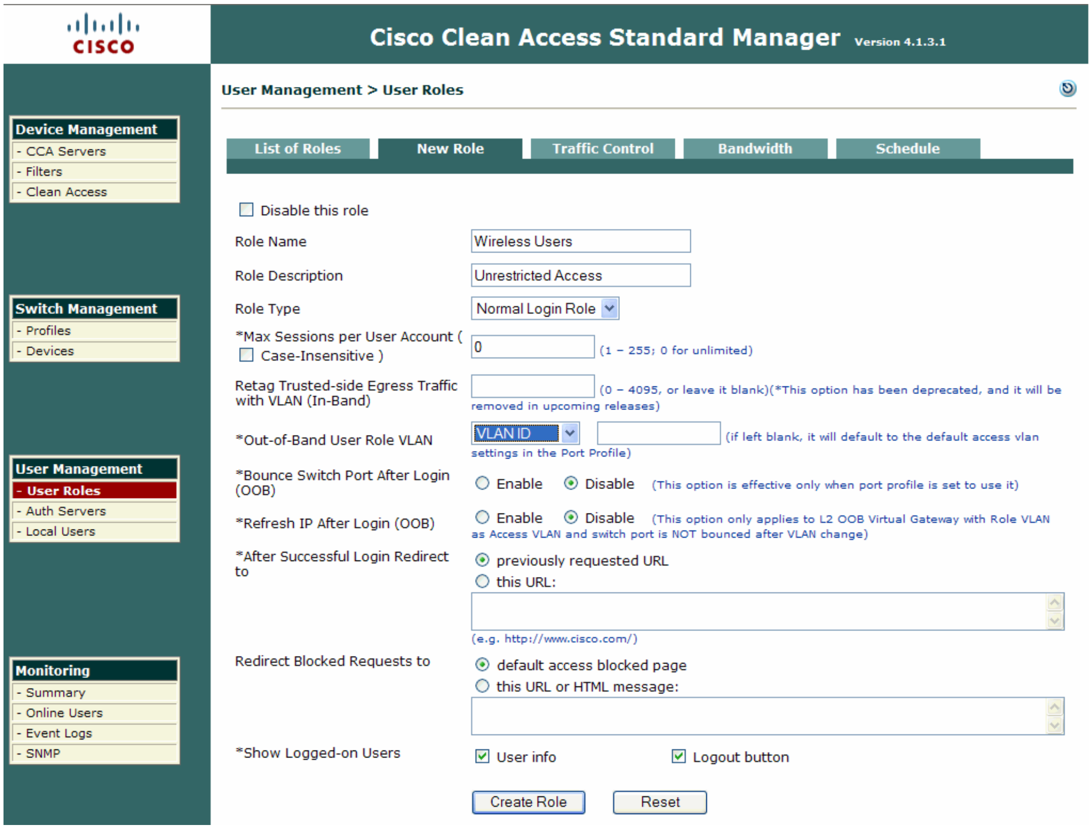


User Management > User Roles

Role Name	VLAN	Description	Policies	BW	Edit	Del
Unauthenticated Role		Role for unauthenticated users		⧗	✎	×
Temporary Role		Role for users to download requirements		⧗	✎	×
Quarantine Role		Role for quarantined users		⧗	✎	×
POD1 WIRELESS VPN SSO		full access wireless		⧗	✎	×
BRANCH WIRELESS VPN SSO		full access branch wireless		⧗	✎	×
WINDOWS AD SSO		Role for AD SSO Clients		⧗	✎	×

Step 2 From this screen, click the **New Role** tab. A new role configuration screen is displayed, as shown in Figure 5-62.

Figure 5-62 New User Role Configuration



User Management > User Roles

☐ Disable this role

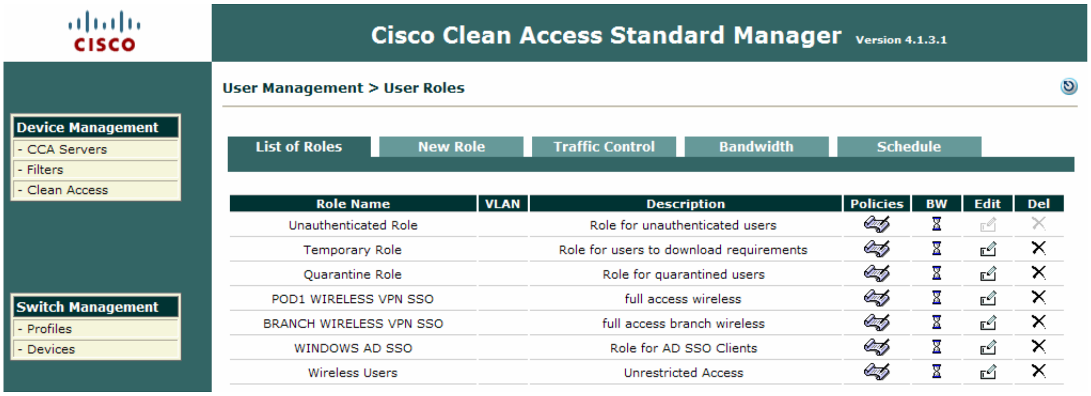
Role Name	Wireless Users
Role Description	Unrestricted Access
Role Type	Normal Login Role
*Max Sessions per User Account (☐ Case-Insensitive)	0 (1 – 255; 0 for unlimited)
Retag Trusted-side Egress Traffic with VLAN (In-Band)	(0 – 4095, or leave it blank)(*This option has been deprecated, and it will be removed in upcoming releases)
*Out-of-Band User Role VLAN	VLAN ID (if left blank, it will default to the default access vlan settings in the Port Profile)
*Bounce Switch Port After Login (OOB)	○ Enable ● Disable (This option is effective only when port profile is set to use it)
*Refresh IP After Login (OOB)	○ Enable ● Disable (This option only applies to L2 OOB Virtual Gateway with Role VLAN as Access VLAN and switch port is NOT bounced after VLAN change)
*After Successful Login Redirect to	● previously requested URL ○ this URL: (e.g. http://www.cisco.com/)
Redirect Blocked Requests to	● default access blocked page ○ this URL or HTML message:
*Show Logged-on Users	☑ User info ☑ Logout button

A name and description is given to the role, as shown in Figure 5-63. All other options shown are defaults. Note that the **Role Type** is normal login role.

Step 3 Click **Create Role**. The list of user roles is updated to include the new role.

Step 4 Click the **Policies** icon associated with the Wireless Users Role to configure traffic policies (see Figure 5-63).

Figure 5-63 New Wireless Users Role

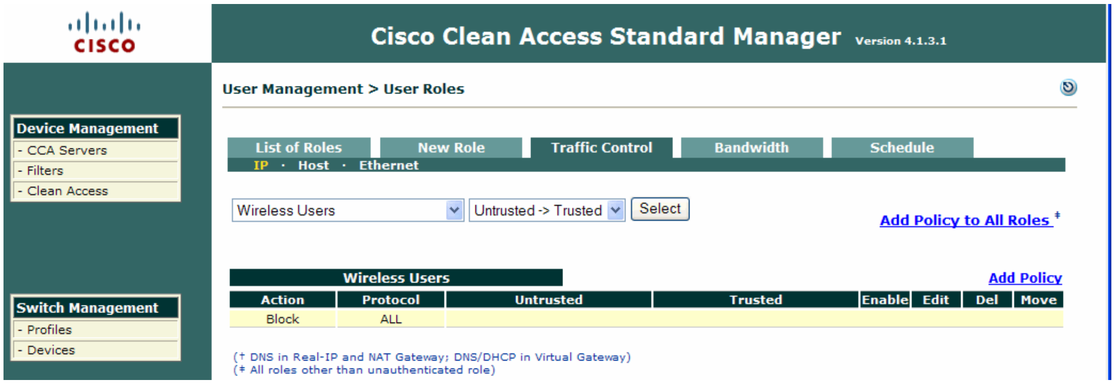


User Management > User Roles

Role Name	VLAN	Description	Policies	BW	Edit	Del
Unauthenticated Role		Role for unauthenticated users	⇆	⧗	✎	✕
Temporary Role		Role for users to download requirements	⇆	⧗	✎	✕
Quarantine Role		Role for quarantined users	⇆	⧗	✎	✕
POD1 WIRELESS VPN SSO		full access wireless	⇆	⧗	✎	✕
BRANCH WIRELESS VPN SSO		full access branch wireless	⇆	⧗	✎	✕
WINDOWS AD SSO		Role for AD SSO Clients	⇆	⧗	✎	✕
Wireless Users		Unrestricted Access	⇆	⧗	✎	✕

Figure 5-64 shows the traffic control configuration detail for the wireless users role. The default policy is to block all traffic.

Figure 5-64 Traffic Control for Wireless Users Role



User Management > User Roles

Wireless Users | Untrusted -> Trusted

Wireless Users

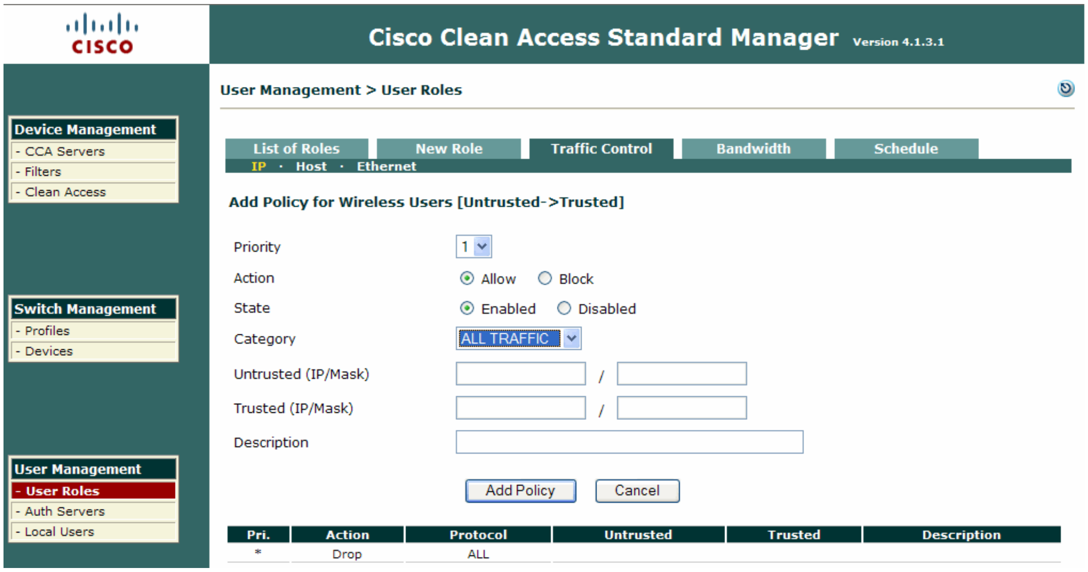
Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Block	ALL						

(† DNS in Real-IP and NAT Gateway; DNS/DHCP in Virtual Gateway)
(‡ All roles other than unauthenticated role)

Step 5 Click **Add Policy** to modify the default policy.

A new policy configuration screen is displayed, as shown in Figure 5-65.

Figure 5-65 New Policy Configuration



User Management > User Roles

Add Policy for Wireless Users [Untrusted->Trusted]

Priority: 1

Action: ● Allow ○ Block

State: ● Enabled ○ Disabled

Category: ALL TRAFFIC

Untrusted (IP/Mask): /

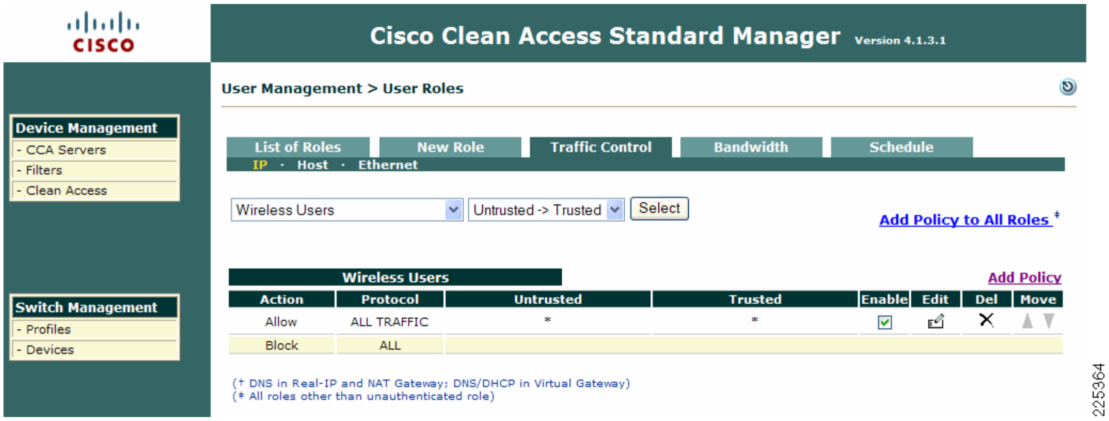
Trusted (IP/Mask): /

Description:

Pri.	Action	Protocol	Untrusted	Trusted	Description
*	Drop	ALL			

Step 6 From the Category pull-down menu shown in Figure 5-65, select **All Traffic** to permit all traffic from the untrusted to the trusted interface, and then click Apply Policy. (See Figure 5-66.)

Figure 5-66 Updated Wireless Users Traffic Policy



User Management > User Roles

Wireless Users | Untrusted -> Trusted | Select

Wireless Users

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	ALL TRAFFIC	*	*	☑		✕	
Block	ALL						

(† DNS in Real-IP and NAT Gateway; DNS/DHCP in Virtual Gateway)
(‡ All roles other than unauthenticated role)

Based on the updated policy shown in Figure 5-62, wireless users who have successfully authenticated and passed posture assessment are unrestricted as to where they can go. Many more policy options can be applied to a given user role.

The examples shown here represent a bare minimum configuration to support wireless client network access through the NAC appliance. For more information on configuring user roles, refer to Chapter 6 of the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Defining an Authentication Server for Wireless Users Role

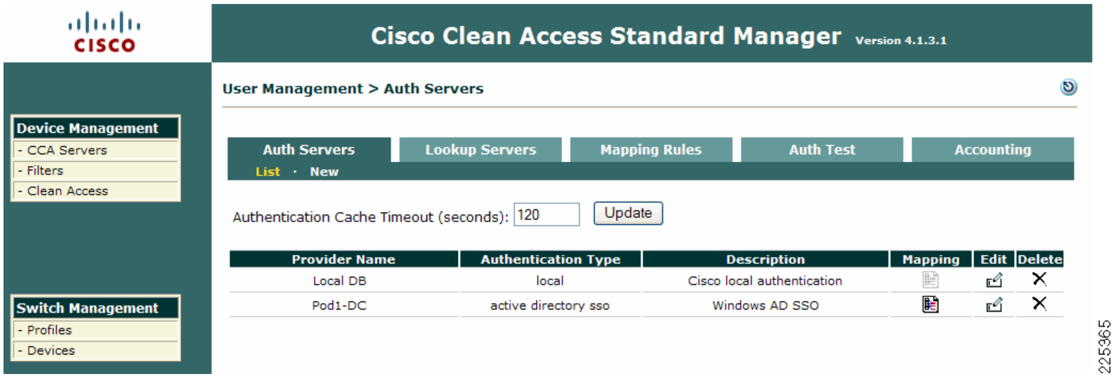
An authentication server must be defined for each user logon role, which in turn determines which method is used to authenticate end users with the NAC appliance. Authentication type/methods include the following:

- Kerberos
- Windows NT
- RADIUS
- LDAP
- Single Sign-On Active Directory
- Single Sign-On VPN

As discussed in Single Sign-On-VPN, page 5-11, Single Sign-On Active Directory, page 5-12, and Enabling Wireless Single Sign-On, page 5-62, wireless user SSO is supported by using the VPN SSO or SSO Active Directory feature of the NAC appliances. The following configuration maps the NAC appliance VPN authentication configuration performed in Figure 5-55 with the newly-created wireless users role defined in Figure 5-67.

Step 1 From the CAM screen, click **Auth Servers** under User Management in the left-hand menu column.

Figure 5-67 Auth Server Configuration



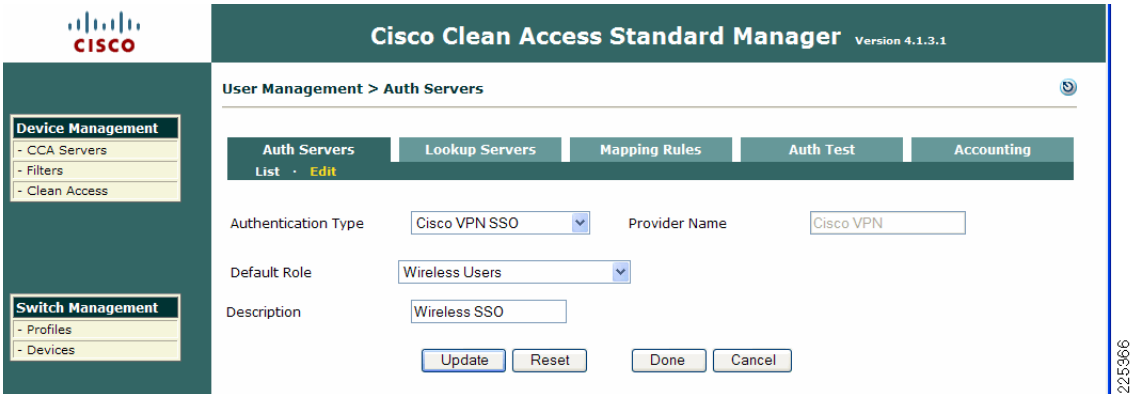
Authentication Cache Timeout (seconds): 120

Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication			✕
Pod1-DC	active directory sso	Windows AD SSO			✕

As seen in Figure 5-67, a default Auth Sever Guest is defined, which uses a local database on the CAM. This Auth Server can be used for guest access services.

Step 2 Click the New button in the Auth Servers sub-menu. (See Figure 5-68.)

Figure 5-68 New Auth Server Configuration

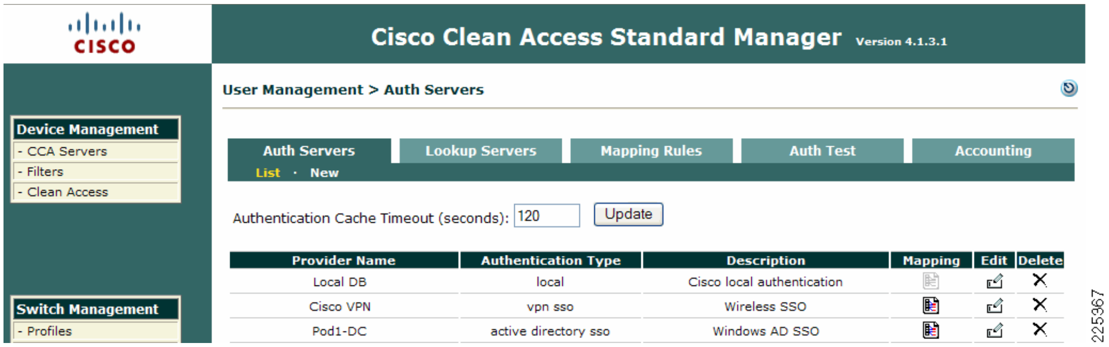


Authentication Type: Cisco VPN SSO
Provider Name: Cisco VPN
Default Role: Wireless Users
Description: Wireless SSO

In Figure 5-68, the Authentication Type is set to "Cisco VPN SSO" and the Default Role is set to Wireless Users (or Active Directory SSO, if that was the chosen mechanism), which was configured in Creating a Wireless User Role.

Step 3 Finish the configuration by added a description and clicking **Add Server**. The new entry is added, as shown in Figure 5-69.

Figure 5-69 VPN SSO Auth Server for Wireless SSO



Authentication Cache Timeout (seconds): 120

Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication	▤	✎	✕
Cisco VPN	vpn sso	Wireless SSO	▤	✎	✕
Pod1-DC	active directory sso	Windows AD SSO	▤	✎	✕

No internal or external authentication server is configured for wireless SSO. Instead, when a wireless user has associated and attempts to connect to the network, the NAC appliance checks the client MAC address and IP against accounting record information that is received from the WLAN controller. If a match is made, the wireless user is automatically authenticated with the NAC. The example shown above maps all wireless users authenticated via the "vpn sso" auth server to the wireless user role. Customized roles can be created on a per-wireless user or per-wireless user group basis by using the auth server mapping feature. In this case, RADIUS VSAs can be used to control to which NAC appliance role a wire user or group is assigned. For more information, see Chapter 7 of the Cisco NAC *Appliance—Clean Access Manager Installation and Administration Guide* at the following URL:

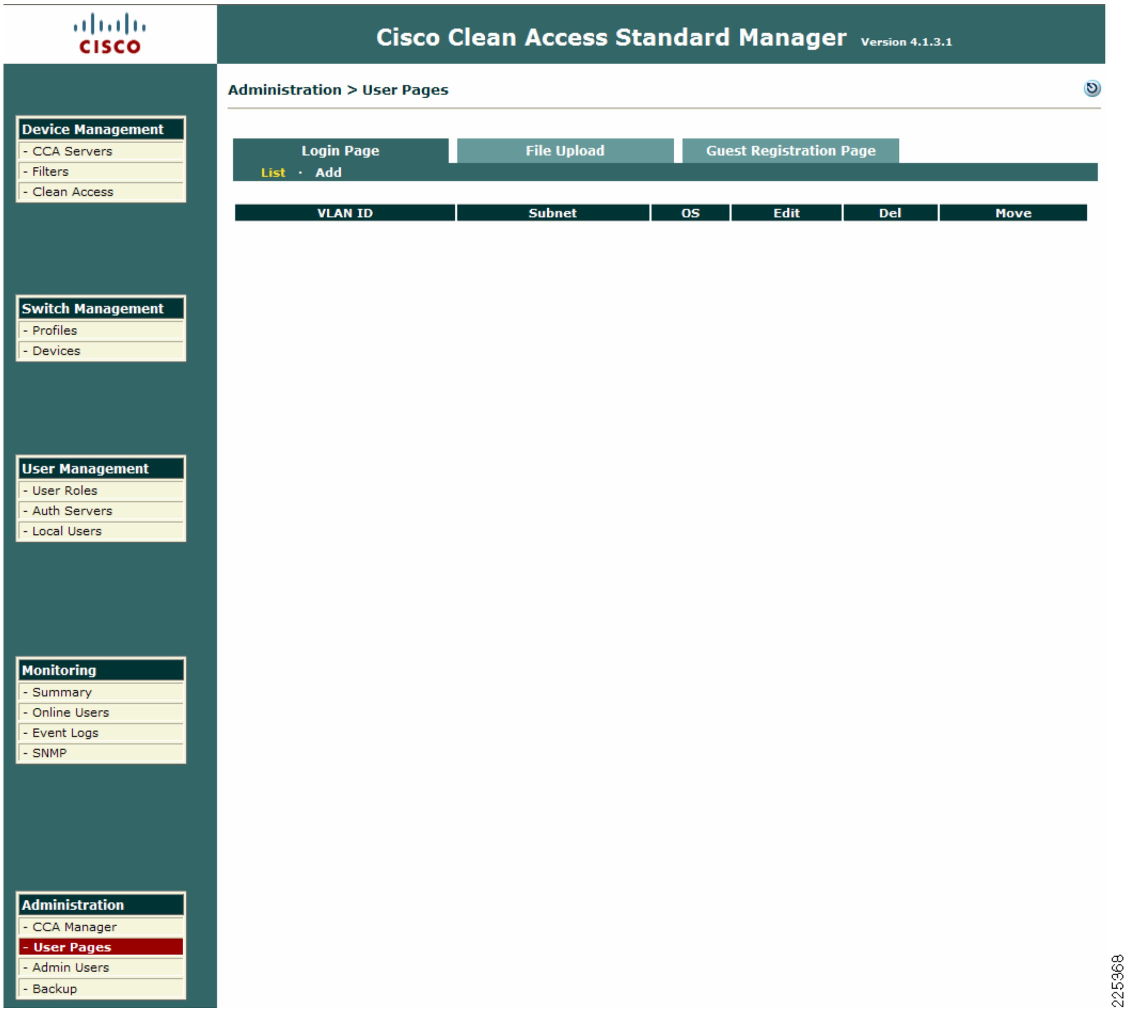
http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Defining User Pages

User pages are what end users see for the first time when they connect and are redirected for authentication, posture assessment, and remediation. Depending on the Clean Access method (posture/policy assessment method) configured for a given user role, users may either be required to use the Clean Access Agent or they may use the network scanning feature resident on the NAC appliance to perform policy and posture assessment. If the Agent is installed on the client machine, those users are, as a rule of thumb, no longer redirected to the user pages. Agentless users, however, depending on policy requirements, may be subjected to the user pages periodically for re-authentication and ongoing posture assessment.

Step 1 From the CAM screen, click **User Pages** under Administration in the left-hand menu column. (See Figure 5-70.)

Figure 5-70 User Login Page List

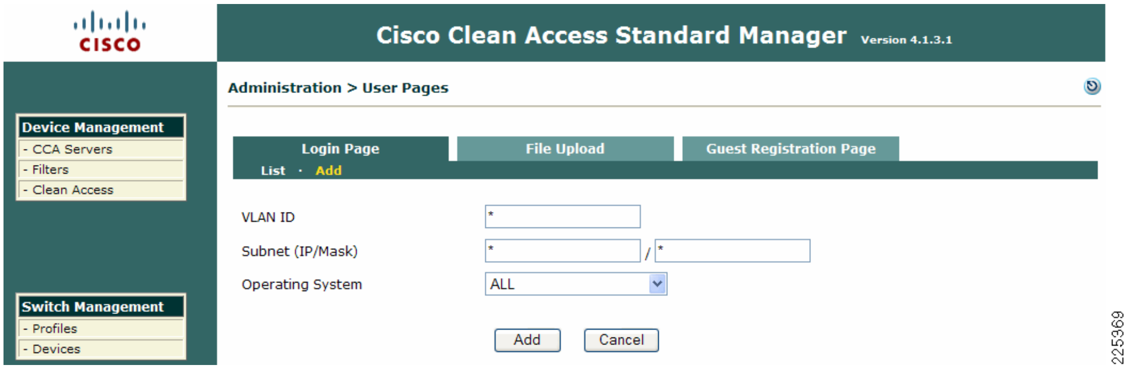


VLAN ID	Subnet	OS	Edit	Del	Move

Step 2 Click **Add** under the Login Page tab.

See Figure 5-71 for new Login Page network and operating system configuration options.

Figure 5-71 Login Page—Network and Operating System Configuration

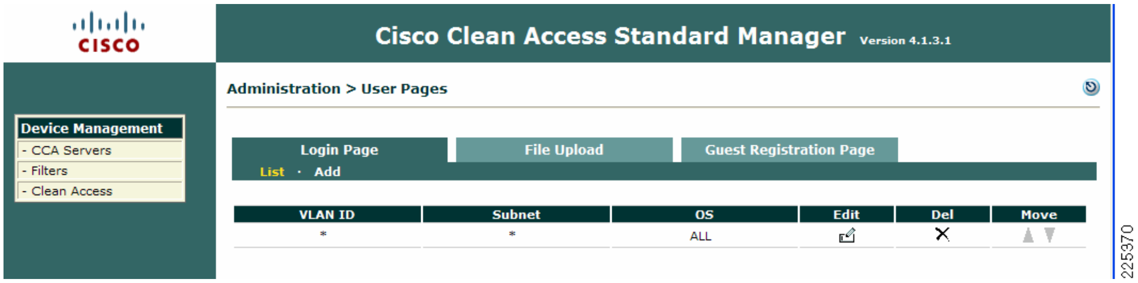


VLAN ID	*
Subnet (IP/Mask)	* / *
Operating System	ALL

Multiple login pages can be configured to accommodate various types of users and user groups. The quickest method for creating a user page is to accept the defaults as shown in Figure 5-44 by clicking **Add**. If multiple pages need to be configured, VLAN and subnet information can be defined to determine which login page is presented to the user.

When defining VLAN information in the context of a wireless deployment (as presented in this guide), use the untrusted-side VLAN IDs, not the trusted-side VLAN IDs (see Mapping WLANs to Untrusted WLC Interfaces, page 5-52). Figure 5-72 shows a login page with default values from above.

Figure 5-72 Newly-Created Login Page



VLAN ID	Subnet	OS	Edit	Del	Move
*	*	ALL		✕	▲ ▼

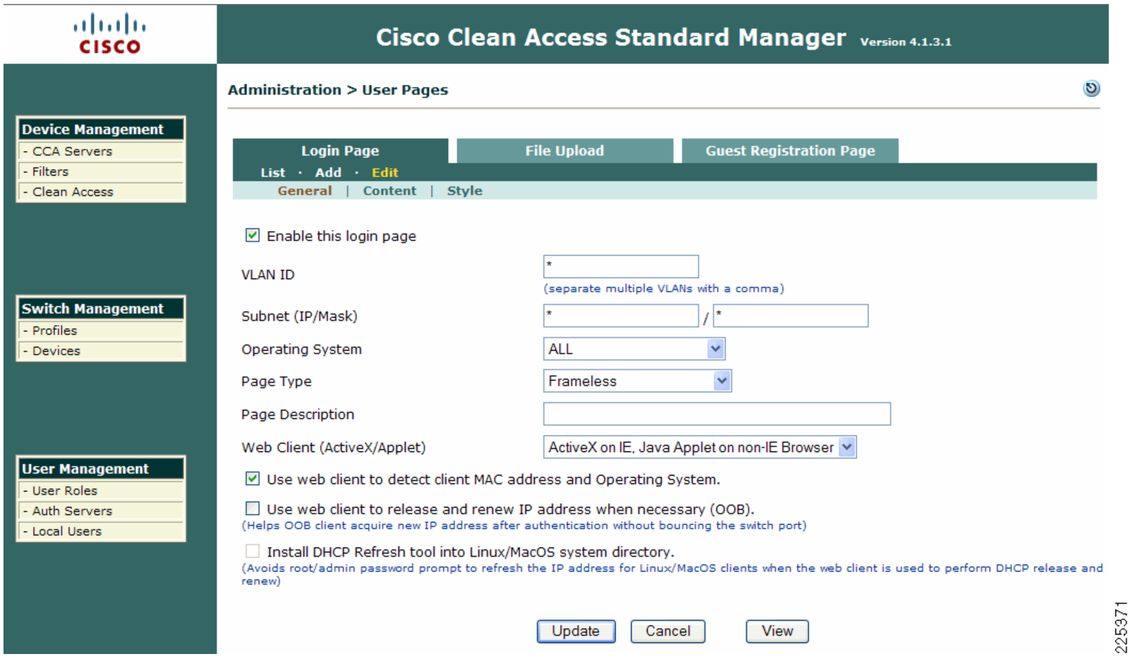
Step 3 Click the **Edit** button to proceed.

General login page configuration options are presented, as shown in Figure 5-73.

For further information on configurable options on this page, refer to the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Figure 5-73 Login Page—General Configuration



☑ 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 on IE, Java Applet on non-IE Browser

☑ 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)

Step 4 Make sure **Enable this login page** is checked in Figure 5-73. Configure any other options as required for the deployment and then click **Update**.

After the page refreshes, click **Content** in the Login Page sub-menu.

Step 5 The content configuration page as shown in Figure 5-74 allows network administrators to customize the page seen by users.

Figure 5-74 Login Page Content Variables

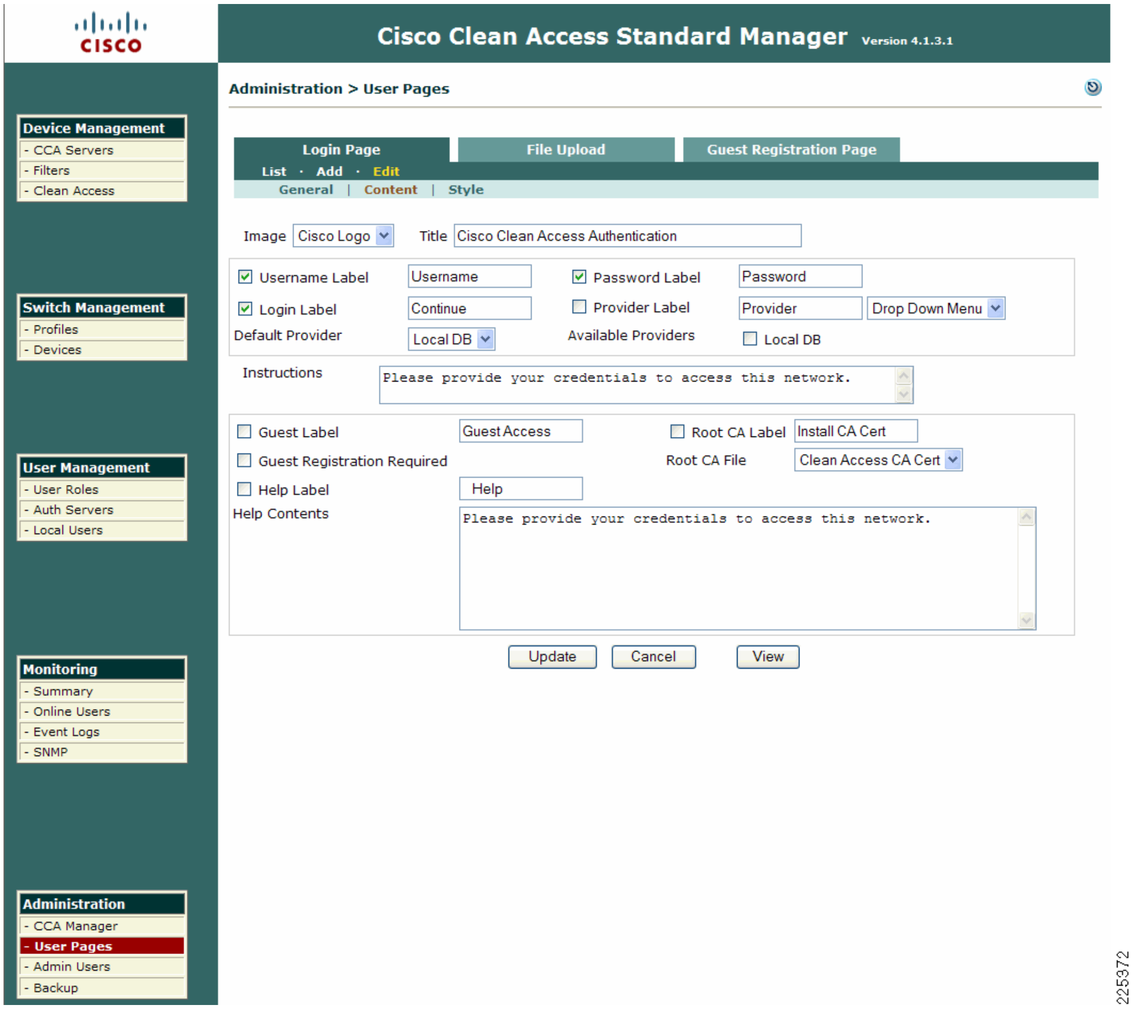


Image: Cisco Logo | Title: Cisco Clean Access Authentication

☑ Username Label: Username | ☑ Password Label: Password

☑ Login Label: Continue | □ Provider Label: Provider | Drop Down Menu

Default Provider: Local DB | Available Providers: □ Local DB

Instructions: Please provide your credentials to access this network.

□ Guest Label: Guest Access | □ Root CA Label: Install CA Cert

□ Guest Registration Required | Root CA File: Clean Access CA Cert

□ Help Label: Help

Help Contents: Please provide your credentials to access this network.

For agent-based wireless SSO, no specific configuration is required. For more information, refer to Chapter 5 of the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following URL:

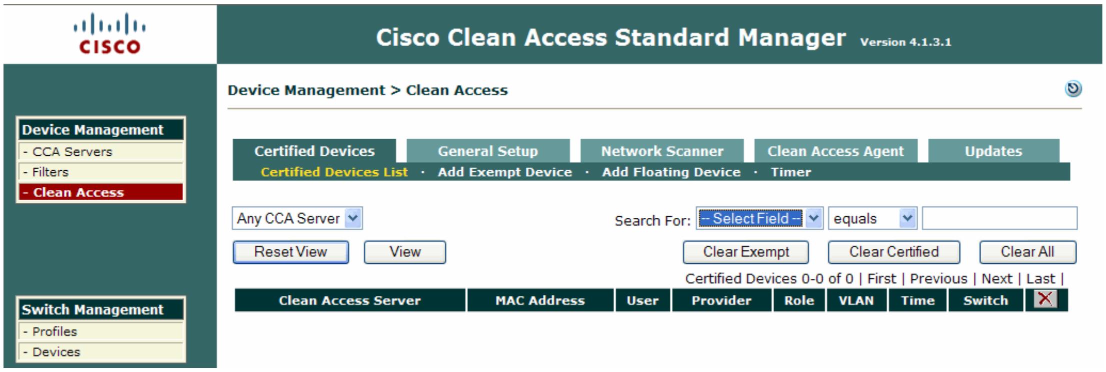
http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Configure Clean Access Method and Policies

The final configuration step is to select the method of posture assessment to be used for a given user role. Up to this point, the solution has been configured to support wireless user SSO. As mentioned previously, the Clean Access Agent in conjunction with the VPN SSO authentication (configured in Enabling Wireless Single Sign-On, page 5-62) offers the best end-user experience as well as more comprehensive posture assessment and policy enforcement.

Step 1 From the CAM screen, click **Clean Access** under Device Management in the left-hand menu column. (See Figure 5-75.)

Figure 5-75 Clean Access Certified List



Any CCA Server

Search For: -- Select Field -- equals

Certified Devices 0-0 of 0 | First | Previous | Next | Last |

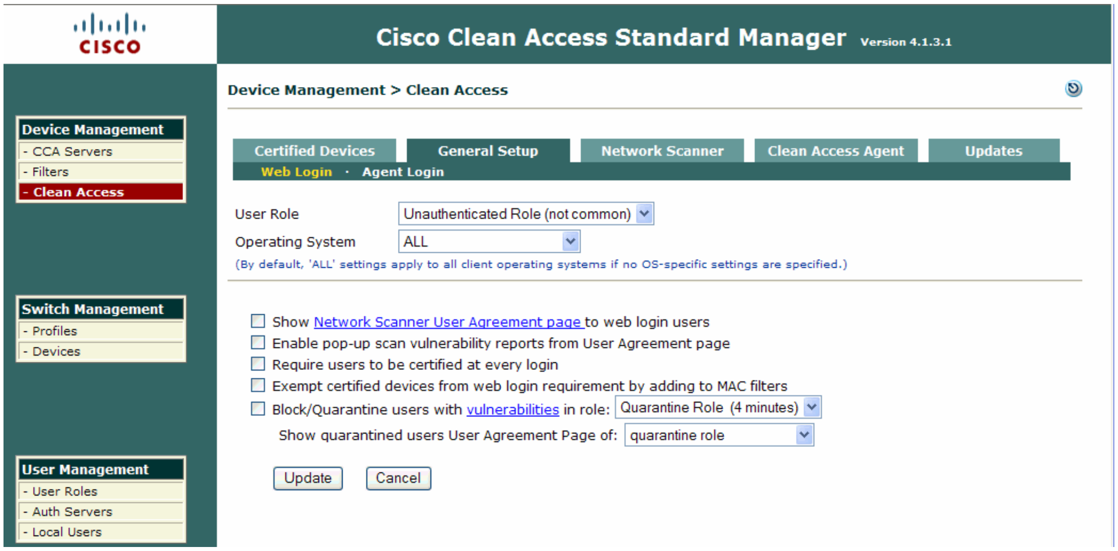
Clean Access Server	MAC Address	User	Provider	Role	VLAN	Time	Switch	☒

The list in Figure 5-75 shows any devices which have been certified as "clean".

Step 2 From this screen, click the **General Setup** tab.

Figure 5-76 shows a summary of actions to take for those users who authenticate via web login and undergo posture assessment via the network scanner method.

Figure 5-76 Web Login Network Scanning Parameters



User Role: Unauthenticated Role (not common)

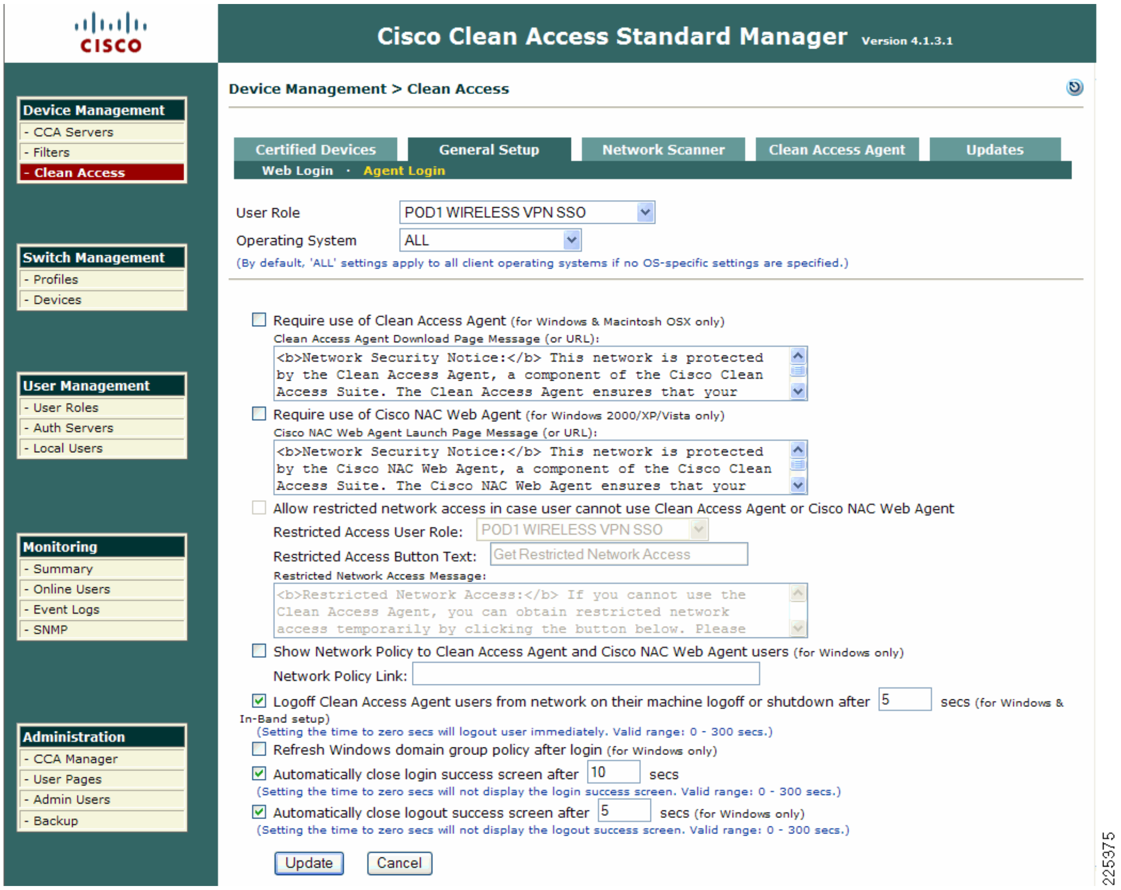
Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

□ Show Network Scanner User Agreement page to web login users
□ Enable pop-up scan vulnerability reports from User Agreement page
□ Require users to be certified at every login
□ Exempt certified devices from web login requirement by adding to MAC filters
□ Block/Quarantine users with vulnerabilities in role: Quarantine Role (4 minutes)
Show quarantined users User Agreement Page of: quarantine role

Step 3 Click the **Agent Login** option under the **General Setup** tab as shown in Figure 5-76. Figure 5-77 shows the configuration parameter associated with using the Clean Access Agent for authentication user login.

Figure 5-77 Clean Access Agent Login Parameter



User Role: POD1 WIRELESS VPN SSO

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

□ Require use of Clean Access Agent (for Windows & Macintosh OSX only)

Clean Access Agent Download Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
by the Clean Access Agent, a component of the Cisco Clean
Access Suite. The Clean Access Agent ensures that your
```

□ Require use of Cisco NAC Web Agent (for Windows 2000/XP/Vista only)

Cisco NAC Web Agent Launch Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
by the Cisco NAC Web Agent, a component of the Cisco Clean
Access Suite. The Cisco NAC Web Agent ensures that your
```

□ Allow restricted network access in case user cannot use Clean Access Agent or Cisco NAC Web Agent

Restricted Access User Role: POD1 WIRELESS VPN SSO

Restricted Access Button Text: Get Restricted Network Access

Restricted Network Access Message:

```
<b>Restricted Network Access:</b> If you cannot use the
Clean Access Agent, you can obtain restricted network
access temporarily by clicking the button below. Please
```

□ Show Network Policy to Clean Access Agent and Cisco NAC Web Agent users (for Windows only)

Network Policy Link:

☑ Logoff Clean Access Agent users from network on their machine logoff or shutdown after 5 secs (for Windows & In-Band setup)

(Setting the time to zero secs will logout user immediately. Valid range: 0 - 300 secs.)

□ Refresh Windows domain group policy after login (for Windows only)

☑ Automatically close login success screen after 10 secs

(Setting the time to zero secs will not display the login success screen. Valid range: 0 - 300 secs.)

☑ Automatically close logout success screen after 5 secs (for Windows only)

(Setting the time to zero secs will not display the logout success screen. Valid range: 0 - 300 secs.)

Step 4 Under the User Role in Figure 5-77, select **Wireless Users**. Be sure to check **Require use of Clean Access Agent**.

For explanations and use of the other options on this page, refer to the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Step 5 Click **Update** when finished. This completes the minimum required configuration steps necessary to support a Unified Wireless deployment with NAC endpoint security. Using the configuration outlined in this guide, wireless users can auto-connect through the NAC appliance via the Clean Access Agent without undergoing any specific posture assessment or policy enforcement actions.

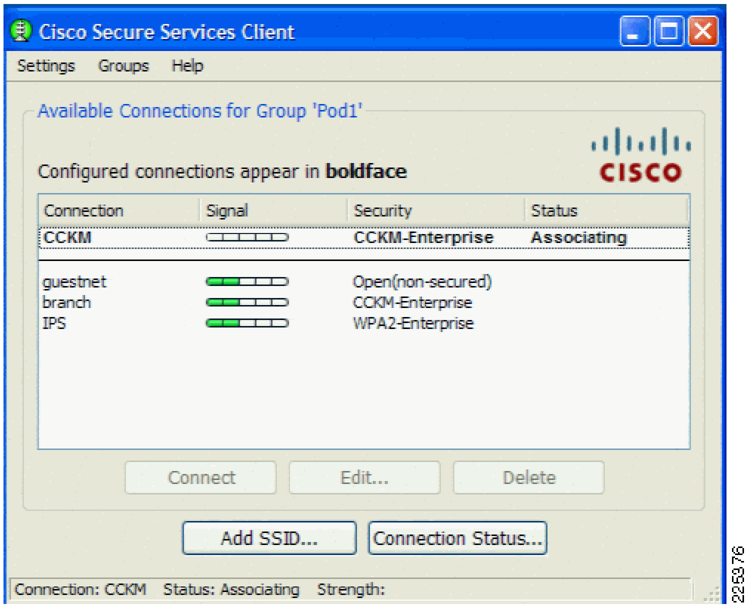
More configuration is required to create policies for posture assessment, quarantine, and remediation. It is beyond the scope of this document to cover those topics. For configuring Clean Access Agent rules, requirements, and role requirements, refer to Chapter 12 of the *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

End User Example—Wireless Single Sign-On

Figure 5-78 through Figure 5-86 show an example of wireless user SSO with Cisco NAC appliance endpoint security.

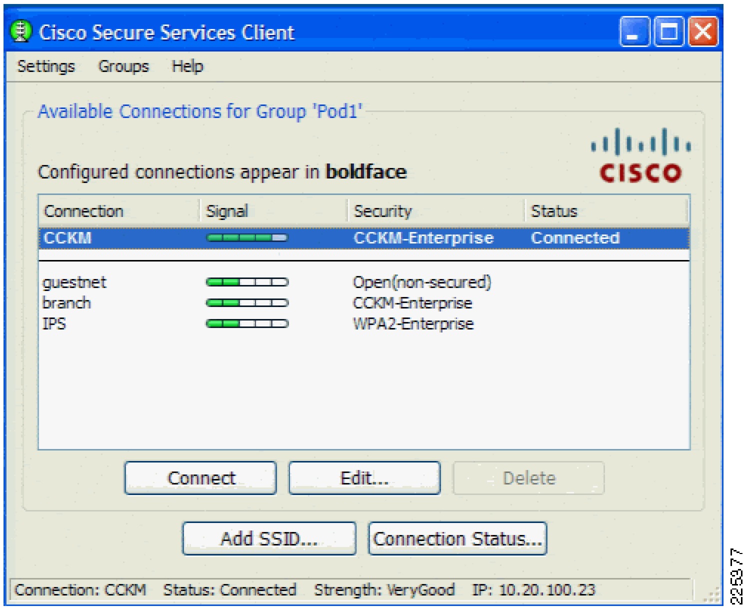
Figure 5-78 Wireless Client with CSSC Supplicant


Cisco Secure Services Client
Settings
Groups
Help
Available Connections for Group 'Pod1'
Configured connections appear in **boldface**
CISCO
Connect
Edit...
Delete
Add SSID...
Connection Status...
225376

Connection	Signal	Security	Status
CCKM		**CCKM-Enterprise**	**Associating**
guestnet		Open(non-secured)	
branch		CCKM-Enterprise	
IPS		WPA2-Enterprise	

Connection: CCKM Status: Associating Strength:

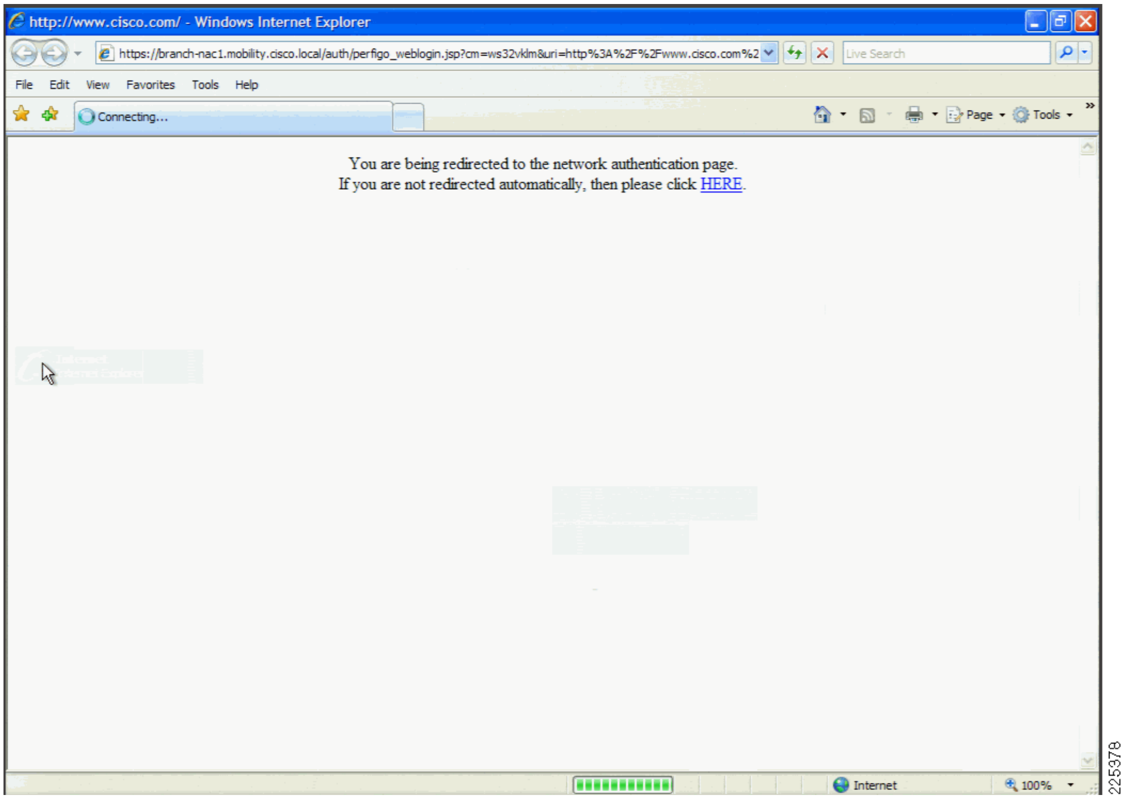
Figure 5-79 Successful 802.1x/PEAP Authentication and Association


Cisco Secure Services Client
Settings
Groups
Help
Available Connections for Group 'Pod1'
Configured connections appear in **boldface**
CISCO
Connect
Edit...
Delete
Add SSID...
Connection Status...
225377

Connection	Signal	Security	Status
CCKM		**CCKM-Enterprise**	**Connected**
guestnet		Open(non-secured)	
branch		CCKM-Enterprise	
IPS		WPA2-Enterprise	

Connection: CCKM Status: Connected Strength: VeryGood IP: 10.20.100.23

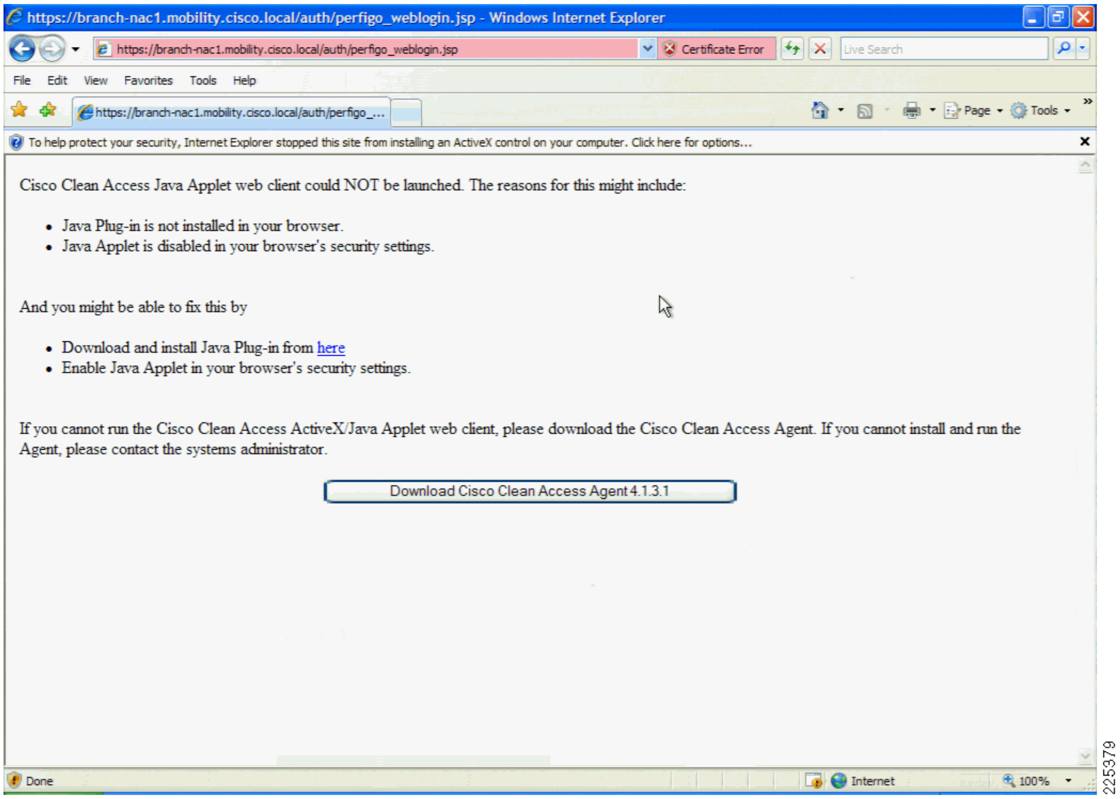
Figure 5-80 Browser Redirect to NAC Appliance User Page



http://www.cisco.com/ - Windows Internet Explorer
https://branch-nac1.mobility.cisco.local/auth/perfigo_weblogin.jsp?cm=ws32vklm&uri=http%3A%2F%2Fwww.cisco.com%2
Live Search
File
Edit
View
Favorites
Tools
Help
Connecting...
Page
Tools
Internet
100%
225378

You are being redirected to the network authentication page.
If you are not redirected automatically, then please click HERE.

Figure 5-81 Mandatory Policy to Use Clean Access Agent


https://branch-nac1.mobility.cisco.local/auth/perfigo_weblogin.jsp - Windows Internet Explorer
https://branch-nac1.mobility.cisco.local/auth/perfigo_weblogin.jsp
Certificate Error
Live Search
File Edit View Favorites Tools Help
https://branch-nac1.mobility.cisco.local/auth/perfigo_...
Page
Tools
To help protect your security, Internet Explorer stopped this site from installing an ActiveX control on your computer. Click here for options...
Done
Internet
100%
225379

Cisco Clean Access Java Applet web client could NOT be launched. The reasons for this might include:

- Java Plug-in is not installed in your browser.
- Java Applet is disabled in your browser's security settings.

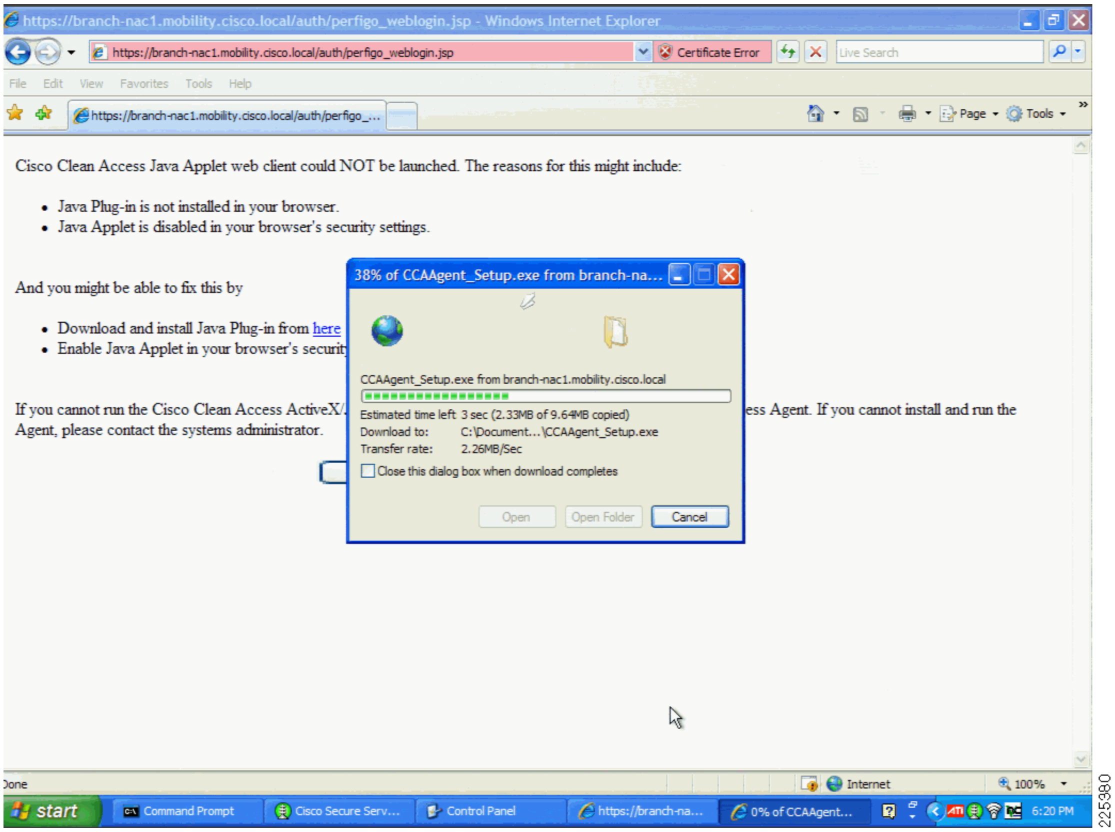
And you might be able to fix this by

- Download and install Java Plug-in from here
- Enable Java Applet in your browser's security settings.

If you cannot run the Cisco Clean Access ActiveX/Java Applet web client, please download the Cisco Clean Access Agent. If you cannot install and run the Agent, please contact the systems administrator.

Download Cisco Clean Access Agent 4.1.3.1

Figure 5-82 Clean Access Agent Installer Download



Cisco Clean Access Java Applet web client could NOT be launched. The reasons for this might include:

- Java Plug-in is not installed in your browser.
- Java Applet is disabled in your browser's security settings.

And you might be able to fix this by

- Download and install Java Plug-in from here
- Enable Java Applet in your browser's securit

If you cannot run the Cisco Clean Access ActiveX/ ... ess Agent. If you cannot install and run the Agent, please contact the systems administrator.

38% of CCAAgent_Setup.exe from branch-na...

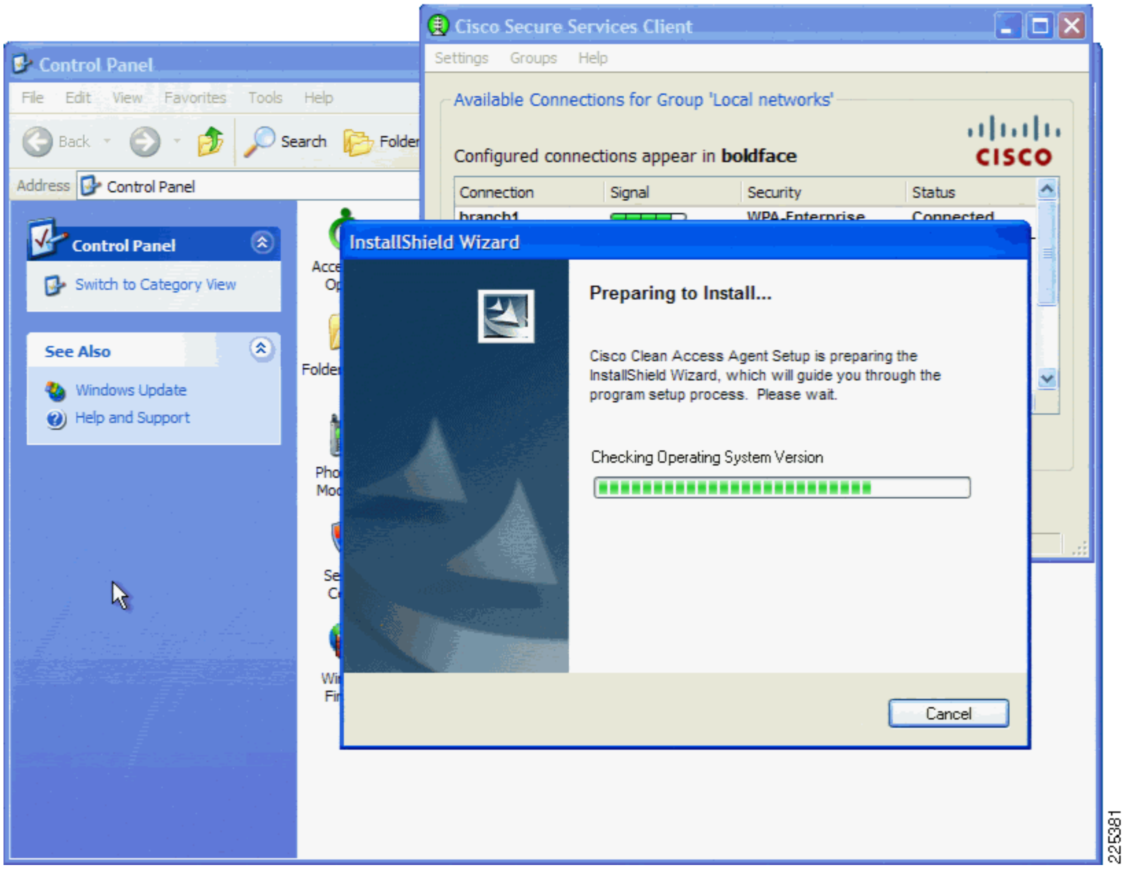
CCAAgent_Setup.exe from branch-nac1.mobility.cisco.local

Estimated time left 3 sec (2.33MB of 9.64MB copied)
Download to: C:\Document...\CCAAgent_Setup.exe
Transfer rate: 2.26MB/Sec

□ Close this dialog box when download completes

https://branch-nac1.mobility.cisco.local/auth/perfigo_weblogin.jsp - Windows Internet Explorer
https://branch-nac1.mobility.cisco.local/auth/perfigo_weblogin.jsp
Certificate Error
Live Search
File Edit View Favorites Tools Help
https://branch-nac1.mobility.cisco.local/auth/perfigo_...
Page
Tools
Open
Open Folder
Cancel
Done
Internet
100%
start
Command Prompt
Cisco Secure Serv...
Control Panel
https://branch-na...
0% of CCAAgent...
6:20 PM
225380

Figure 5-83 Clean Access Agent Auto Installation



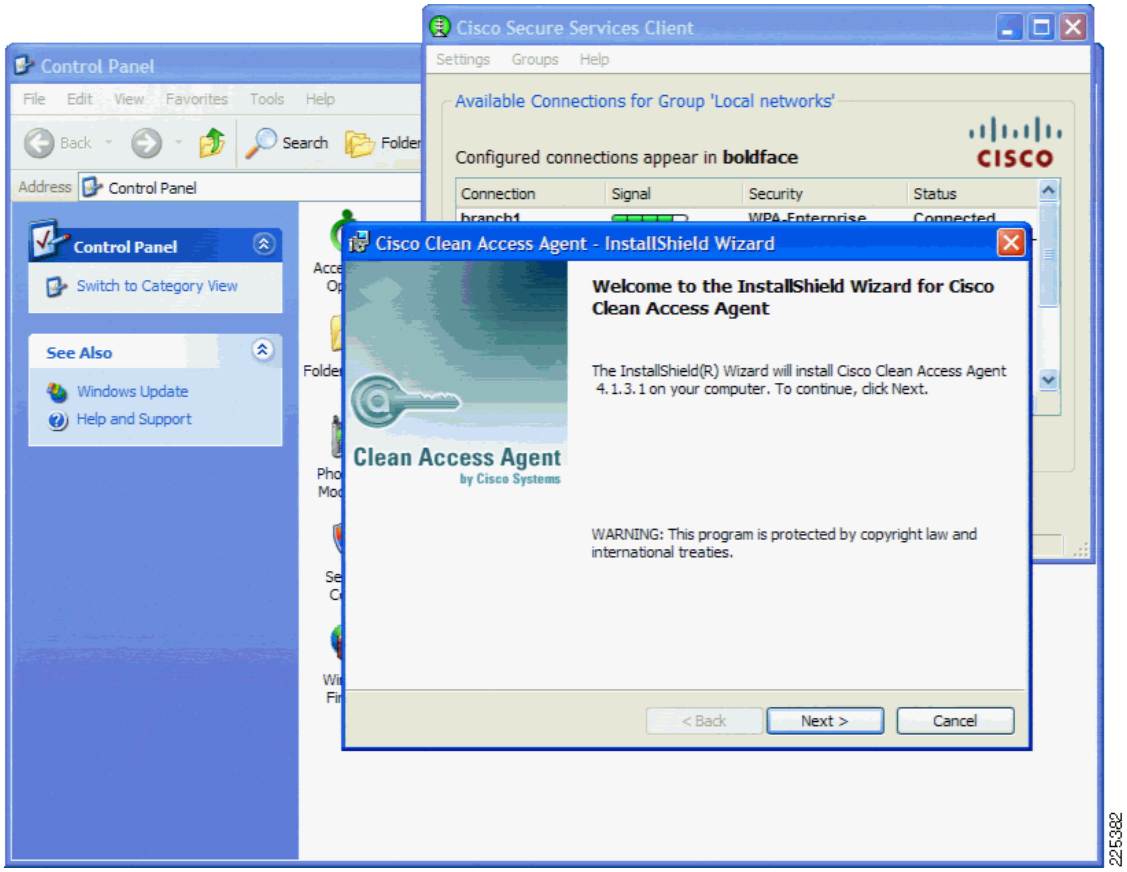
Configured connections appear in **boldface**

Preparing to Install...

Cisco Clean Access Agent Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Checking Operating System Version

Figure 5-84 Clean Access Agent Installation in Progress



Configured connections appear in **boldface**

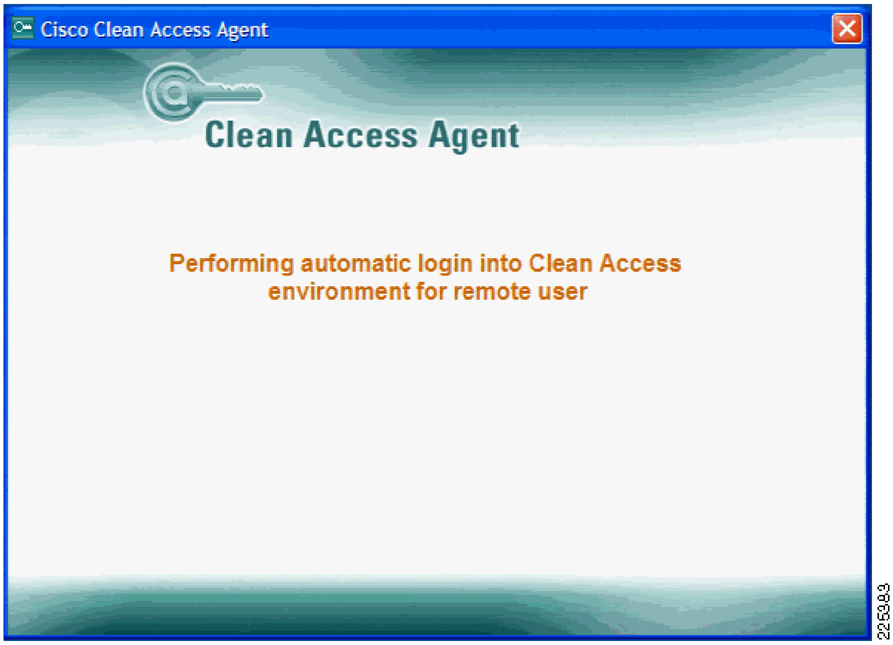
Connection	Signal	Security	Status
branch1		WPA-Enterprise	Connected

Welcome to the InstallShield Wizard for Cisco Clean Access Agent

The InstallShield(R) Wizard will install Cisco Clean Access Agent 4.1.3.1 on your computer. To continue, click Next.

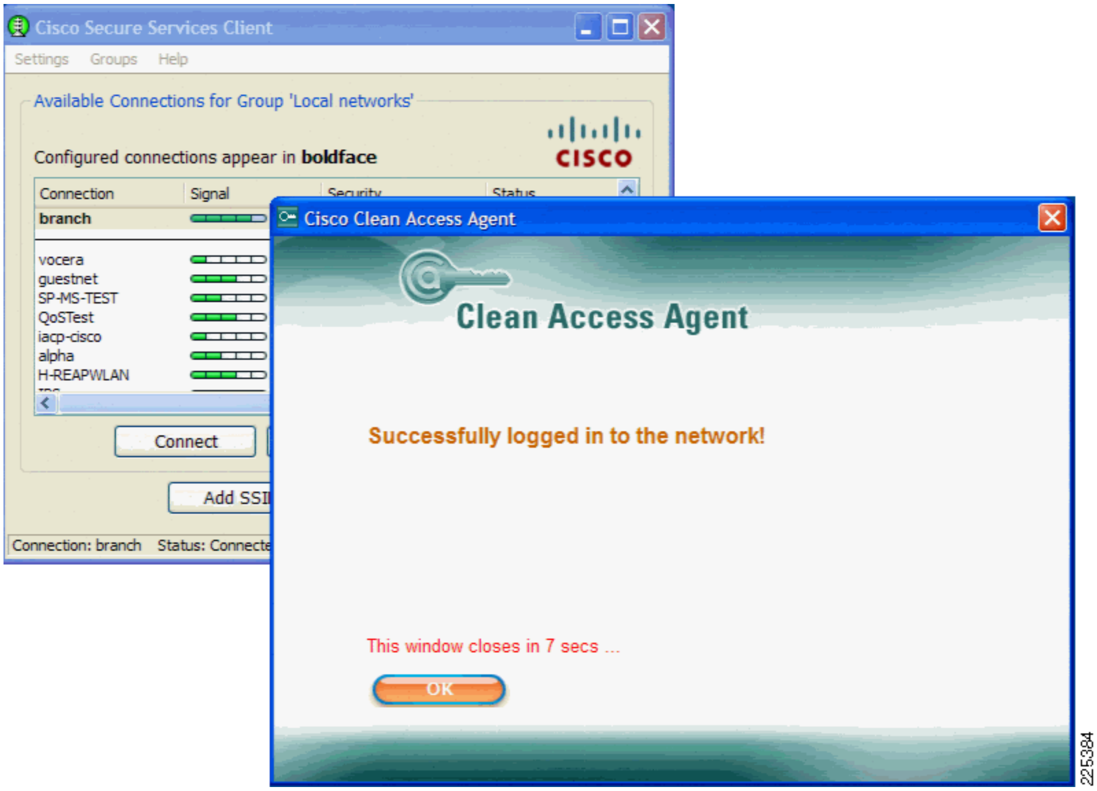
WARNING: This program is protected by copyright law and international treaties.

Figure 5-85 NAC Appliance Auto-Logon via Agent



Performing automatic login into Clean Access environment for remote user

Figure 5-86 Successful NAC Authentication



Available Connections for Group 'Local networks'

Configured connections appear in **boldface**

Connection: branch Status: Connecte

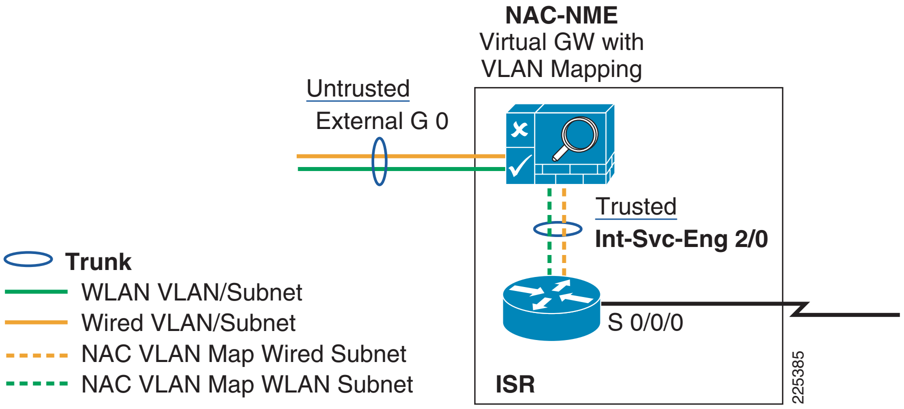
Successfully logged in to the network!

This window closes in 7 secs ...

Branch Deployments and NAC Network Module (NME)

The Cisco NAC Network Module is supported on modular Integrated Services Routers (ISR) with a network module slot—namely the Cisco 2811, 2821, 2851, 3825, and 3845 platforms. The Cisco NAC Network Module for ISRs (NME-NAC-K9) extends the Cisco NAC Appliance portfolio of products to smaller locations, helping enable network admission control (NAC) capabilities from the headquarters to the branch office. The integration of NAC appliance server capabilities into a network module for ISRs allows network administrators to manage a single device in the branch office for data, voice, and security requirements, reducing network complexity, IT staff training needs, equipment sparing requirements, and maintenance costs. The Cisco NAC Network Module for Integrated Services Routers deployed at the branch office remedies potential threats locally before they traverse the WAN and potentially infect the network. Figure 5-87 shows a schematic of the NAC NME and its integration into the ISR. The NAC-NME provides the same logical interfaces as the standard NAC Appliance, with trusted and untrusted interfaces. The untrusted interface is a physical RJ-45 connector on the NAC-NME, and the trusted interfaces is terminated on the ISR backplane.

Figure 5-87 NAC-NME and ISR Connections

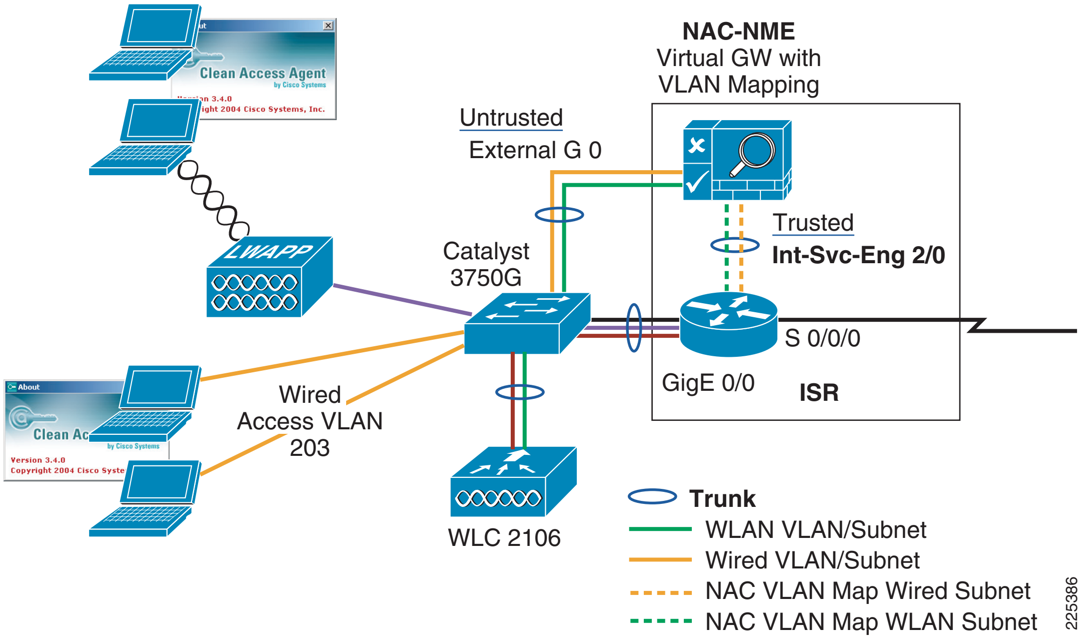


The NAC-NME is managed through the same interface and has the same feature set as the NAC appliance, apart from the high availability and scaling features of the NAC appliance. Because the configuration of the NAC-NME is through the same management interface as the NAC appliance and the same features are used, the configuration is not repeated here. Here, the focus is only the example network configuration shown in Figure 5-88.

High Availability Considerations

This NAC branch solution requires communication with a centralized Clean Access Manager; therefore, a high availability WAN connection is assumed for this design. This high availability WAN connection is also assumed for 802.1X/RADIUS authentication. While local EAP authentication features are available on the branch WLC for local authentication, no RADIUS accounting information is generated from these authentications, making it unsuitable for use in a VPN single sign implementation.

Figure 5-88 NAC-NME and Branch Connection Example



The following configuration shows how the NAC-NME trusted interface terminates on the ISR. As shown in the configuration, the NAC-NME trusted interface terminates as as a trunk interface with the **interface Integrated-Service-Engine2/0** command. the management interface of the the NAC-NME is native interface and client traffic is set on separate subinterfaces.

```
!
interface Integrated-Service-Engine2/0
 ip address 10.20.200.17 255.255.255.252
 service-module ip address 10.20.200.18 255.255.255.252
 no keepalive
!
interface Integrated-Service-Engine2/0.4
 description WLAN 204 Clients
 encapsulation dot1Q 4
 ip address 10.20.204.1 255.255.255.0
 ip helper-address 10.20.30.11
!
interface Integrated-Service-Engine2/0.6
 description Wired Clients
 encapsulation dot1Q 6
 ip address 10.20.206.1 255.255.255.0
 ip helper-address 10.20.30.11
```

Branch NAC and SSO

SSO is just as important for the branch as it is for the campus. In a branch deployment, the NAC NME is likely to be used by both wired and WLAN clients. If the wired clients are 802.1X authenticated at the branch switch then VPN SSO may be a suitable solution, but if the wired NAC clients are not using 802.1X/EAP authentication, then Active Directory SSO is the best SSO solution for the branch.

WLCM and the NAC-NME

The focus of the branch testing for this version of the design guide has been the design and testing of a design using the WLC 2106, but given that the Wireless LAN Controller Module (WLCM) is also potentially part of a branch deployment of the Cisco Unified Wireless Network, it is design was also considered in the NAC-NME implementation. The fundamental Cisco Unified Wireless Network and NAC configuration are the same for either the WLC 2106 or the WLCM. The primary difference between a WLC 2106 deployment and a WLCM deployment is driven by the WLCM terminating on the ISR. This means that WLAN client traffic needs to be routed to the NAC-NME, and requires a policy route to force outbound traffic through the NAC-NME. This is illustrated in Figure 5-89. Although a the policy route is able force outbound traffic through the NAC-NME it is unable to divert incoming traffic through the NAC-NME, as the WLAN client subnets are directly connected to the ISR. This is illustrated in Figure 5-90. Implementing integrated routing and bridging IRB or VPN routing and forwarding (VRF) to provide bridging or separate Layer 3 forwarding paths within the router may be a suitable mechanism for forcing WLCM client traffic through the NAC-NME in both directions, but this was not tested in this design guide.

Figure 5-89 WLCM and Policy Routing Outbound Traffic

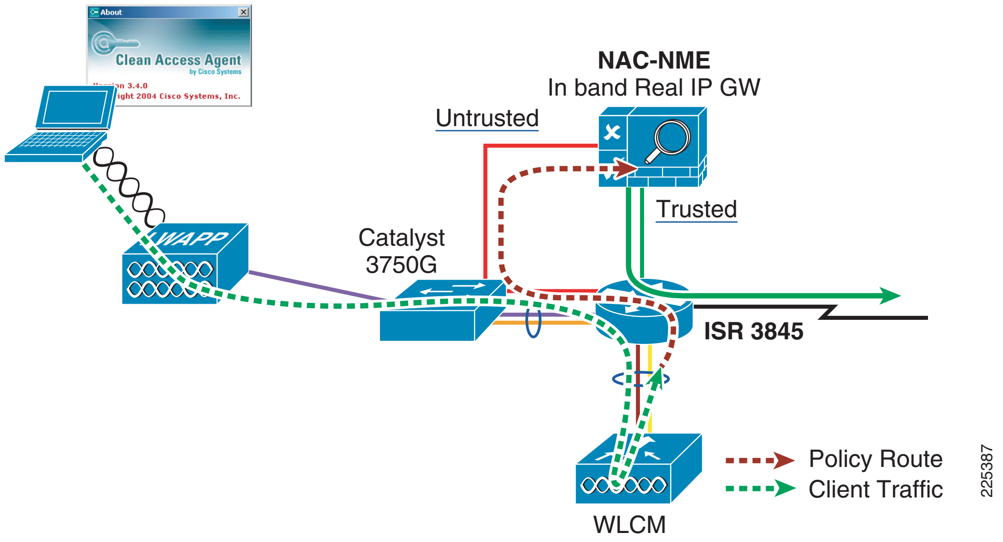
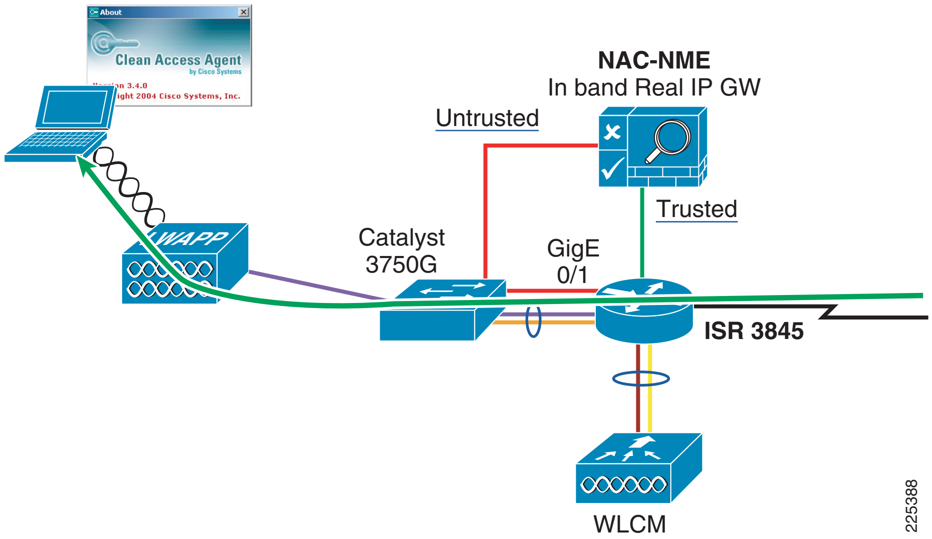


Figure 5-90 WLCM and Inbound Traffic

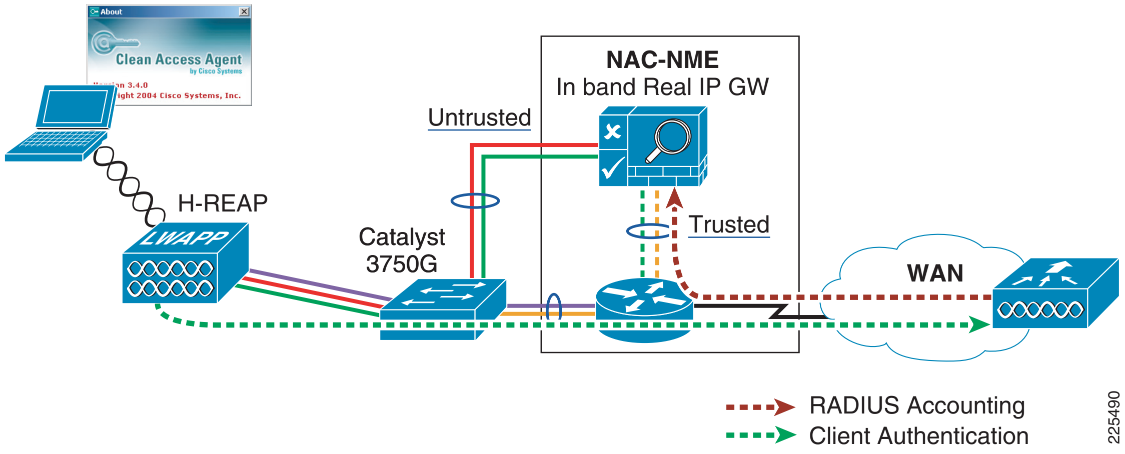


H-REAP and NAC-NME

Another possible Cisco Unified Wireless network branch deployment option is to use a H-REAP where the WLC provides H-REAP management, but WLAN client traffic can be terminated at the H-REAP interface as shown in Figure 5-91. An H-REAP dot1q trunk can terminate on a branch switch and these VLANs can be mapped to the NAC-NME untrusted interface. This makes the H-REAP client traffic path the same as the WLC 2106.

If using this mode of H-REAP, local branch NAC appliance and central WLC authentication SSO VPN is not recommended, because a central WLC managing multiple H-REAPs in different branch locations does not have a mechanism for determining the appropriate NAC NME to send RADIUS accounting messages to. For example, if there are multiple branches all with H-REAPs and NAC NMEs, the central WLC would typically be configured with the same WLANs for all the H-REAPs in the different branches, and the RADIUS authentications would be performed by the central WLC. The WLAN configuration in the central WLC will only have one preferred RADIUS accounting address for any of the WLAN clients, even though there would be multiple NAC NMEs.

Figure 5-91 H-REAP and NAC-NME


About
Clean Access Agent
by Cisco Systems
Version 3.4.0
ight 2004 Cisco Systems, Inc.
H-REAP
LWAPP
Catalyst
3750G
Untrusted
NAC-NME
In band Real IP GW
Trusted
WAN
RADIUS Accounting
Client Authentication
225490