CHAPTER 5

Enterprise Campus

The enterprise campus is the portion of the infrastructure that provides network access to end users and devices located at the same geographical location. It may span over several floors in a single building, or over multiple buildings covering a larger geographical area. The campus typically connects to a network core that provides access to the other parts of the network such as data centers, WAN edge, other campuses, and the Internet edge modules.

This chapter covers the best practices for implementing security within a campus network. It does not provide design guidance or recommendations on the type of distribution-access design that should be deployed within a campus network such as multi-tier, virtual switching system (VSS), or routed access designs. This chapter discusses the security best practices applicable to these designs.

For information on the various campus distribution-access designs, see the *Enterprise Campus 3.0 Architecture: Overview and Framework Document* at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html

From a security perspective, the following are the key requirements to be satisfied by the campus design:

- Service availability and resiliency
- Prevent unauthorized access, network abuse, intrusions, data leak, and fraud
- Ensure data confidentiality, integrity, and availability
- Ensure user segmentation
- Enforce access control
- Protect the endpoints
- Protect the infrastructure

Key Threats in the Campus

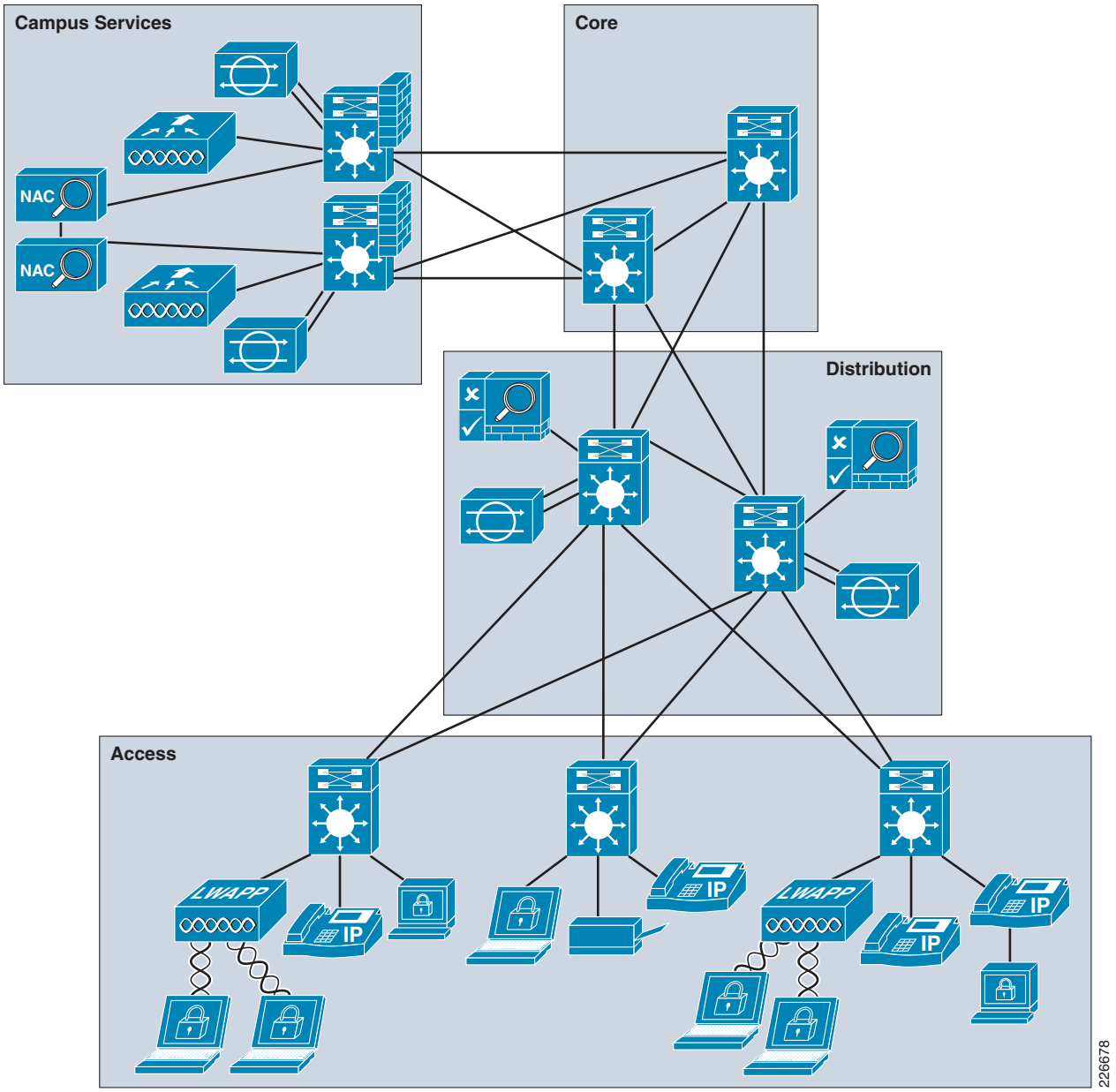
The following are some of the key threats that affect the campus:

- Service disruption—Botnets, malware, adware, spyware, viruses, DoS attacks (buffer overflows and endpoint exploitation), Layer-2 attacks, and DDoS on services and infrastructure.
- Unauthorized access—Intrusions, unauthorized users, escalation of privileges, IP Spoofing, and unauthorized access to restricted resources.
- Data disclosure and modification—Sniffing, man-in-the-middle (MITM) attacks of data while in transit.
- Network abuse—Peer-to-peer and instant messaging abuse, out-of-policy browsing, and access to forbidden content.
- Data leak—From servers and user endpoints, data in transit and in rest.
- Identity theft and fraud—On servers and end users, phishing, and E-mail spam.

Enterprise Campus Design

The campus design follows a modular hierarchical design comprising of core, distribution, and access layers. An optional services block using a set of switches providing distribution/access services may be implemented to host certain services for the local campus users. The modular hierarchical design segregates the functions of the network into separate building blocks to provide for availability, flexibility, scalability, and fault isolation. Redundancy is achieved by implementing switches in pairs, deploying redundant links, and implementing dynamic routing protocols. This results in a full topological redundancy as illustrated in Figure 5-1.

Figure 5-1 Campus Design



In the typical hierarchical model, the individual network modules such as the data center, WAN edge, Internet edge, and other campuses are interconnected using the core layer switches. As discussed in Chapter 3, "Enterprise Core," the core serves as the backbone for the network. The core needs to be fast and extremely resilient because every building block depends on it for connectivity. A minimal configuration in the core reduces configuration complexity limiting the possibility for operational error.

The distribution layer acts as a services and control boundary between the access and core layers. It aggregates switches from the access layer and protects the core from high-density peering requirements from the access layer. Additionally, the distribution block provides for policy enforcement, access control, route aggregation, and acts as an isolation demarcation between the access layer and the rest of

the network. Typically, deployed as a pair (or multiple pairs) of Layer 3 switches for redundancy, the distribution layer uses Layer-3 switching for its connectivity to the core layer and Layer 2 trunks or Layer 3 point-to-point routed interfaces for its connectivity to the access layer.

The access layer is the first point of entry into the network for edge devices, end stations, and IP phones. The switches in the access layer are connected to two separate distribution-layer switches for redundancy. The access switches in the access layer can connect to the distribution layer switches using Layer 2 trunks or Layer-3 point-to-point routed interfaces.

Within the enterprise campus, an optional campus services block may be deployed to provide application services to end users and devices within the campus network such as centralized LWAPP wireless controllers and IPv6 ISATAP tunnel termination. Additionally, for small campuses that only require a few servers, this block could also be used to host a small number of localized foundational servers such as local DHCP, DNS, FTP, and NAC Profiler servers. For larger campuses requiring many servers, a data center design should be deployed to host these servers using the security best practices described in Chapter 4, "Intranet Data Center."

There are three basic choices for deploying the distribution-access design within a campus network. They include:

- Multi-Tier, page 5-4
- Virtual Switch System (VSS), page 5-6
- Routed Access, page 5-7

While all three of these designs use the same basic physical topology and cable plant, there are differences in where the Layer-2 and Layer-3 boundaries exist, how the network topology redundancy is implemented, and how load-balancing works-along with a number of other key differences between each of the design options. The following sections provide a short description of each design option. A complete description for each of these design models can be found within the *Enterprise Campus 3.0 Architecture: Overview and Framework* document at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html

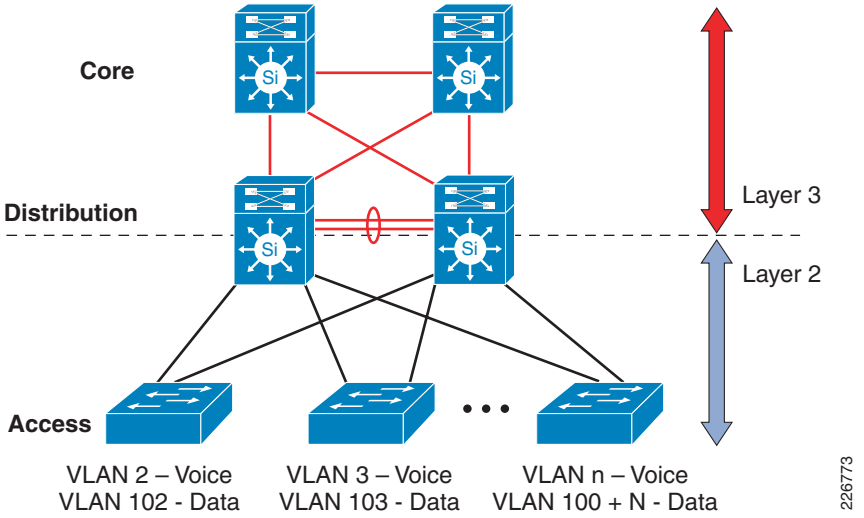
Multi-Tier

In a multi-tier distribution-access design, all the access switches are configured to run in Layer-2 forwarding mode and the distribution switches are configured to run both Layer-2 and Layer-3 forwarding. VLAN-based trunks are used to extend the subnets from the distribution switches down to the access layer. A default gateway protocol such as Hot Standby Router Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP) is run on the distribution layer switches along with a routing protocol to provide upstream routing to the core of the campus. One version of spanning tree and the use of the spanning tree hardening features (such as Loopguard, Rootguard, and BPDUGuard) are configured on the access ports and switch-to-switch links as appropriate.

Note It is a good practice to implement Per VLAN Spanning Tree (PVST). PVST defines a separate instance of spanning tree for each VLAN configured in the network, making the network more resilient from attacks against spanning tree. Cisco switches support several versions of PVST, including PVST+ and Rapid-PVST+. Rapid-PVST+ provides faster convergence of the spanning tree by using Rapid Spanning Tree Protocol (RSTP).

The multi-tier design has two basic variations that primarily differ only in the manner in which VLANs are defined. In the looped design, one-to-many VLANs are configured to span multiple access switches. As a result, each of these *spanned* VLANs has a spanning tree or Layer-2 looped topology. The other alternative—*loop-free*— design follows the current best practice guidance for the multi-tier design and defines unique VLANs for each access switch as shown in Figure 5-2.

Figure 5-2 Multi-Tier Design

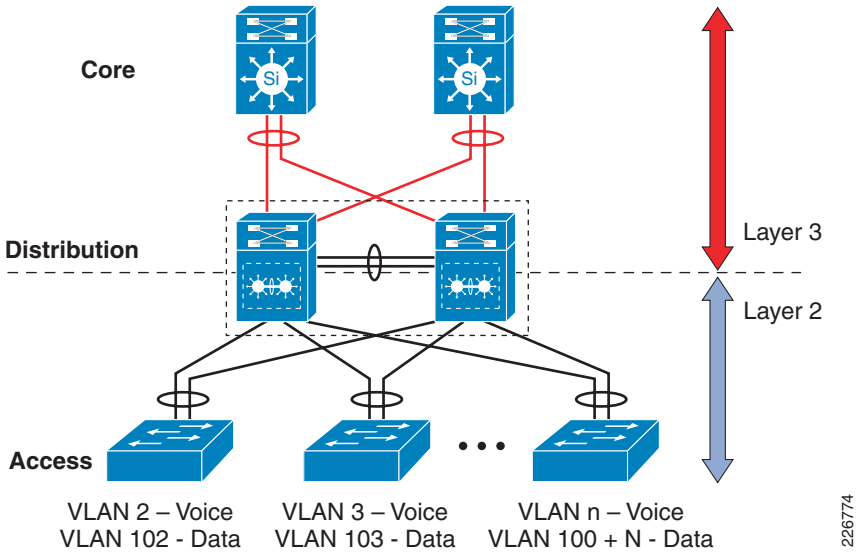


The detailed design guidance for the multi-tier distribution block design can be found in the campus section of the Cisco Design Zone website at http://www.cisco.com/go/designzone

Virtual Switch System (VSS)

In the VSS design, the distribution switch pair acts as a single logical switch. By converting the redundant physical distribution switches into a single logical switch, a significant change is made to the topology of the network. Rather than an access switch configured with two uplinks to two distribution switches and needing a control protocol to determine which of the uplinks to use, now the access switch has a single multi-chassis Etherchannel (MEC) upstream link connected to a single distribution switch. This design is illustrated in Figure 5-3.

Figure 5-3 VSS Design



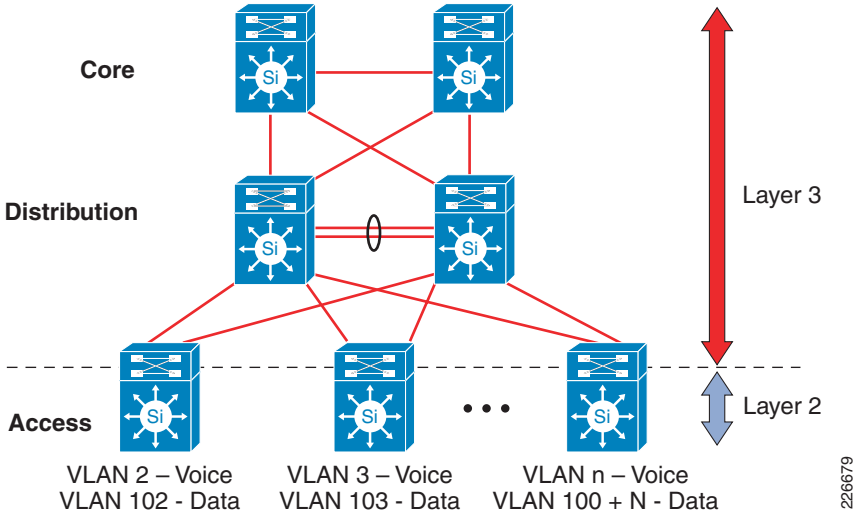
For details on the design of the virtual switching distribution design, see the upcoming virtual switch distribution block design guide at http://www.cisco.com/go/designzone

Routed Access

In a routed access design, the access switches act as a full Layer-3 routing node providing both Layer-2 and Layer-3 switching and acts as the Layer 2/3 demarcation point in the campus network design. Layer-3 point-to-point routed interfaces are used to connect to the distribution switches. Each access switch is configured with unique voice, data, and any other required VLANs. In addition, in a routed access design, the default gateway and root bridge for these VLANs exists on the access switch.

Figure 5-4 illustrates the Layer-3 routed access design.

Figure 5-4 Routed Access Design

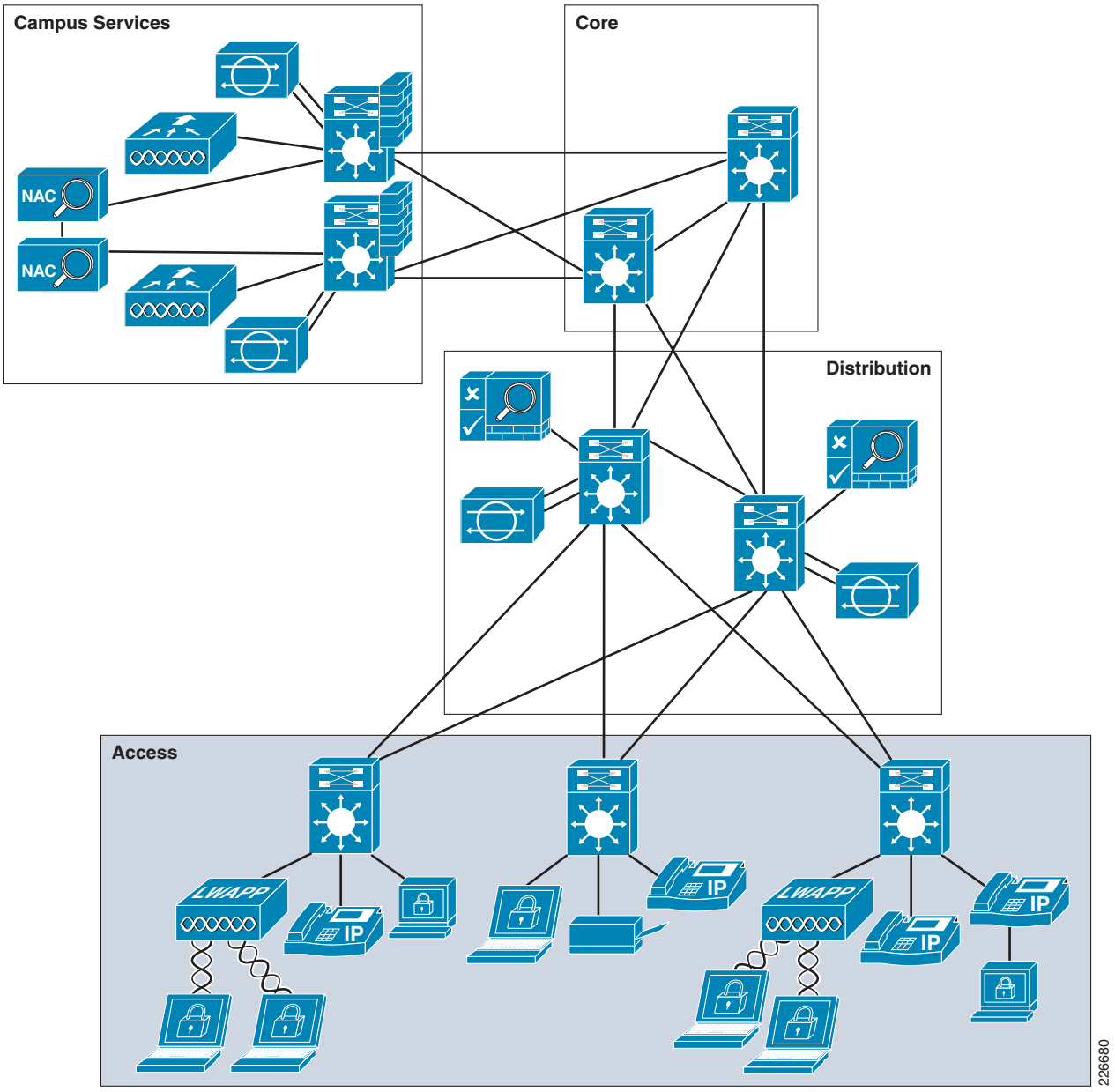


The detailed design guidance for the routed access distribution block design can be found in the campus section of the Cisco Design Zone site at http://www.cisco.com/go/designzone

Campus Access Layer

The campus access layer is the first tier or edge of the campus where end devices such as end-user workstations, printers, and cameras attach to the wired portion of the network. Additionally, this is also where devices such as IP phones and wireless access points (APs) are attached to extend the network out from the access switches. Each access switch is deployed with redundant links to the distribution layer switches. See Figure 5-5.

Figure 5-5 Campus Access Module Design



Campus Access Layer Design Guidelines

The campus access layer provides the demarcation point between the network infrastructure and the end devices that use the network infrastructure. It is the first line of defense in the network against threats generated by devices connecting to them. This section discusses the various security measures used for securing the campus access layer, including the following:

- Securing the endpoints using endpoint security software
- Securing the access infrastructure and protecting network services including DHCP, ARP, IP spoofing protection and protecting against inadvertent loops using Network Foundation Protection (NFP) best practices and Catalyst Integrated Security Features (CISF).

Endpoint Protection

Network endpoints are defined as any systems that connect to the network and communicate with other entities over the network infrastructure such as servers, desktop computers, laptops, printers, and IP phones. These endpoints can vary greatly in hardware types, operating systems, and applications making it very difficult to keep them updated with latest patches to vulnerabilities and virus signature files. In addition, portable devices such as laptops can be used at hotels, employee's homes, and other places outside the corporate controls making it difficult to protect these devices. The list of threats to these endpoints include malware, adware, spyware, viruses, worms, botnets, and E-mail spam.

The vulnerability of any particular endpoint can impact the security and availability of an entire enterprise. Thus, endpoint security is a critical element of an integrated, defense-in-depth approach to protecting both clients and servers themselves and the network to which they connect. The first step in properly securing the endpoints requires end-user awareness and the adoption of the appropriate technical controls. End-users must be continuously educated on current threats and the security measures needed for keeping endpoints up-to-date with the latest updates, patches, and fixes. In addition, this must be complemented by implementing a range of security controls focused on protecting the endpoints such as endpoint security software, network-based intrusion prevention systems, and web and E-mail traffic security.

Endpoint security software must harden the endpoint against an initial attack as well the activities associated with compromised endpoints. The key elements include the following:

- Protection against known attacks— Signature-based threat detection and mitigation such as known worms and viruses.
- Protection against zero-day or unpatched attacks—Behavioral-based threat detection and mitigation such as attempts to load an unauthorized kernel driver, capture keystrokes, buffer overflows, modify system configuration settings, and inset code into other processes.
- Policy enforcement—Visibility and protection against non-compliant behavior such as data loss, unauthorized access, and network and application abuse.

These elements are addressed by host-based intrusion prevention systems (HIPS) such as the Cisco Security Agent (CSA). The Cisco SAFE leverages CSA on end-user workstation and servers to provide endpoint security. CSA takes a proactive and preventative approach, using behavior-based and signature-based security to focus on preventing malicious activity on the host. Cisco Security Agents are centrally managed using the Management Center for Cisco Security Agents (CSA-MC) including behavioral policies, data loss prevention, and antivirus protection. The CSA-MC also provides centralized reporting and global correlation.

CSA can be deployed in conjunction with IPS to enhance threat visibility within the network. CSA can provide endpoint posture information to IPS to reduce false-positives and allow dynamic quarantine of compromised hosts. For more information on CSA and IPS collaboration, refer to Chapter 11, "Threat Control and Containment."

Access Security Best Practices

In addition to protecting the endpoints themselves, the infrastructure devices and network services such as DHCP and ARP also need to be protected. Cisco SAFE leverages the NFP security best practices and the Catalyst Integrated Security Features (CISF) for hardening the access switches in the campus access layer. This includes restricting and controlling administrative access, protecting the management and control planes, securing the dynamic exchange of routing information, and securing the switching infrastructure.

The following are the key areas of the NFP best practices applicable to securing the access layer switches. All best practices listed below are applicable to the access switches in all three distribution-access design models unless otherwise noted:

- Infrastructure device access
  - Implement dedicated management interfaces to the out-of-band (OOB) management network; for more information on implementing an OOB management network, refer to Chapter 9, "Management."
  - Limit the accessible ports and restrict the permitted communicators and the permitted methods of access.
  - Present legal notification.
  - Authenticate and authorize access using AAA.
  - Log and account for all access.
  - Protect locally stored sensitive data (such as local passwords) from viewing and copying.
- Routing infrastructure
  - Authenticate routing neighbors.
  - Use default passive interfaces.
  - Log neighbor changes.
  - Implement EIGRP stub routing.

Note Routing infrastructure protection is only applicable in the access layer of a routed access design since Layer-3 routing is enabled between the access and distribution switches. In a multi-tier and VSS design, this is enabled in the distribution layer.

- Device resiliency and survivability
  - Disable unnecessary services.
  - Filter and rate-limit control-plane traffic.
  - Implement redundancy.
- Network telemetry
  - Implement NTP to synchronize time to the same network clock.
  - Maintain and monitor device global and interface traffic statistics.

  - Maintain system status information (memory, CPU, and process).
  - Log and collect system status, traffic statistics, and device access information.
- Network policy enforcement
  - Implement management and infrastructure ACLs (iACLs).

Note iACLs are only applicable in the access layer of a routed access design where the routed edge interface is on the access switches. In a multi-tier and VSS design, this is enabled in the distribution layer.

  - Protect against IP spoofing using IP Source Guard on access ports and uRPF on routed edge interfaces.

Note URPF is only applicable in the access layer of a routed access design where the routed edge interface is on the access switches. In a multi-tier and VSS design, this is enabled in the distribution layer.

For more information on many of the NFP security best practices listed above, including design and configuration guidelines for each of the areas, refer to the Chapter 2, "Network Foundation Protection." Additional details and requirements for implementing switching security and infrastructure ACLs in the campus access layer are provided in the following subsections.

Switching Security

The campus access layer switching infrastructure must be resilient to attacks including direct, indirect, intentional, and unintentional types of attacks. In addition, they must offer protection to users and devices within the Layer 2 domain. The key measures for providing switching security on the access switches include the following:

- Restrict broadcast domains
- Spanning Tree Protocol (STP) Security—Implement Rapid Per-VLAN Spanning Tree (Rapid PVST+), BPDU Guard, and STP Root Guard to protect against inadvertent loops
- DHCP Protection—Implement DHCP snooping on access VLANs to protect against DHCP starvation and rogue DHCP server attacks
- IP Spoofing Protection—Implement IP Source Guard on access ports
- ARP Spoofing Protection—Implement dynamic ARP inspection (DAI) on access VLANs
- MAC Flooding Protection—Enable Port Security on access ports
- Broadcast and Multicast Storm Protection—Enable storm control on access ports
- VLAN Best Common Practices
  - Restrict VLANs to a single switch
  - Configure separate VLANs for voice and data
  - Configure all user-facing ports as non-trunking (DTP off)
  - Disable VLAN dynamic trunk negotiation trunking on user ports
  - Explicitly configure trunking on infrastructure ports rather than autonegotiation
  - Use VTP transparent mode

- Disable unused ports and place in unused VLAN
- Do not use VLAN 1 for anything
- Use all tagged mode for native VLAN on trunks

Port Security Considerations

Port security builds a list of secure MAC addresses in one of the following two ways, configurable on a per-interface basis:

- Dynamic learning of MAC addresses—Defines a maximum number of MAC addresses that will be learned and permitted on a port. This is useful for dynamic environments, such as at the access edge.
- Static configuration of MAC addresses—Defines the static MAC addresses permitted on a port. This is useful for static environments, such as a serverfarm, a lobby, or a demilitarized network (DMZ).

Typical port security deployment scenarios consist of the following:

- A dynamic environment, such as an access edge, where a port may have port security enabled with the maximum number of MAC addresses set to one, enabling only one MAC address to be dynamically learned at a time, and a security violation action of *protect* enabled.
- A static, controlled environment, such as a serverfarm or a lobby, where a port may have port security enabled with the server or lobby client MAC address statically defined and the more severe security violation response action of *shutdown* is enabled.
- A VoIP deployment, where a port may have port security enabled with the maximum number of MAC addresses defined as three. One MAC address is required for the workstation, and depending on the switch hardware and software, one or two MAC addresses may be required for the phone. In addition, it is generally recommended that the security violation action be set to *restrict* so that the port is not entirely taken down when a violation occurs.

For more information on switching security, including design and configuration guidelines for many areas highlighted above, refer to the Chapter 2, "Network Foundation Protection." The specific requirements and implementation of DHCP protection, ARP spoofing protection and storm protection in the campus access layer are covered in detail below.

DHCP Protection

DHCP protection is critical to ensure that a client on an access edge port is not able to spoof or accidentally bring up a DHCP server, nor exhaust the entire DHCP address space by using a sophisticated DHCP starvation attack. Both these attacks are addressed with the Cisco IOS DHCP snooping feature that performs two key functions to address these attacks:

- Rogue DHCP Server Protection—If reserved DHCP server responses (DHCPOFFER, DHCPACK, and DHCPNAK) are received on an untrusted port (such as an access port), the interface is shut down.
- DHCP Starvation Protection—Validates that the source MAC address in the DHCP payload on an untrusted (access) interface matches the source MAC address registered on that interface.

DHCP snooping is enabled on a per-VLAN basis and all interfaces in that VLAN are untrusted by default. Consequently, an interface hosting a DHCP server must be explicitly defined as trusted.

Note DHCP snooping rate-limiting should be enabled to harden the switch against a resource exhaustion-based DoS attack.

A sample DHCP snooping configuration on a Catalyst 4500 deployed in a routed access design is shown below. Similar configuration can be used in a multi-tier or VSS design. An example DHCP snooping rate-limit value of 15 pps is shown. The recommended rate-limit value depends on whether it is applied on trusted or untrusted interfaces, access or trunk ports, the size of the access switch, and the amount of acceptable DHCP traffic.

```
!
! On each interface in a VLAN where DHCP Snooping is to be enforced (access data and voice
VLANs)
! Rate limit DHCP snooping to ensure device resiliency
interface x/x
 switchport access vlan 120
 switchport mode access
 switchport voice vlan 110
 ip dhcp snooping limit rate 15
!
! Define the VLANs on which to enforce DHCP Snooping in global configuration mode
ip dhcp snooping vlan 100,110,120
! DHCP Option 82 is not being used, so it is disabled
no ip dhcp snooping information option
! Enable DHCP Snooping
ip dhcp snooping
!
! Enable automatic re-enablement of an interface shutdown due to the DHCP rate limit being
exceeded
errdisable recovery interval 120
errdisable recovery cause dhcp-rate-limit
!
```

For more information on the DHCP snooping feature, refer to the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/dhcp.html

ARP Spoofing Protection

ARP spoofing protection ensures that a client on an access edge port is not able to perform a MITM attack by sending a gratuitous ARP that presents its MAC address as that associated with a different IP address, such as that of the default gateway. This attack is addressed with the Cisco IOS Dynamic ARP Inspection (DAI) feature that validates that the source MAC and IP address in an ARP packet received on an untrusted interface matches the source MAC and IP address registered on that interface.

DAI is enabled on a per-VLAN basis and all interfaces in that VLAN are untrusted by default. Consequently, a device that does not use DHCP, such as the default gateway, ARP inspection must be bypassed by either explicitly defining the interface it is connected to as trusted, or creating an ARP inspection ACL to permit the source MAC and IP address of that device.

The following is a sample DAI configuration on a Cisco Catalyst 4500 deployed in a routed access design. Similar configuration can be used in a multi-tier or VSS design. The ARP inspection rate-limit of 100 pps is given as an example. The recommended value depends on the individual network environment, including type of access switch and the amount of valid ARP request traffic.

```
!
! Define the VLANs on which to enforce DAI (e.g. access and voice VLANs)
ip arp inspection vlan 100,110,120
!
! Enable automatic re-enablement of an interface shut down due to the DAI rate limit being
exceeded
errdisable recovery cause arp-inspection
errdisable recovery interval 120
!
! On each interface in a VLAN where DAI is enforced, rate limit DAI to ensure device
resiliency
```

```
interface x/x
 switchport access vlan 120
 switchport mode access
 switchport voice vlan 110
 ip arp inspection limit rate 100
!
```

For more information on the DAI feature, refer to the Infrastructure Protection on Cisco Catalyst 6500 and 4500 Series Switches whitepaper at the following URL:

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a0080825564.pdf

Traffic Storm Protection

When a large amount of broadcast (and/or multicast) packets congest a network, the event is referred to as a broadcast storm. A storm occurs when broadcast or multicast packets flood the subnet, creating excessive traffic and degrading network performance. Storm control prevents LAN interfaces from being disrupted by these broadcast and multicast storms. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service (DoS) attack can cause a storm.

Storm control (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold. Once the suppression-level threshold is reached, the port blocks traffic until the traffic falls below the threshold level.

The following is a sample storm-control configuration on a Cisco Catalyst 4500 deployed in a routed access design. Similar configuration can be used in a multi-tier or VSS design. The threshold value of 1 percent is given as an example. The recommended value depends on the broadcast and multicast traffic characteristics of individual networks. Different networks may have varying degrees of acceptable broadcast or multicast traffic.

```
! Configure broadcast storm-control and define the upper level suppression threshold on
! the access ports
! Configure a trap to be sent once a storm is detected
interface x/x
 switchport access vlan 120
 switchport mode access
 switchport voice vlan 110
 storm-control broadcast level 1.00
 storm-control action trap
! Enable multicast suppression on ports that already have broadcast suppression enable
! This is configured in the global configuration
storm-control broadcast include multicast
```

For more information on configuring Storm control, refer to the *Infrastructure Protection on Cisco Catalyst 6500 and 4500 Series Switches* whitepaper at the following URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a0080825564.pdf

Infrastructure ACLs

Proper network policy-enforcement at the edge of a network ensures that traffic entering the network conforms to the general and corporate network policy. Direct access to the infrastructure devices and management network should be strictly controlled to minimize the risk of exposure. Infrastructure ACLs (iACLs) are deployed to restrict direct access to the network infrastructure address space and should be deployed closest to the edge as possible. In addition, management ACLs are deployed to restrict access to the address space assigned to the management network. In a routed access design, iACLs are applied on the client gateway interface on the access switches. If the access switches connect to an OOB

management network, management ACLs are applied on the interface connecting to the OOB management network. If they are being managed in-band, then the management ACLs should be incorporated into the iACLs.

The following should be considered when implementing iACLs:

- A carefully planned addressing scheme will simplify deployment and management.
- Ping and traceroute traffic can be allowed to facilitate troubleshooting.
- Block client access to addresses assigned to the infrastructure devices.
- Block client access to addresses assigned to the network management subnet.
- Permit client transit traffic.

A sample configuration fragment for an access edge iACL in Cisco IOS is provided below. For detailed information on defining iACLs, refer to Chapter 2, "Network Foundation Protection."

```
! Define Campus Edge infrastructure ACL
ip access-list extended campus_iACL
! permit clients to perform ping and traceroutes needed for troubleshooting
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo

! Deny Client Access to Network Infrastructure Address Space
 deny ip any <MGMT_Network_subnet> <inverse-mask>
 deny ip any <Network_Infrastructure_subnet> <inverse-mask>
! Permit All Other Client Traffic not destined to Infrastructure addresses (transit
traffic)
 permit ip any any

! Apply Campus Edge iACL to the client default gateway interface on access switch
interface Vlan100
 description VLAN 100 - Client Data VLAN
 ip address 10.240.100.1 255.255.255.0
 ip access-group campus_iACL in
```

Note It is not necessary to specify the particular access subnet as the source address in the ACL entries if IP source address validation is already being enforced; for example, through IP Source Guard on the access ports. This enables generic and consistent iACLs to be deployed across the enterprise access edge, thereby minimizing the operational overhead.

Management ACLs are used to restrict traffic to and from the OOB management network. If the access switches connect directly to an OOB management network using a dedicated management interface, management access-lists using inbound and outbound access-groups are applied to the management interface to only allow access to the management network from the IP address assigned to the management interface assigned to the managed device and, conversely, only allow access from the management network to that management interface address. Data traffic should never transit the devices using the connection to the management network. In addition, the management ACL should only permit protocols that are needed for the management of these devices. These protocols could include SSH, NTP, FTP, SNMP, TACACS+, etc.

For further information on the OOB management best practices and sample management ACL configuration, refer to Chapter 9, "Management."

Operational Considerations

The operational management of the switching infrastructure can be greatly enhanced by using Smartports macros on a Cisco switch. Smartports macros enable customized port templates to be defined according to corporate policy and applied to ports on an as-needed basis. Each SmartPort macro is a set of CLI commands that the user define. SmartPort macro sets do not contain new CLI commands; each SmartPort macro is a group of existing CLI commands. When the user apply a SmartPort macro on an interface, the CLI commands contained within the macro are configured on the interface. When the macro is applied to an interface, the existing interface configurations are not lost. The new commands are added to interface and are saved in the running configuration file. In addition, there are Cisco default Smartports macros embedded in the switch software that can be used. The use of SmartPort macros ensures consistent policy enforcement, eases operations and avoids misconfiguration. For more information on Smartports macros, refer to the following URL:

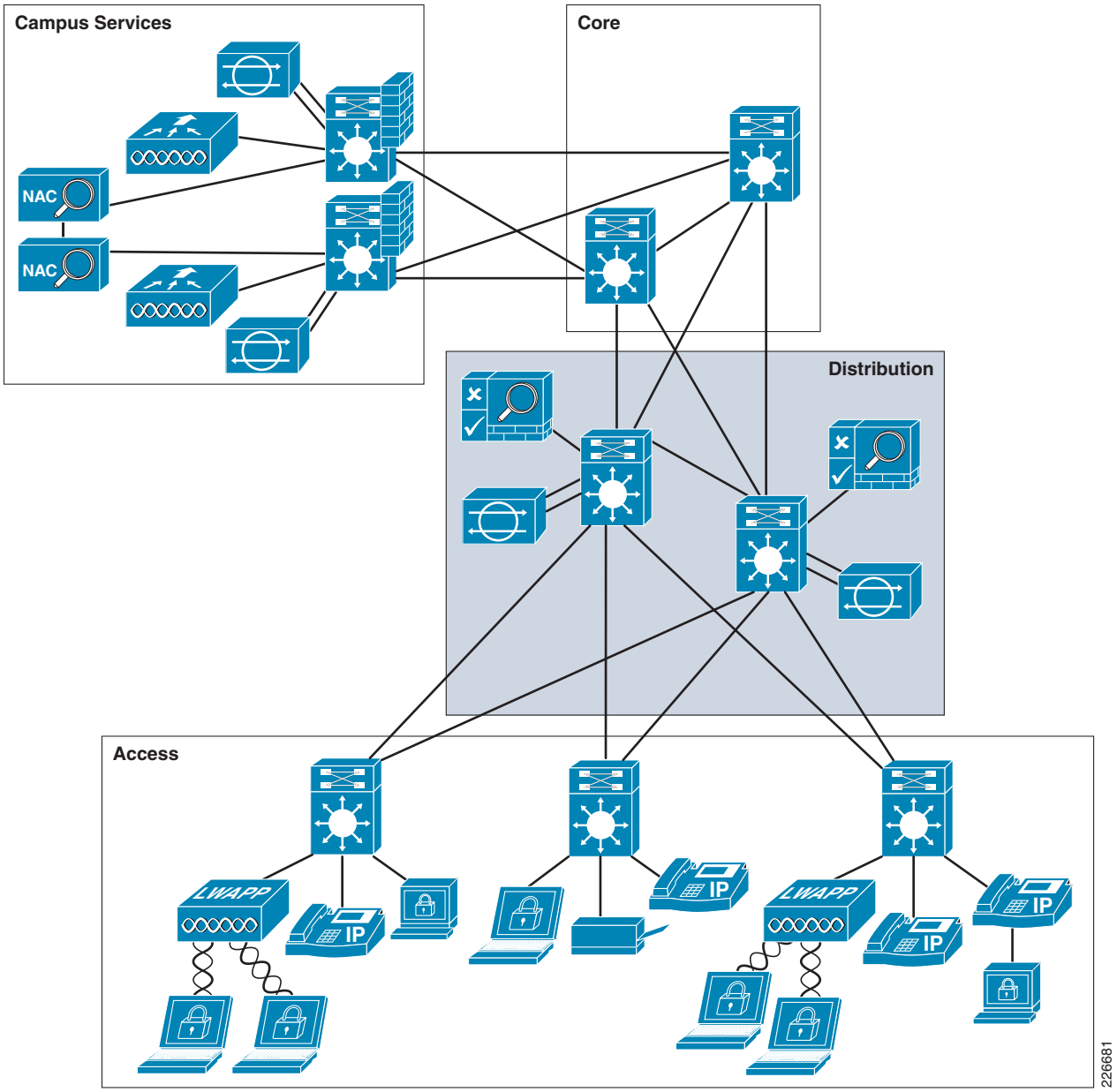
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/macro.html

Campus Distribution Layer

The campus distribution layer acts as a services and control boundary between the campus access layer and the enterprise core. It is an aggregation point for all of the access switches providing policy enforcement, access control, route and link aggregation, and the isolation demarcation point between the campus access layer and the rest of the network. The distribution switches are implemented in pairs and deployed with redundant links to the core and access layers. In large campus networks, there may be several pairs of distribution layer switches. In those cases, each of the security best practices described in this section should be applied to every distribution layer switch pairs.

Figure 5-6 highlights the distribution layer in the overall campus hierarchical design.

Figure 5-6 Campus Distribution Layer



Campus Distribution Layer Design Guidelines

The campus distribution layer provides connectivity to the enterprise core for clients in the campus access layer. It aggregates the links from the access switches and serves as an integration point for campus security services such as IPS and network policy enforcement. This section discusses the various security measures used for securing the campus distribution layer including the following:

- Protecting the endpoints using network-based intrusion prevention
- Protection the infrastructure using NFP best practices

Campus IPS Design

IPS provide filtering of known network worms and viruses, DoS traffic, and directed hacking attacks. This functionality is highly beneficial in a campus environment by quickly identifying attacks and providing forensic information so that attacks can be cleaned up before substantial damage is done to network assets. IPS is designed to monitor and permit all traffic that is not malicious and can be deployed with a single campus-wide protection policy allowing for a pervasive campus-wide IPS deployment.

To get the most benefit, IPS needs to cover a majority of the network segments in a campus. Since the distribution switches provide the aggregation point for all of the access switches and provides connectivity and policy services for traffic flows between the access layer and the rest of the network, it is recommended that IPS devices be deployed in the distribution layer.

- Deploying IPS in a campus network is driven by three key design considerations:
- Deployment Model, page 5-18
- Scalability and Availability, page 5-19
- Traffic Symmetry, page 5-19

Deployment Model

Cisco IPS appliances and modules can be deployed in inline or promiscuous mode, typically referred to as IPS or IDS modes. When deployed in the inline mode, the Cisco IPS is placed in the traffic path. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a strong protective service. IPS inline mode enables automatic threat detection and mitigation capabilities that offer some clear advantages in terms of timely threat mitigation and degree of protection. In addition, signature tuning enables the automated response actions to be tuned according to customer policy. Since IPS is in the data path, however, it is critical to ensure that the deployment is well designed, architected and tuned to ensure that it does not have a negative impact on network latency, convergence, and service availability. Additionally, when deployed in the inline mode, traffic is bridged through the sensors by pairing interfaces or VLANs within the sensor. This requires additional VLANs and modifications to be made to the campus architecture to accommodate the IPS insertion.

Cisco IPS can also be deployed in promiscuous mode. In this mode, the IPS is not in the data path, but rather performs passive monitoring, with traffic being passed to it through a monitoring port using traffic mirroring techniques such as Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), or VLAN ACL (VACL) capture. The Cisco IPS sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. Upon detection of anomalous behavior, management systems are informed of an event and operational staff can subsequently decide what action, if any, to take in response to an incident. The time between threat detection and mitigation may thus be extended and requires a manual response.

The decision to deploy IPS in inline mode or promiscuous mode varies based on the goals and policies of an enterprise. Deploying IPS inline has some clear advantages from a security perspective with its timely threat detection and mitigation, but requires some architecture modifications and careful planning to ensure network latency, convergence, and availability is not compromised. Deploying IPS in promiscuous mode avoids architectural changes, but it provides a lesser degree of security.

Scalability and Availability

For scalability, Cisco offers a range of different IPS platforms that can be deployed according to a particular customer's needs. For networks with a high level of activity and traffic, IPS appliances can be used. For networks with a lower level of activity and traffic or where integrated security is preferred, Cisco IPS modules are viable options.

For increased scalability and high availability, multiple IPS sensors can be bundled together using a load-balancing mechanism. IPS load-balancing can be accomplished using the EtherChannel load-balancing (ECLB) feature within a switch to perform intelligent load-balancing across the IPS devices. In addition, multiple IPS sensors may also be deployed by using a load-balancing module or appliance such as the ACE module.

Traffic Symmetry

For maximum visibility, the IPS sensors must be able to see traffic in both directions. For this reason, it is important to ensure the symmetry of the traffic as it traverses or reaches the IPS sensor.

Symmetrical traffic flows offer a number of important benefits, including enhanced threat detection, reduced vulnerability to IPS evasion techniques, and improved operations through reduced false-positives and false-negatives. Consequently, this is a key design element. For example, if multiple IPS exist in a single flow for availability and scalability purposes, maintaining symmetric flows requires some consideration of the IPS integration design. There are a number of options available to ensure symmetric traffic flows, including:

- Copy traffic across all IPS senders—Use of SPAN, VLAN ACL (VACL) capture, or taps to duplicate traffic across all IPS, ensuring any single IPS sees all flows. This can become a challenge once more than two IPS are involved and results in all IPS being loaded with the active traffic flows.
- Integration of an IPS switch—Topological design to consolidate traffic into a single switch, thereby leveraging the switch to provide predictable and consistent forward and return paths through the same IPS. This is simple design, but introduces a single point-of-failure.
- Routing manipulation—Use of techniques such as path cost metrics or policy-based routing (PBR) to provide predictable and consistent forward and return paths through the same switch and, consequently, the same IPS. This is cost-effective design, but introduces some complexity and requires an agreement from network operations (NetOps).
- Sticky load-balancing—Insertion of a sticky load-balancing device, such as the ACE module, to provide predictable and consistent forward and return paths through the same IPS. This is a flexible design, but introduces additional equipment to deploy and manage.

For more information on Cisco IPS, refer to the following URL: http://www.cisco.com/go/ips

Campus Distribution Layer Infrastructure Security

In addition to deploying IPS within the Campus distribution layer, the distribution layer switches also need to be protected. These switches should be hardened following the best practices described in the Chapter 2, “Network Foundation Protection.” The following bullets summarize the key NFP areas for securing the distribution layer infrastructure devices. All best practices listed below are applicable to the access switches in all three distribution-access design models unless otherwise noted.

- Infrastructure device access—Implement dedicated management interfaces to the OOB management network, limit the accessible ports and restrict the permitted communicators and the permitted methods of access, present legal notification, authenticate and authorize access using AAA, log and account for all access, and protect locally stored sensitive data (such as local passwords) from viewing and copying.

Note For more information on implementing an OOB management network, refer to Chapter 9, "Management."

- Routing infrastructure—Authenticate routing neighbors, implement route filtering, implement EIGRP stub routing, use default passive interfaces, and log neighbor changes.

Note Route filtering and EIGRP stub routing in the distribution layer are only recommended for a multi-tier or VSS design where the routed edge interface is on the distribution switches. In a routed access design, these features are used in the access layer.

- Device resiliency and survivability—Disable unnecessary services, filter and rate-limit control-plane traffic, and implement redundancy.
- Network telemetry—Implement NTP to synchronize time to the same network clock, maintain device global and interface traffic statistics, maintain system status information (memory, CPU, and process), log and collect system status, traffic statistics, and device access information, and enable NetFlow.
- Network policy enforcement
  - Implement management ACLs and iACLs to restrict access to infrastructure and management devices.

Note iACLs are only applicable in the distribution layer of a multi-tier design where the routed edge interface is on the distribution switches. In a routed access design, this is enabled in the access layer.

  - Apply uRPF to block packets with spoofed IP addresses.

Note uRPF is only applicable in the distribution layer of a multi-tier design where the routed edge interface is on the distribution switches. In a routed access design, this is enabled in the access layer.

- Secure switching infrastructure—Restrict broadcast domains, harden spanning tree to prevent against inadvertent loops, and apply VLAN best practices.

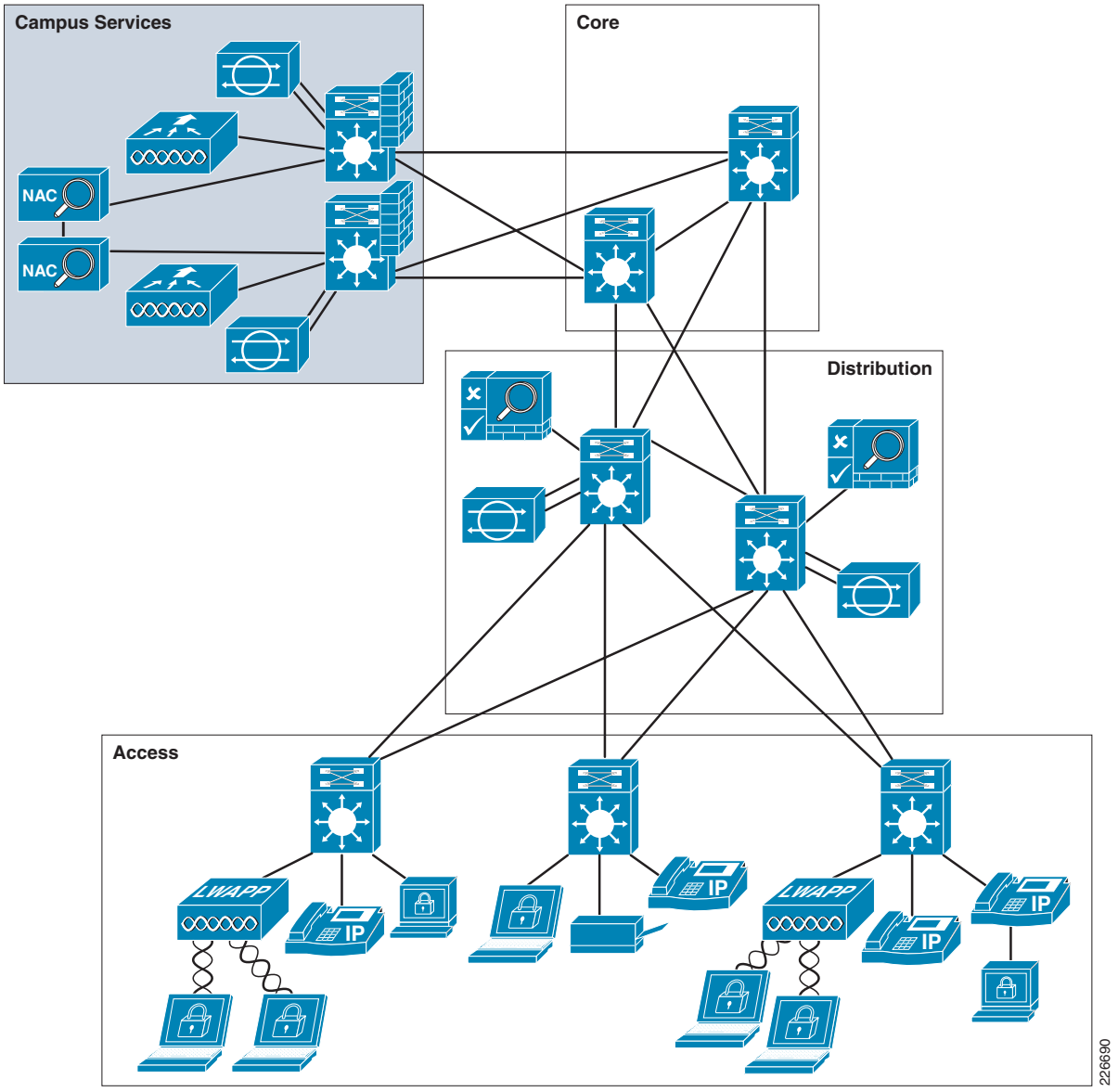
Note VLAN and spanning tree best practices are only applicable in the distribution layer of a multi-tier design where Layer 2 extends to the distribution layer switches.

Campus Services Block

Within the enterprise campus, the primary role of the services block is to provide application services to end users and devices within the campus network such as centralized LWAPP wireless controllers and IPv6 ISATAP tunnel termination. Additionally, for small campuses that only require a few servers, this block could also optionally be used to host a small number of localized foundational servers such as local DHCP, DNS, FTP, NAC Profiler servers. For larger campuses requiring many servers, a data center design should be deployed to host these servers using the security best practices described in the Chapter 4, "Intranet Data Center."

The campus services block connects to the core switches using a pair of services switches using redundant Layer-3 links as shown in Figure 5-7.

Figure 5-7 Campus Services Block Design Diagram



In Figure 5-7, a pair of switches are shown that are acting as a collapsed distribution-access layer providing Layer 2 and Layer 3 services for the devices hosted in the services network segment. These switches also provides for routing separation and policy enforcement for the devices residing in this network.

Given the level of access that employees have to the services located in the campus services block, it is critical that they are protected from internally originated attacks. Simply relying on effective passwords does not provide for a comprehensive attack mitigation strategy. Using host and network-based IPS, private VLANs, switch security, stateful firewalls for access control, and good system administration practices (such as keeping systems up to date with the latest patches), provides a much more comprehensive response to attacks.

The same security best practices to secure servers in the data center should be applied to securing the campus services block. These best practices can be found in Chapter 4, "Intranet Data Center."

Network Access Control in the Campus

In today's diverse workplaces, consultants, contractors, and even guests require access to network resources over the same LAN connections as regular employees. As data networks become increasingly indispensable in day-to-day business operations, the possibility that unauthorized people will gain access to controlled or confidential information also increases.

One of the most vulnerable points of the network is the access edge. The access layer is where end users connect to the network. In the past, corporations have largely relied on physical security to protect this part of the network. Unauthorized users were not allowed to enter a secure building where they could plug into the network. Today, contractors and consultants regularly have access to secure areas. Once inside, there is nothing to prevent a contractor from plugging into a wall jack and gaining access to the corporate network. There is no need to enter an employee cube to do this. Conference rooms frequently offer network access through wall jacks or even desktop switches. Once connected to the network, everyone (employees, contractors, consultants, guests, and malicious users) has access to all the resources on the network.

To protect against unauthorized access to controlled or confidential information, customers are demanding that network access-control be embedded within the network infrastructure. This allows for greater flexibility in expanding the application of network access-control throughout the network.

Campus network designs should provide identity- or role-based access controls for systems connecting to them. Implementing role-based access controls for users and devices help reduce the potential loss of sensitive information by enabling organizations to verify a user or devices' identity, privilege level, and security policy compliance before granting network access. Security compliance could consist of requiring antivirus software, OS updates or patches. Unauthorized, or noncompliant devices can be placed in a quarantine area where remediation can occur prior to gaining access to the network.

Cisco SAFE design uses the following network access control solutions:

- Cisco Identity-Based Network Networking Services (IBNS)
- Cisco NAC Appliance

Cisco IBNS solution is a set of Cisco IOS software services designed to enable secure user and host access to enterprise networks powered by Cisco Catalyst switches and wireless LANs. It provides standards-based network access control at the access layer by using the 802.1X protocol to secure the physical ports where end users connect. 802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the end user or device enabling enterprise policy enforcement of all users and hosts, whether managed or

unmanaged. In addition to holistic access-control provided by 802.1X, IBNS also offers device-specific access-control through MAC-Authentication Bypass (MAB) and user-based access-control through Web-Auth.

The Cisco Network Admission Control (NAC) Appliance uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerability before permitting access to the network. Noncompliant machines are redirected into a quarantine area, where remediation occurs at the discretion of the administrator.

The choice of which NAC solution to use depends on the security goals and the direction of the network design. For networks using or moving towards 802.1x-based wired or wireless access and interested in identity-based access control, Cisco IBNS solution should be considered. For networks requiring role-based access control using posture assessments to ensure security compliance, Cisco NAC Appliance should be considered.

The Cisco Identity-Based Networking Services (IBNS) and NAC Appliance access control solutions are discussed in the following sections.

Cisco Identity-Based Networking Services

Cisco IBNS is an integrated solution comprising several Cisco products that offer authentication and identity-based access control to secure network connectivity and resources. With Cisco IBNS, you can facilitate greater security and enable cost-effective management of changes throughout your network. A secure IBNS framework helps enterprises better manage employee mobility, reduce network access expenses and boost overall productivity while lowering operating costs.

This section of the document provides high-level design recommendations for deploying Cisco IBNS in a campus network along with covering important planning and deployment considerations. For complete details on Cisco IBNS including configuration details, refer to the Cisco IBNS site at the following: www.cisco.com/go/ibns

Deployment Considerations

Cisco IBNS provides customized access to the network based on a person's (or device's) identity. Therefore, a well-defined security policy should be created to provide broad guidelines for who can access which corporate resources and under what conditions. The following sections cover some of the things that should be considered for implementing an IBNS solution that that suits your network.

User and Device Categories

When implementing an IBNS solution, the first and most fundamental question that must be answered is: *Who gets what access?* Once answered, categories of users and devices that connect to your network can be defined. For initial deployments, use broad categories for users and devices (e.g., employee, managed asset, unknown Asset). The simpler the policy, the smoother and more successful your initial deployment will be. Once basic access control has been successfully deployed, more granular groups and policies can be deployed to move towards a more highly differentiated model of access control.

Once categories of users and devices on the network are defined, use the guidelines from your security policy to map each category to a network access level. The example in Table 5-1, while very simple, has been used as the basis for many successful deployments.

Table 5-1 User and device category access levels for initial deployment

Category	Network Access Level
Employee	Full Access (Intranet & Internet)
Managed Asset	Full Access (Intranet & Internet)
Unknown Device	Connectivity services (DHCP, DNS, TFTP) only
Pre-Authentication	Connectivity services only
Failed Authentication	Connectivity services only

- The **Pre-Authentication** category refers to the level of access that a user or device will get before its identity has been determined. Under a very strict security policy, this level could be *no access*. Alternatively, it could be limited to a small set of services (such as DHCP, DNS, TFTP) that would allow devices that depend on immediate network access (e.g. a device that needs to download its operating system or a device that needs enough connectivity to perform a web-authentication) to function normally even before its identity has been established.
- The **Failed Authentication** category refers to the level of access that a user or device will get if it fails to provide valid credentials. Under a very strict security policy, this could be *no access* (this is the default). However, if the policy is *no access*, a manual process must be provided by which legitimate users can remediate their credentials (e.g., renew an expired password). An example of a manual process might be to have employees take their laptops to a physically secure location where an IT administrator can update the credential. Such a process can be resource-intensive, both in terms of end-user education and IT support. Therefore, if your security policy permits, you might want to consider modifying the default **Failed Authentication** access to permit a small set of services that would allow a device to automatically update or request credentials.

User and Device Identification Authentication

Authentication is the process by which the network establishes the identity of devices and users that are attempting to connect. To be able to authenticate users and devices, you must first decide what kind of credentials is acceptable for valid identification. Ideally, strong forms of identification such as digital certificates or properly encrypted usernames and password should be used. A much weaker form of identification would be the MAC address of the connecting device.

Acceptable credentials is determined by the method that is used to validate those credentials. The authentication method determines how a device submits its credentials to the network. 802.1X is an IEEE standard that defines a process by which a device can submit strong credentials like digital certificates and passwords using a client (called a *supplicant*). 802.1X is a strong authentication method and is preferred in all cases where the device can support the required client. The specific details of which credentials are accepted and how they are submitted are determined by what is known as the EAP method. Common EAP methods include PEAP-MSCHAPv2 (for username/password credentials) and EAP-TLS (for certificate-based credentials).

For devices that do not support the required 802.1X client, a supplementary form of authentication must be used. MAC-Authentication Bypass (MAB) is a secondary authentication method in which the access switch detects the device's MAC address and submits it as a form of identification.

Once the type of credential is chosen, it must be validated. A database of allowed devices and their credentials and (for certificate-based authentication) a certificate chain of trust is required for authentication. If MAC address-based authentication is used, then a database of valid MAC addresses to validate against is required as well.

In most cases, there is no need to build a credential database from scratch. For example, many organizations already possess a database of valid users and computers in the form of Microsoft Active Directory. Some organizations also maintain databases with the MAC addresses of corporate assets. Very often, these databases can be re-used for 802.1X and MAB. Using these databases will greatly simplify your 802.1X deployment.

Levels of Authorization

Authorization is the process by which an endpoint is granted a certain level of access to the network. In an identity-enabled network, network access should correspond to the authenticated identity of the endpoint. But an endpoint's network access can also depend on where the endpoint is in the authentication process. When planning a deployment, consider what access the endpoint should have at each of these stages:

- Pre-authentication
- Successful authentication
- Failed authentication

The authorization options available in each stage are discussed in detail below.

Pre-Authentication

By default, endpoints are not authorized for network access prior to authentication. Before a device has successfully authenticated via 802.1X or MAB, the port allows no traffic other than that required for authentication. Access to the port is effectively closed. While very secure, this method of access control can cause problems for devices that need network access before they authenticate (e.g., PXE devices that boot an OS from the network) or devices that are sensitive to delays in network access that may result from the authentication process.

As an alternative, it is possible to configure Cisco switches for two other levels of Pre-Authentication authorization: *Open Access* and S*electively Open Access*.

Open Access is the opposite of the default Pre-Authentication authorization. With Open Access, all traffic is allowed through the port before authentication. While Open Access is obviously not an effective way to enforce network access control, it does have an important role in initial stages of deploying 802.1X. This will be discussed later in the section on the Monitor Mode deployment scenario.

Selectively Open Access represents a middle-ground between the default *Closed* access and Open Access. With Selectively Open Access, you can use a default port access-lists (ACLs) to permit or deny specific traffic (e.g., permit TFTP and DHCP traffic to allow PXE devices to boot before they authenticate).

Table 5-2 summarizes the pre-authentication access levels.

Table 5-2 pre-authentication access levels

Pre-Authentication Access Level	Implementation
No Access	Default —Closed
Open Access	Open
Selectively Open Access	Open with port ACL to control access

Successful Authentication

After a successful authentication, the port is, by default, opened up completely and all traffic is allowed in the configured native VLAN of the port. This is a simple, binary decision: anyone who successfully authenticates by any method is granted full access. To achieve differentiated access based on the identity of the authenticated user or device, it is necessary to use dynamic access control with VLANs and/or ACLs.

When post-authentication access is implemented with VLANs, the switch dynamically assigns a VLAN to a port based on the identity of the device that authenticated. Engineers could be assigned the ENG VLAN while accountants could be assigned the FINANCE VLAN. While this form of dynamic authorization is a powerful tool for differentiating access for different user groups, it comes at a cost. Supporting multiple VLANs on every switch may require changes to the network architecture and addressing scheme. In addition, VLANs isolate traffic at Layer 2 in the OSI stack so dynamic VLAN assignment by itself cannot restrict access to specific subnets (at Layer 3) or applications (Layer 4 and above). However, dynamic VLAN assignment does provide the foundation for virtualizing IT resources using network virtualization solutions.

When successful authentication authorization is implemented with ACLs, the switch dynamically assigns an ACL to a port based on the identity of the device that authenticated. Engineers could be assigned an ACL that permits access to engineering subnets and applications while accountants get a different ACL. While ACLs do not achieve the same level of logical isolation that VLANs provide, dynamic ACLs can be deployed without changing the existing network architecture and addressing schemes. On the other hand, care must be taken to ensure that the dynamic ACLs do not overwhelm the TCAM capacity of the access switch. Well-summarized networks and good network design are essential to the creation of short but effective ACLs.

When deciding between dynamic VLANs and dynamic ACLs, another factor to consider is the form of Pre-Authentication authorization that you have chosen to implement. Dynamic ACLs work well with any kind of Pre-Authentication authorization. Dynamic VLAN assignment, on the other hand, does not typically work well with Open or Selectively Open Pre-Authentication authorization. When Pre-Authentication authorization is Open, devices can receive IP addresses on the switchport VLAN subnet at link up. If a different VLAN is assigned as the result of an authentication, the old address will not be valid on the new VLAN. 802.1X-capable devices with modern supplicants can typically detect the VLAN change and request a new address on the new VLAN but clientless devices (such as printer) will not be able to.

The different kinds of authorization available after successful authentication and the deployment considerations for each method are summarized in Table 5-3.

Table 5-3 Successful Authentication

Post-Authentication Authorization Method	Impact to Network Architecture	TCAM impact	Compatible Pre-Authentication Methods	Notes
Default “Open”	Minimal	None	Closed	May be sufficient for simple deployments or as a first step for more complex deployments.

Table 5-3 Successful Authentication (continued)

Dynamic VLAN	Significant	None	Closed	Required for network virtualization. Provides logical isolation of traffic at L2.
Dynamic ACL	Minimal	Significant	All	Does not support network virtualization. Provides access control at Layer 3 and Layer 4.

Failed Authentication

After a failed authentication, the port is, by default, left in the same state as it was before authentication was attempted. If the port was in the default Closed state before authentication, it will remain closed after a failed authentication. If the port was in a Selectively Open state before authentication, it will remain that way: open in the statically configured VLAN and subject to the default port ACL.

Since failed authentications revert to the pre-authentication authorization, it is necessary to decide whether the chosen pre-authentication network access is adequate for endpoints that fail authentication. If not, it may be necessary to modify your pre-authentication network authorization policy or to utilize some of the mechanisms available for modifying the default Failed Authentication network access levels.

User and Device Physical Connectivity

Hosts connect to the access layer switches in several ways. The simplest connection is a direct point-to-point connection of one host to one switch port. In IBNS deployments, this is sometimes referred to as "single host mode." Single host mode is the most secure form of connection and the default mode on Cisco switches enabled for 802.1X and MAB. A switch running 802.1X in single host mode will only allow one device at a time on that port. If another device appears on the port, the switch shuts down the port as a security precaution. Because only one device is allowed to connect to the port, there is no possibility of another device snooping the traffic from the authenticated device. A port in single-host mode effectively prevents casual port-piggybacking.

Although it is the most secure mode, single host mode is not always sufficient. One common exception to the point-to-point connection assumption is IP Telephony. In IP Telephony deployments, two devices are often connected to the same switch port: the phone itself and a PC behind the phone. In this case, a new host mode, "multi-domain," is required. With multi-domain host mode, the switch allows two devices to authenticate and gain access to the network: one voice device in the voice VLAN and one data device in the data VLAN.

Some deployments include devices that include multiple virtual machines even though there is physically only one connected device. Cisco switches support a third host mode, "multi-auth," that allows each virtual machine to access the port after being authenticated. The multi-auth host mode is a superset of multi-domain host mode, meaning that the multi-auth host mode allows one voice device in the voice VLAN and any number of data devices in the data VLAN.

The most appropriate host mode to configure on the switch is determined by how hosts are connecting to the network. 802.1X is most effective when it is most restrictive. If IP Telephony is not deployed, don't configure multi-domain host mode. If there are no virtual machines with unique MAC addresses on the same physical host, do not configure multi-auth host mode. If possible, use the same host-mode throughout your network. Using a standardized configuration will minimize operational costs.

Table 5-4 summarizes the available host modes.

Table 5-4 Host Modes

With this Endpoint…	…Use this Host Mode
Point-to-point only (PC, printer, etc)	Single-host
IP Telephony	Multi-domain
Virtual Machines (with or without IP Telephony)	Multi-auth

Deployment Best Practices

Once it has been determined how users and devices will be authenticated, what network access they will be granted before and after authentication, and how devices will be allowed to connect to the network, the next step is to deploy the solution. The SAFE design leverages a phased deployment strategy. The next couple of sections will look at three generic deployment scenarios that can be rolled out as a three-phase deployment (or two-phase, depending on your ultimate design goals). IBNS deployments are most successful when implemented in phases, gradually adding in network access restrictions to minimize impact to end users.

The three scenarios discussed below are as follows:

- Monitor Mode, page 5-28
- Low Impact Mode, page 5-30
- High Security Mode, page 5-31

Monitor Mode

Monitor mode is the first phase of a three-phase (or two-phase) IBNS deployment. In this phase, access is not physically prevented, but visibility into who is connecting is obtained. Having this visibility provides invaluable insight into who is getting access, who has an operational 802.1X client, who is already known to existing identity stores, who has credentials, etc. As a side benefit, some intruders may be deterred by the simple knowledge that someone is watching. In addition, it prepares the network for the access-control phases as described in the next couple of sections.

When deploying IBNS in Monitor Mode, authentication (802.1X and MAB) is enabled without enforcing any kind of authorization. There is no impact to users or endpoints of any kind: they continue to get exactly the same kind of network access that they did before you deployed IBNS. The authorization level Pre-Authentication is the same as after Successful Authentications and Failed Authentications access: completely open. In the background, however, the network is querying each endpoint as it connects and validates its credentials. By examining the authentication and accounting records (at the ACS server), it is possible to determine the information in Table 5-5.

Table 5-5 Authentication and Accounting Records

Endpoints on the Network	How Determined
All endpoints/users with 802.1X clients and valid credentials	Passed 802.1X Authentication Records
All endpoints/users with 802.1X clients and invalid credentials	Failed 802.1X Authentication Records
All endpoints without 802.1X clients and known MAC addresses	Passed MAB Authentication Records
All endpoints without 802.1X clients and known MAC addresses	Failed MAB Authentication Records
Ports with multiple connected devices	Multiple Authentications Records for the same port on same switch.

Combining the information in authentication and accounting records results in very detailed knowledge of each endpoint that connects to the network including: username, IP address, MAC address, port and switch where connected, time of connection, etc.

After implementing the Monitor Mode phase, the network will immediately begin authenticating users and devices and you will have visibility into who and what is connecting to the network. This visibility information includes which endpoints (PC, printer, camera, etc.) are connecting to your network; where they connected; whether they are 802.1X capable or not; and whether they have valid credentials. Additionally, you will know if the endpoints are known valid MAC addresses via the failed MAB attempts.

The primary benefit of Monitor Mode is that it enables IT administrators to proactively address any issues that would impact end users once access control is enabled.

These issues are summarized in Table 5-6.

Table 5-6 Monitor Mode Values

To Do	Key Issue	Remediation
Analyze 802.1X failures.	Are these valid devices or users that should be allowed access but are failing 802.1X?	Update credentials for valid devices and users so they will pass 802.1X.
Analyze MAB success.	Are there any devices doing MAB that should be capable of 802.1X?	Update those devices with supplicants and credentials so they can authenticate using 802.1X
Analyze MAB failures	Are there managed assets that should be allowed access to the network but are failing MAB?	Update your asset database with these MAC addresses.
Analyze ports that have multiple devices on them.	Are these rogue hubs or valid virtual machines?	Remove rogue devices. Note ports that may legitimately require support for multiple hosts per port.

Once all the issues uncovered by deploying IBNS in Monitor Mode are addressed, the next step is to deploy identity-based access control. The next two scenarios describe common ways to deploy access control. Many customers will choose to implement Low Impact Mode only. Others may start with Low Impact Mode to help assess the impact of access control to end users and then later move on to High Security Mode. Other customers may move straight from Monitor Mode to High Security Mode.

Low Impact Mode

Low Impact Mode provides an incremental increase in the level of port-based access control without impacting the existing network infrastructure. Low Impact Mode does not require the addition of any new VLANs nor does it impact your existing network addressing scheme. With Low Impact Mode, as little or as much access control can be enforced.

Low Impact Mode builds on top of Monitor Mode. In Monitor Mode, the Pre-Authentication authorization level was completely open. In Low Impact Mode, the Pre-Authentication level is selectively open. The difference is that Low Impact Mode adds an ingress port ACL that specifies exactly what traffic will be allowed before authentication. This ACL can be as restrictive or permissive as the corporate network security policy requires.

In Low Impact Mode, a successful authentication causes the switch to download a dynamic ACL (dACL) that is applied on top of the ingress port ACL. The contents of the dACL will be determined by the identity of the user or device that authenticated. In a simple deployment, an employee or managed asset that authenticates successfully could receive a **permit ip any any** dACL that fully opens up the port. More complex deployments could assign different ACLs based on different classes of employee. For example, engineers might be assigned a dACL that permits all engineering related subnets, whereas accountants could be assigned a different dACL that denies access to engineering subnets but permitted all other access.

With the dACL implementation, the switch will substitute the source address of each access-list element with the source address of the authenticated host, ensuring that only that host is allowed by the dACL. Devices that fail authentication (via 802.1X or MAB) will continue to have their access limited by the ingress port ACL defined by the Pre Authentication or Fail Authentication access policies.

Because Low Impact Mode can be deployed with little or no change to the existing campus network design, it is attractive to deploy access control without altering the existing VLAN infrastructure or IP addressing scheme as will be described in the following High Security Mode section. Additional VLANs requires additional IT overhead and in some cases customers may not control the VLAN infrastructure at all (e.g., at a branch office where the Service Provider owns the routers and has implemented MPLS). In the latter case, ACL-based enforcement is the only choice for port-based access control. When ACL-based access enforcement is deployed, the following items need to be considered:

- The current implementation of dACLs requires a pre-configured static port ACL on every access port that may download an ACL. If the switch attempts to apply a dACL to a port without a pre-existing port ACL, the authorization will fail and users will not be able to gain access (even if they present valid credentials and pass authentication).
- The static port ACL is a port-based ACL, it applies to both the data VLAN and, if present, the voice VLAN. The switch performs source address substitution on the dACL, traffic from the phone will not be permitted by a dACL downloaded by a data device authenticating behind the phone. This means that both the phone and any devices behind the phone must authenticate individually and download their own dACL and the host mode on the port must be multi-domain.
- Cisco switches use Ternary Content Addressable Memory (TCAM) to support wire-rate ACL enforcement. TCAM is a limited resource which varies by platform. If the TCAM is exhausted, switching performance can be degraded. It is important to verify that the access switches have sufficient TCAM to support the number and length of ACLs (static and dynamic) that IBNS deployment will require.

- Dynamic (or "downloadable") ACLs extend the standard RADIUS protocol in order to optimize the downloading process and support ACLs of arbitrary size. Use the Cisco ACS server as the AAA server to support downloadable ACLs.
- Because the switch performs source substitution on the source address of the dynamic ACL, the switch does not enforce the dACL until it learns the source address of the authenticated host. IP address learning is enabled by the IP Device Tracking feature on the switch.
- When designing ingress port ACLs, this ACL will restrict access before authentication and after failed authentications. The ingress port ACL must be designed with this in mind. For example, if you want employees that fail 802.1X because of an expired certificate to be able to download a new certificate, you should consider allowing access to the CA server in the ingress ACL. Or, if you want a contractor that fails 802.1X or MAB to be able to access the Internet or VPN to a home network, you should also allow that traffic in the ingress port ACL.

In many cases, Low Impact Mode will be the final step in the IBNS deployment. If this mode sufficiently provides the needed access control, then the only "next step" will be monitoring the network and fine-tuning ACLs as required by the corporate security policy. However, if the network security requirements evolve and pre-authentication access no longer meets the security requirements, IBNS deployment can move to the next phase: High Security Mode.

Additionally, if Low Impact mode does not meet the network and design security requirements in the first place, the Low Impact Mode can be skipped altogether and the deployment can move straight to the High Security Mode phase from the Monitoring Mode phase.

High Security Mode

High Security Mode returns to a more traditional deployment model of 802.1X. In a properly prepared network, High Security Mode provides total control over network access at Layer 2.

In High Security Mode, the port is kept completely closed until a successful authentication takes place. There is no concept of Pre-Authentication access. For users and devices that successfully complete 802.1X, this is not typically an issue since 802.1X authentication is usually very quick assuming a single sign-on (SSO) deployment where credentials are automatically gleaned from the device or user. In environments that require manual log-on (e.g., with a pop-up window to enter username and password), there may be some delay.

For devices that cannot perform 802.1X, however, there may be a significant delay in network access. Since the switch always attempts the strongest secure authentication method first, non-802.1X-capable devices must wait until the switch times out the 802.1X authentication and falls back to MAB as a secondary authentication method. To avoid the delays associated with MAB in High Security Mode, configure the switch to perform MAB first, before 802.1X. This enable non-802.1X devices to get immediate access after successful MAB.

After a successful authentication, network access will, by default, change from completely closed to completely open. To add more granular access control, High Security Mode uses dynamic VLAN assignment to isolate different classes of users into different broadcast domains. Devices that can't authenticate or fail to authenticate retain the same level of access that they had before authentication. In the case of the High Security Mode, devices will have no access at all.

By isolating traffic from different classes of users into separate VLANs, High Security Mode provides the foundation for virtualized network services.

For more information on network virtualization solutions, refer to the following URL:
http://www.cisco.com/en/US/netsol/ns658/networking_solutions_package.html

Deploying High Security Mode with VLAN assignment can have an impact on the network architecture. The following considerations should be noted when deploying IBNS in the High Security Mode Scenario:

- Dynamic VLAN assignment requires that every dynamic VLAN be supported on every access switch to which a user might connect and authenticate. This requirement has several repercussions: If you have three user groups to which you wish to assign unique VLANs - Engineering, Finance, HR - then every access switch must have those three VLANs defined by name (the number of the VLAN does not have to be the same). If the switch attempts to apply a non-existent VLAN to a port, the authorization will fail and users will not be able to gain access (even if they presented valid credentials and passed authentication).
- Supporting multiple VLANs per access switch is non-trivial from an IP addressing perspective. Good campus design principles dictate a single subnet per VLAN with no VLAN spanning more than one switch. The IP addressing scheme should support multiple subnets per switch in such a way that that does not over-burden the control and data planes of the campus distribution block. The fewer the VLANs, the more manageable and scalable the solution will be.
- If you choose to change the order of authentication to perform MAB before 802.1X, be aware that this will mean that every device (even those capable of 802.1X) will be subject to MAB. This could increase the amount of control plane traffic in the network. If there are devices in the network that might pass both 802.1X and MAB, be sure to either 1) ensure that no 802.1X-capable devices are in the MAB database; or 2) configure the switch to prioritize 802.1X over MAB so that the port will process an 802.1X authentication after a successful MAB authentication.
- If some level of access is needed for devices that fail 802.1X (for example, to allow employees with expired certificates to download a new certificate), it is possible to configure the solution to grant limited access based on the type of authentication method that failed. If 802.1X fails, the switch can be configured to open the port into a special VLAN -- the Auth-Fail VLAN -- for this purpose. The switch can also be configured to "fail back" to a MAB authentication if 802.1X fails. However, 802.1X with failover to MAB should typically not be deployed if the authentication order has been changed to do MAB first.
- There may be devices on the network that cannot perform 802.1X and cannot pass MAB (for example, contractors with no supplicants that need to VPN to their home network). For unknown MAC addresses that fail MAB, it is possible to configure the Cisco ACS server with an unknown MAC address policy. Such a policy allows ACS to instruct the switch to allow devices with unknown MACs into a dynamically assigned VLAN. In essence, an unknown MAC policy enables a dynamic version of the Auth-Fail VLAN for failed MAB attempts.

Deployment Scenarios Summary

Table 5-7 provides a quick summary of the three deployment scenarios discussed in the previous sections:

Table 5-7 Deployment Scenario Summary Table

Deployment Scenario	Best for…	Auth Types	Host Mode	Pre-Auth	Successful Auth	Failed Auth
Monitor Mode	All Customers (Initial Deployment)	802.1X & MAB	multi-auth	Open	Open	Open
Low Impact Mode	Customers seeking simple access control with minimal impact to end users and network infrastructure	802.1X & MAB	single-auth (non-IPT) multi-domain (IPT)	Selectively Open	Dynamic ACL	Selectively Open
High Security Mode	Customers seeking the security of traditional 802.1X with L2 traffic isolation and/or network virtualization	802.1X & MAB	single-auth (non-IPT) multi-domain (IPT)	Closed	Dynamic VLAN	Closed (or Auth-Fail VLAN)

Deploying IBNS in a Monitor Mode and adding in access control in a phased transition, 802.1X can be deployed with minimal impact to the end users. For more information on Cisco IBNS including configuration specifics on deploying the different deployment scenarios outlined in this section, please see the deployment guide at www.cisco.com/go/ibns.

NAC Appliance

Cisco NAC Appliance is a network access control solution that integrates with the network infrastructure to enforce security policy compliance at the network level. Access is controlled based on device compliance status, device behavior, and user credentials. It identifies whether networked devices such as laptops, IP phones, or printers seeking access to the network are compliant with your network's security policies and noncompliant devices or redirected to a quarantine area for remediation.

Cisco NAC provides a scalable access control solution using a central policy decision component and a distributed security enforcement component at the network level. The Cisco NAC solution consists of the following components:

- Cisco NAC Manager—Provides a web-based interface for creating security policies and managing online users. It can also act as an authentication proxy for authentication servers on the backend such as an ACS. Administrators can use Cisco NAC Manager to establish user roles, compliance checks, and remediation requirements. Cisco NAC Manager communicates with and manages the Cisco NAC Server, which is the enforcement component of the Cisco NAC.

- Cisco NAC Server—Performs device compliance checks as users attempt to access the network. This security enforcement device is deployed at the network level. Cisco NAC Server can be implemented in band or out of band, in Layer 2 or Layer 3, and as a virtual gateway or as a real IP gateway. It can be deployed locally or centrally.
- Cisco NAC Agent—This lightweight, read-only agent runs on an endpoint device. It performs deep inspection of a local device's security profile by analyzing registry settings, services, and files on the endpoint. Through this inspection, it can determine whether a device has a required hotfix, runs the correct antivirus software version, or runs other security software, such as Cisco Security Agent. Cisco NAC Agent is available as both a persistent agent and as a Web-based, dissolvable agent that is installed and removed on the client at the time of authentication.
- Cisco NAC Profiler—Provides device profiling by keeping a real-time, contextual inventory of all devices in a network, including non-authenticating devices such as IP phones, printers, and scanners. It facilitates the deployment and management of the Cisco NAC Appliance by discovering, tracking, and monitoring the location, types, and behavior of all LAN-attached endpoints. It can also use the information about the device to apply appropriate Cisco NAC policies.
- Cisco NAC Guest Server—The optional Cisco NAC Guest Server simplifies the provisioning, notification, management, and reporting of guest users on wired and wireless networks, offloading from IT staff much of the challenges commonly associated with supporting corporate visitors. The Secure Guest service enhances IT's ability to protect its own organization's assets, employees, and information from guests and their devices while providing secure and flexible network access to meet visitors' business needs.

Note The Cisco NAC Guest Server was listed for completeness. However, it was not included in this phase of the SAFE project and will not be covered in this design guide. It will be covered in a later phase of the project. For more information on the NAC Guest Server, refer to www.cisco.com/go/nac.

Deployment Considerations

Cisco NAC Appliance provides access control to the network based on their role in the network and security policy compliance. Security policies can include specific antivirus or anti-spyware software, OS updates, or patches. When deploying the NAC Appliance solution in a campus network, consider the following:

- In-Band (IB) and Out-of-Band (OOB) Mode, page 5-34
- High Availability, page 5-36

This section covers the above deployment considerations. The NAC profiler deployment integration is covered in the "NAC Profiler" section on page 5-45.

In-Band (IB) and Out-of-Band (OOB) Mode

The NAC server is the enforcement server and acts as a gateway between the untrusted (managed) network and the trusted network. The NAC server enforces the policies that have been defined in the NAC Manager web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and client system requirements. The NAC Server can be deployed in IB or OOB mode. In IB mode, the NAC server is always inline with the user traffic (before and after posture assessment). In OOB mode, the NAC server is only inline during the process of authentication, posture assessment, and remediation. Once a user's device has successfully logged on, its traffic traverses the switch port directly without having to go through the NAC Server.

The NAC server can also operate in one of the following IB or OOB modes:

- IB virtual gateway (Layer-2 transparent bridge mode)—Operates as a bridge between the untrusted network and an existing gateway, while providing posture assessment, filtering and other services inline.
- IB Real-IP gateway (Layer-3 routing mode)—Operates as the default gateway for the untrusted network.
- OOB virtual gateway (Layer-2 transparent bridge mode)—Operates as a virtual gateway during authentication and certification, before the user is switched out-of-band to the access network.
- OOB Real-IP gateway (Layer-3 routing mode)—Operates as a Real-IP Gateway during authentication and certification, before the user is switched out-of-band and connected directly to the access network.

In virtual gateway deployments, the NAC server operates as a standard Ethernet bridge. This configuration is typically used when the untrusted network already has a gateway and you do not wish to alter the existing configuration. In the Real-IP gateway configuration, the NAC server operates as the default gateway for untrusted network (managed) clients. The NAC server can be one hop or multiple hops away.

Consider the following when deciding whether to deploy an IB or OOB NAC solution:

In-band (IB)

- Typically deployed for segments that need continuous user management in the form of source/destination/protocol bandwidth controls.
- Required for wireless.
- Deployed where one switch port supports multiple end stations.
- Deployed where the network infrastructure is partially or fully non-Cisco.
- Time to production is generally much quicker.
- Deployed in 'Real-IP' mode when users are multiple hops away from the NAC Server.
- Direct traffic to the untrusted interface using 802.1q or policy-based routing for users or VLANs that need to become certified.
- Remote locations can have their own NAC Server or become certified when user comes to main site to access shared resources.

Out-of-Band (OOB)

- Deployed in networks where high network throughput is required (e.g., large campuses).
- Ensure switch types and IOS/Cat OS types meet the latest compatibility list.
- Allow for greater time for deployment and preparation.
- SNMP and the use of MAC or link up/down traps becomes the mechanism for OOB. Ensure that all community strings match as well as traps arrive at the NAC Manager without interference from an ACL/firewall.
- If deploying into a network with VoIP, MAC notification is required on the access switch if PCs will be plugged into the back of the phone. MAC notification is preferable to link-state notification as a means of trap reporting because it is quicker.
- Microsoft operating systems below Windows 2000 have a more delayed response to VLAN/DHCP changes.
- OOB is only supported when the access layer switch is a supported Cisco switch.

Real IP (Layer-3) OOB NAC deployments are the recommended option for routed access campus designs. The following sections will focus on the deployment best practices for integrating the Real IP OOB NAC solution within the campus design.

High Availability

It is recommended that the NAC solution be deployed using a high availability design to ensure the availability of the network access control security. In a high availability design, each of the NAC components are deployed in pairs using active/standby stateful failover configurations.

When the NAC Manager and NAC server pairs are configured in an active/standby failover configuration, the active unit does all the work and the standby unit monitors the active unit and keeps its database synchronized via direct failover connection between the servers. A virtual IP address is configured and always resides on the active server. Both units exchange UDP heartbeat packets every 2 seconds and if the heartbeat timer expires, stateful failover occurs. The virtual IP (service IP) address should be used for the SSL certificate. Ethernet 2 on the active and standby units should be used for the failover link connection used to share heartbeat packets and database synchronization information. In the case of the NAC server pairs, most of the NAC server configuration is stored on the NAC Manager and when the NAC server failover occurs the NAC Manager pushes the configuration to the standby NAC server when it becomes active.

In addition to the heartbeat, the NAC server can also failover due to Eth0 or Eth1 link failure. This is accomplished by configuring two IP addresses external to the NAC server, one on the trusted network and the other on the untrusted network. The active and standby NAC server will send ICMP ping packets via Eth0 to the IP address on the trusted network and ICMP ping packets via Eth1 to the IP address on the untrusted network. The status of these pings packets is communicated between the NAC servers via the heartbeat signal. If the active and standby NAC servers can ping both external IPs, no failover occurs. If the active and standby NAC server cannot ping either of the external IPs, no failover occurs. If active NAC server cannot ping either of the external IPs, but standby NAC server can ping it, failover occurs.

Deployment Best Practices

When deploying the NAC Appliance solution into a campus network, consider the following to ensure pervasive coverage seamless integration with the campus architecture:

- NAC Server and Manager Placement, page 5-36
- Access Switch VLAN Requirements, page 5-39
- Client Redirection to the NAC Server, page 5-39
- NAC Agent Considerations, page 5-40
- Client Authentication , page 5-41

This section of the document will provide deployment best practice recommendations for integrating a Layer-3 OOB NAC deployment into a routed access campus design. For information on integrating an IB NAC deployment or integration of NAC into a multi-tier access design, refer to the following URL: www.cisco.com/go/nac

NAC Server and Manager Placement

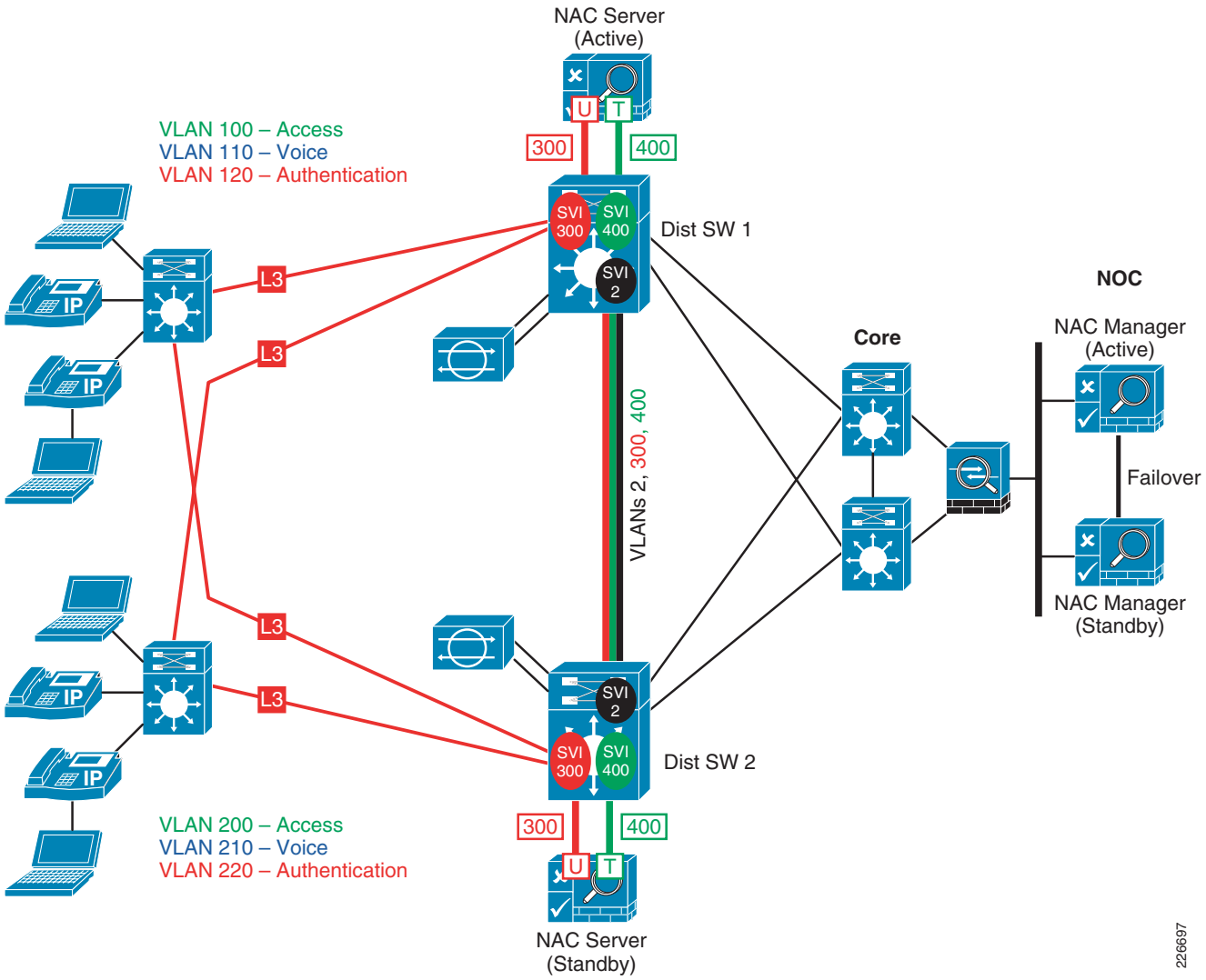
Placement of the NAC components within the campus design is important to provide pervasive coverage and ensure that the individual components can communicate with each other as needed. This section outlines the recommended placement of the NAC components in an Layer-3 routed access campus design.

Some of the communication requirements between the NAC components are as follows:

- The users and devices that need to be certified needs to communicate with the NAC Server for authentication and posture assessment.
- The NAC Manager needs to communicate with the NAC servers in order to manage the security policies, online users, and provide proxy authentication to external authentication servers.
- The NAC Manager must communicate with the access switches that the clients are connecting to in order to enforce proper network policy.
- The collectors running on the NAC servers must be able to communicate with the NAC profiler in order to send endpoint profile information that it has gathered.
- The NAC collectors need to communicate with the access switches to obtain endpoint profile and mapping information.
- The NAC profiler must communicate with the NAC Manager create NAC policies based on endpoint profile data.
- The NAC Manager needs to communicate with external authentication servers if using external authentication servers to authenticate the users.

Placement of the NAC solution components into an Layer-3 routed campus access design is shown in Figure 5-8.

Figure 5-8 Campus NAC Server and Manager Integration



The NAC Manager is placed in the NOC management segment. The NOC management segment needs to provide the connectivity the NAC Manager needs to communicate with the access switches via SNMP. It is recommended that this communication occur over the out-of-band management access that the NOC segment has to the switches outside of the data path traffic.

The NAC Manager also needs to communicate with the NAC server's trusted interface. The NAC server does not have an OOB management interface so the communication occurs over the data path. If a firewall is used between the NAC Servers and NAC Managers, the appropriate access rules must be permitted to allow proper communication. If NAT is used on the firewall to hide the NOC management addresses from the data path, a static NAT translation must exist for the NAC Managers IP address.

The trusted and untrusted interfaces on the NAC server connects to the distribution switches. The trusted and untrusted interfaces need to be in separate VLANs (VLAN 300 and 400 in Figure 5-8 above). The active and standby NAC servers are connected to different switches for redundancy. The users that want to connect to the network need to access the untrusted interface on the NAC server for authentication and posture assessment. The distribution switches aggregate all the connections from the access switches making it easy to redirect all the unauthenticated users to the NAC server.

The trusted VLAN (VLAN 400) and the untrusted VLAN (VLAN 300) are trunked across the distribution switches along with the VLAN for Layer-3 route peering (VLAN 2). HSRP is used between the trusted SVI (400) and the untrusted SVI (300) for resiliency.

Access Switch VLAN Requirements

The access switches should be configured with at least three VLANs as follows:

- Authentication VLAN (120, 220)—Users are placed in this VLAN prior to NAC certification
- Access VLAN (100, 200)—Users are placed in this VLAN after NAC certification
- Voice VLAN (110, 210)—VLAN for IP phones

The default VLAN configuration for all NAC managed ports should be the authentication VLAN. The NAC Manager will place the interface into the authentication VLAN once a user connects; however, if there is a communication failure between the NAC Manager and the access switch, preconfiguring all the managed interfaces in the authentication VLAN prevents a user from accessing the network if there is a NAC failure. If a user is connected behind an IP phone and there is a data VLAN and voice VLAN configured on the interface, the NAC Manager only changes the data VLAN and not the voice VLAN.

Client Redirection to the NAC Server

When a user connects to the access switch that has not been certified by the NAC server, the user will be placed in the authentication VLAN. The user should not have access to any part of the network from the authentication VLAN except for the NAC server and the remediation servers in the quarantine segment. Access lists are applied on the authentication SVI to enforce this. The access-lists should only allow the following:

- UDP port 8906 to the virtual IP of the NAC Server—Used by the NAC agent to communicate with the server
- TCP port 80 (http)—If NAC agent is not used, NAC authentication is done via web interface
- TCP port 443 (https)—If NAC agent is not used, NAC authentication is done via web interface (HTTP is redirected to use HTTPS)
- UDP port 67 (bootps)—Needed for DHCP IP requests
- UDP 53 (domain) —Needed for DNS resolution
- Traffic to the remediation servers on the quarantine segment— Depending on how antivirus updates or OS patches are distributed, you will need to permit this traffic

In addition to configuring access lists on the authentication SVI, you will need to configure policy-based routing to redirect all web traffic (TCP port 80 and 443) to the NAC server. Using policy-based routing to redirect all web-based traffic to the NAC server will allow a user to open a browser to any website and get automatically redirected to the NAC server for authentication. The user will not need to know or manually type the IP address or host name of the NAC server in their browser. The policy-based routing policy will need to be applied to all Layer-3 interfaces peering the with the access switches to ensure all traffic will be redirected to the NAC server regardless of what path is taken.

If the NAC Agent is used, the discovery host configured on the client should point to the untrusted interface of the NAC server. This should be configured on the NAC Agent kit prior to distributing to the clients.

Once the client is certified by the NAC server, the client is placed in the access VLAN to gain access to the network and traffic will bypass the NAC server. Network access enforcement now occurs on the access switches. In NAC Layer-3 OOB deployments, the NAC server only facilitates authentication and posture assessment.

Note If using the NAC Agent, you will need to add an ACL entry to block UDP port 8906 on the access VLAN SVI. Otherwise, the NAC Agent login screen will continue to appear even after the user is certified by NAC.

NAC Agent Considerations

Users who need to be certified by NAC can access the NAC server using the NAC Agent or using web login. Posture assessments can only be done when the NAC Agent is used. When the NAC Agent is not used, only authentication can be done.

The NAC Agent is a lightweight, read-only agent that runs on an endpoint device. The Cisco NAC Agent is available as both a persistent agent and as a web-based, dissolvable agent that is installed and removed on the client at the time of authentication.

Persistent NAC Agent

The persistent NAC Agent provides local-machine, agent-based vulnerability assessment and remediation for client machines. Users download and install the NAC Agent (read-only client software), which can check the host registry, processes, applications, and services. The NAC Agent can be used to perform Windows updates or antivirus/anti-spyware definition updates, launch qualified remediation programs, distribute files uploaded to the NAC Manager, and distribute website links to remediation websites in order for users to download files to fix their systems, or simply distribute information/instructions.

The following steps outline the login process using the persistent NAC Agent:

Step 1 Users login using the NAC Agent.

Step 2 The agent gets the requirements configured for the user role/operating system from the NAC Server.

Step 3 The agent checks for the required packages.

Step 4 The agent sends a report back to the NAC Manager (via the NAC Server).

If requirements are met on the client, the user is allowed network access. If requirements are not met, the agent presents a dialog to the user for each unmet requirement. The dialog (configured in the New Requirement form) provides the user with instructions and the action to take for the client machine to meet the requirement.

NAC Web Agent

The Cisco NAC Web Agent provides temporal vulnerability assessment for client machines. Users launch the Cisco NAC Web Agent executable, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet. When the user terminates the Web Agent session, the Web Agent logs the user off of the network and their user ID disappears from the online users list.

The following steps outline the login process using the NAC Web Agent:

Step 1 Users login using the NAC Web Agent.

Step 2 Web Agent gets the requirements configured for the user role/OS from the NAC Server.

Step 3 Web Agent checks the host registry, processes, applications, and services for required packages.

Step 4 Web Agent sends a report back to the NAC Manager (via the NAC Server).

If requirements are met on the client, the user is allowed network access. If requirements are not met, the Web Agent presents a dialog to the user for each unmet requirement. The dialog (configured in the New Requirement form) provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept *restricted* network access (if you have enabled that option) while they try to remediate the client machine so that it meets requirements for the user login role. You can set up a restricted user role to provide access to only limited applications/network resources in the same way you configure a standard user login role.

It is recommended that NAC be deployed using the NAC Agent on employee endpoints. Vulnerability assessments and automated remediation can only be done using the NAC Agent. Additionally, once the user is certified, they need to obtain a new IP address in the access VLAN. The NAC Agent can refresh the IP address on the user's machine without requiring the switch port to be bounced. Without the NAC Agent, the NAC Manager needs to bounce the switch port to force DHCP refresh or the user will have to manually force a DHCP refresh. Users connected behind IP phones should always use the NAC Agent since bouncing the port will cause the IP phone to reboot.

Client Authentication

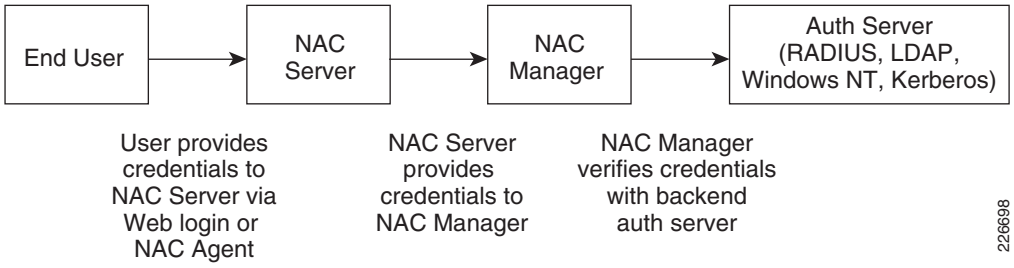
Part of the NAC certification process requires clients to authenticate prior to being granted network access. Authentication can be accomplished using a local username and password database configured on the NAC Manager or using external authentication servers. By connecting the Clean Access Manager to external authentication sources, you can use existing user data to authenticate users in the untrusted network.

When working with existing backend authentication servers, Cisco supports the following authentication protocol types:

- Kerberos
- Remote Authentication Dial-In User Service (RADIUS)
- Windows NT (NTLM Auth Server)
- Lightweight Directory Access Protocol (LDAP)

When using external authentication servers, the NAC Manager is the authentication client that communicates with the backend auth server. Figure 5-9 illustrates the authentication flow.

Figure 5-9 NAC Authentication Flow Using External Auth Servers



It is recommended that external authentication servers are used for NAC appliance deployments. It greatly simplifies management of user credentials by providing a central location for maintaining username and passwords. The choice of which option is used is dependant on a customer's environment and existing authentication techniques.

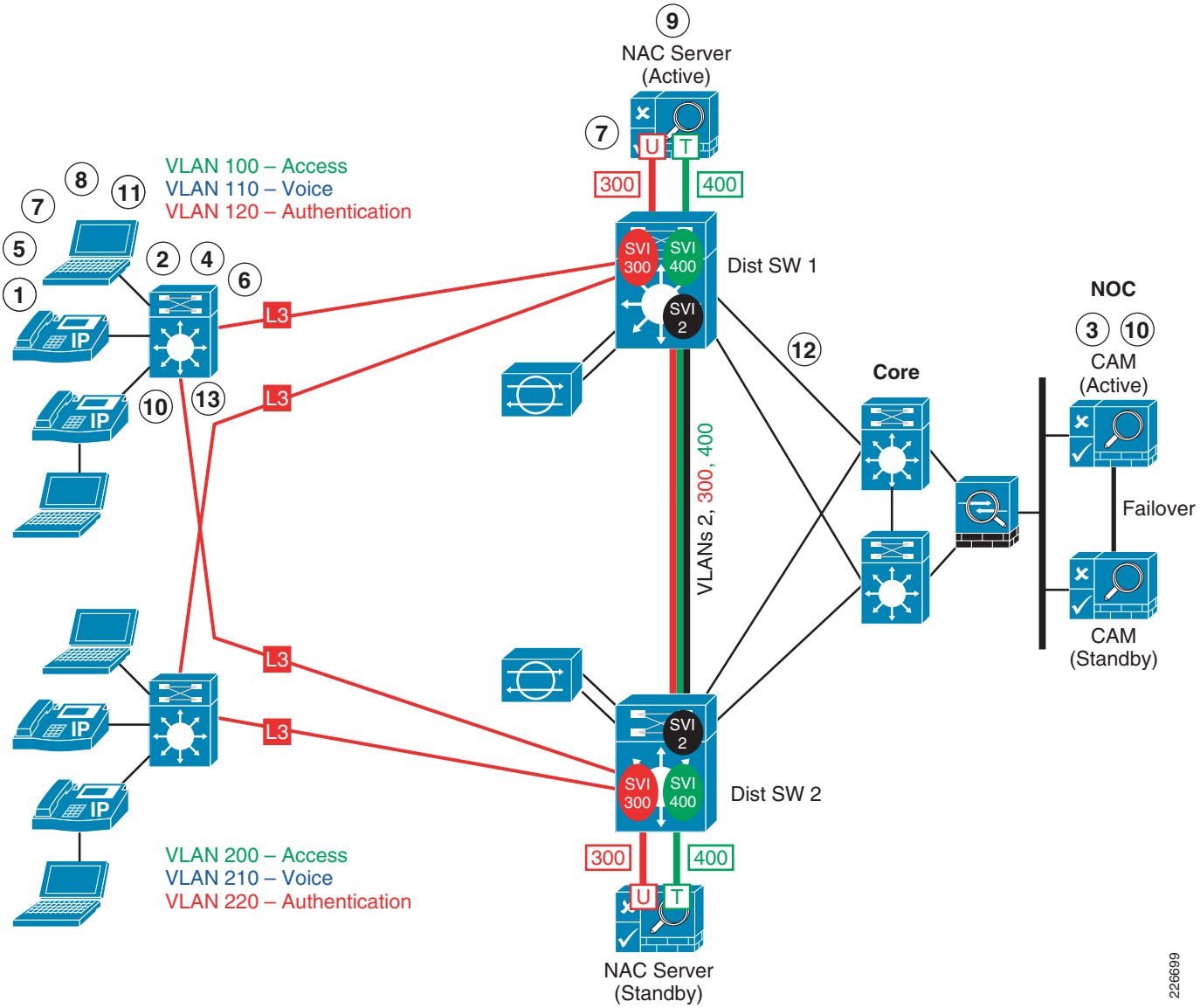
For information on configuring backend authentication servers, refer to the configuration guides for NAC appliance at the following URL:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/416/CAM/m_auth.html

NAC Operation and Traffic Flow

Figure 5-10 illustrates the process that occurs during NAC authentication and posture assessment for a user that *is* running the NAC Agent.

Figure 5-10 Traffic Flow with NAC Agent



The following steps provide details of what occurs in the process shown in Figure 5-10:

Step 1 User connects to switch port.

Step 2 Switch sends SNMP MAC notification trap to the NAC Manager informing it that a new device has connected to the network.

Step 3 NAC Manager checks its database to see if user is certified.

Step 4 If user is not certified, user is placed in the authentication VLAN

Step 5 The NAC agent starts sending discovery packets destined to NAC Server untrusted port.

Step 6 ACL on untrusted VLAN allows NAC Agent traffic through. ACL will block all other traffic not destined to the NAC Server or Remediation servers, hence infected machines unable to propagate.

Step 7 Agent discovers NAC Server and the user is prompted for authentication and goes thru posture assessment.

Step 8 If users needs remediation, remediation occurs manually or via the NAC agent.

Step 9 Step 8 Once user is authenticated, the NAC Server informs the NAC Manager that the user is certified.

Step 10 The NAC Manager moves user to Trusted Access vlan via SNMP write.

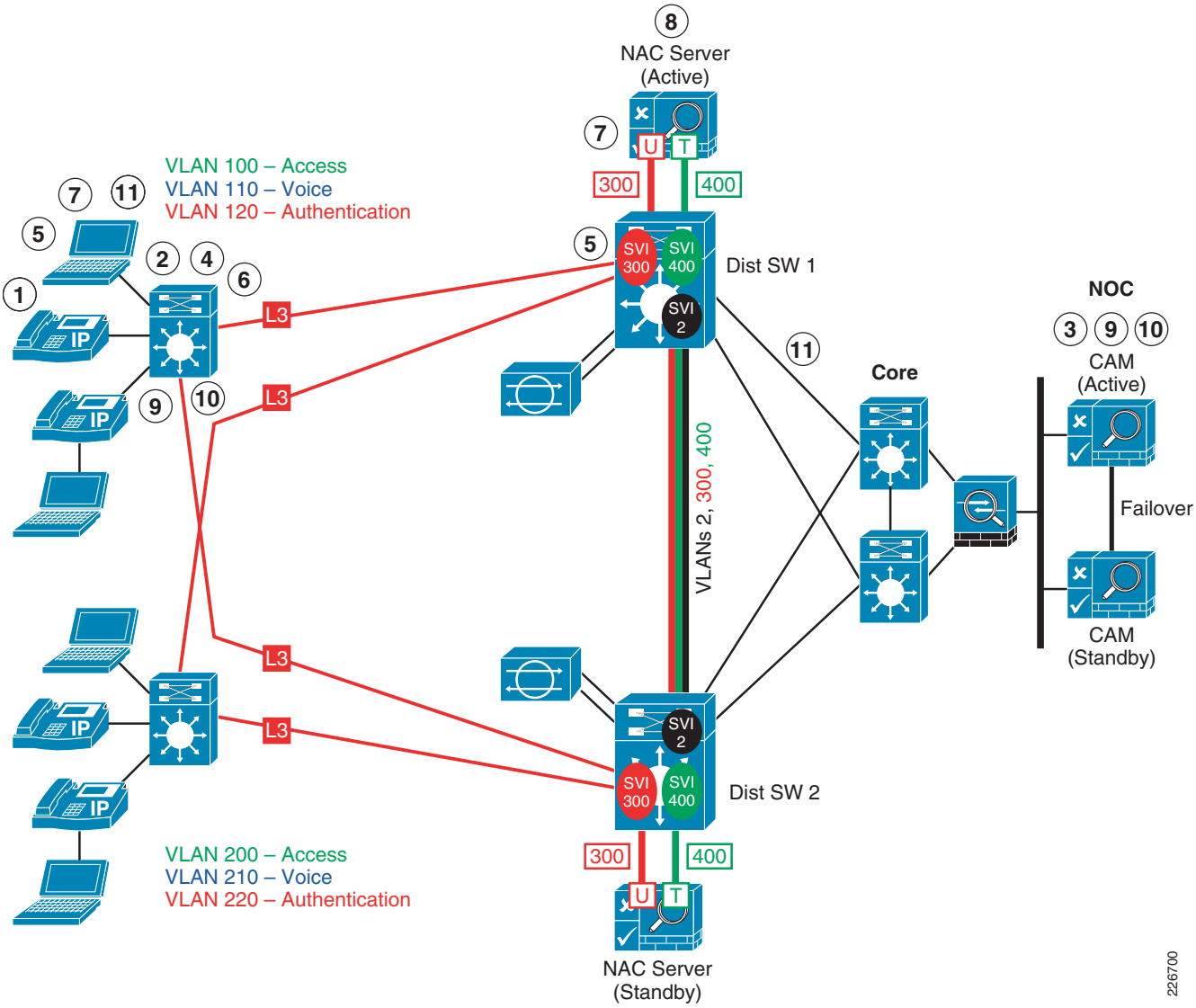
Step 11 The NAC agent forces a DHCP refresh to obtain an IP address in the Access VLAN.

Step 12 User gets access to network and completely bypasses NAC Server.

Step 13 ACL on trusted Access VLAN blocks NAC Agent discovery packets.

Figure 5-11 illustrates the process that occurs during NAC authentication and posture assessment for a user that is *not* running the NAC Agent.

Figure 5-11 Traffic Flow without NAC Agent



The following steps provide details of what occurs in the process shown in Figure 5-11:

Step 1 User connects to switch port.

Step 2 Switch sends SNMP MAC notification trap to the NAC Manager informing it that a new device has connected to the network.

Step 3 NAC Manager checks its database to see if user is certified.

Step 4 If user is not certified, user is placed in the authentication VLAN.

Step 5 The user opens a web browser and points to any website and the browser is redirected to the NAC Server's untrusted port via the policy-based routing policy on the distribution switches.

Step 6 ACL on untrusted VLAN allows this traffic through. ACL blocks all other traffic not destined to the NAC Server or remediation servers; therefore, infected machines are unable to propagate.

Step 7 Web login Active X or java applet agent is downloaded and user is prompted for login.

Step 8 Once user is healthy and certified, the NAC Server informs the NAC Manager that the user is certified.

Step 9 The NAC Manager moves user to trusted access VLAN via SNMP write.

Step 10 The NAC Manager bounces the switch port to force a DHCP refresh to obtain an IP address in the access VLAN.

Step 11 User gets access to network and completely bypasses NAC Server.

NAC Profiler

The Cisco NAC Profiler enables network administrators to efficiently deploy and manage NAC solutions in enterprise networks of varying scale and complexity by identifying, locating and determining the capabilities of all attached network endpoints, regardless of device type, in order to ensure and maintain appropriate network access. The Cisco NAC Profiler is an agentless system that discovers, catalogs, and profiles all endpoints connected to a network.

Typically, devices such as printers, FAX machines, IP Telephones and Uninterruptible Power Supplies, are not capable of running a NAC client. This means that in the deployment of NAC solutions, special purpose devices such as these do not have an agent available, nor do they provide a means by which a user can manually intervene through a browser. In this case, the ports connecting these endpoints must either be provisioned to circumvent the NAC system (e.g., placed on a special VLAN) or alternatively, the NAC system configured to recognize these devices via their unique hardware address in order to provide them access without direct participation in the admission control protocol. This typically requires that the NAC system be made aware of these endpoints by MAC address so that they can be admitted based on that credential alone with no further interaction with the NAC system. In the case of Cisco NAC Appliance, non-NAC devices such as these are accommodated via the Device Filters list on the NAC Manager.

In addition, the endpoint profiling information obtained by the NAC Profiler can be leveraged by the Cisco IBNS solution. The Profiler can be used by ACS as the backend database for MAB authentication. In the same way the Profiler adds entries to the device filters list on the NAC Manager, the information can be used for white listing MAC addresses for IBNS MAB authentication.

Cisco NAC Profiler provides endpoint profiling and behavior monitoring functions to allow administrators to understand the types of devices connecting to the network, their location and their abilities relative to the state of the port on which they currently reside. Endpoint profiling and behavior monitoring can be deployed in enterprise networks ranging from hundreds to tens of thousands of users. Once endpoints are profiled, the profiler can automatically apply NAC polices and update the device filter list on the NAC Manager.

Endpoint profiling and behavior monitoring requires the following functional components:

- Cisco NAC Profiler Server appliance
- Collector component on the NAC Server (Cisco NAC Appliance)

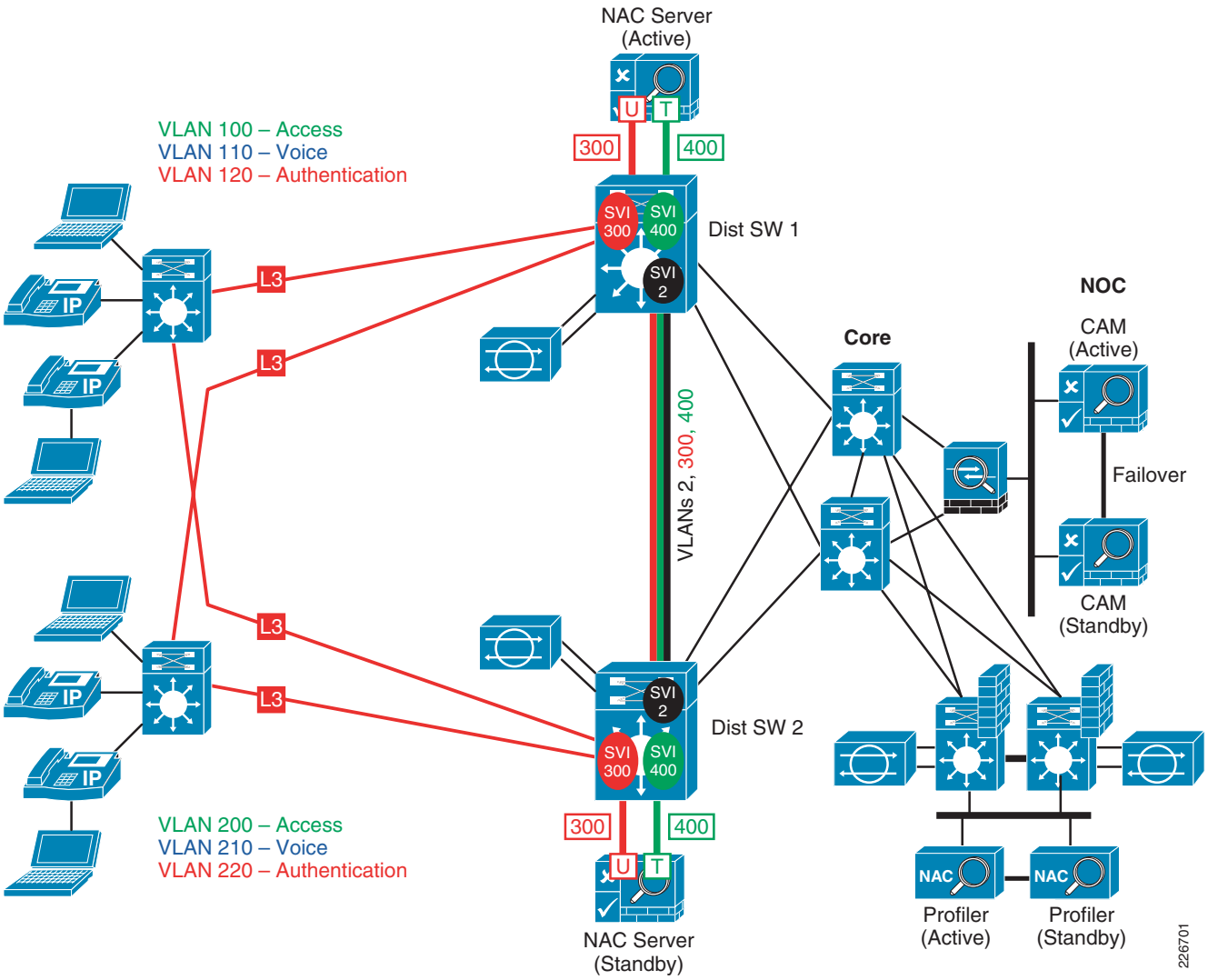
Deployment Best Practices

The following subsections cover the best practices for deploying the NAC Profiler in a routed-access campus design. Recommendations for the following deployment areas are provided:

NAC Profiler Placement

The NAC Profiler communicates with the NAC Collector modules running on the NAC Servers. It is recommended that the NAC Profiler server be placed in the NOC alongside the NAC Manager. However, if the firewall protecting the management network is performing NAT to hide the Management addresses from the data path of the network, then the NAC Profiler needs to be placed on the inside of your network where no NAT is being performed between the profiler server and the collectors. The communication between the NAC Profiler Server and the NAC Collectors does not work if the address of the NAC Profiler is being NAT'ed. In this case, the NAC Profiler server can be placed in the Campus Services Block connecting to the Core switches to provide central access to all the collectors deployed within the Campus. Stateful firewalls and IPS are used to protect the Profiler server and any other devices attached to the security service switch as depicted in Figure 5-12.

Figure 5-12 Campus NAC Profiler Design Diagram



High Availability

As with the NAC Manager and NAC Server, the Profiler server should be deployed for HA and should be deployed in an active/standby stateful failover configuration. Similar to the NAC Manager, the active profiler does all the work and the standby profiler monitors the active profiler and keeps its database synchronized via direct failover connection between the servers. A virtual IP address is configured and always resides on the active server. The virtual IP (service IP) address should be used for the SSL certificate. Ethernet 1 on both units should be used for the failover link connection used to share heartbeat packets and database synchronization information.

The collector functionality resides on the NAC Servers. If the NAC servers are configured in active/standby mode, it is recommended that the collectors be configured in this mode as well to provide redundancy. When configured in active/standby failover mode, only the active collector will collect endpoint profiling information and send it to the active profiler server. The active collector will coincide with the active NAC server.

Some of the key things to consider when deploying the collectors in HA mode are as follows:

- The NAC Collector uses the Virtual IP address of the NAC server to communicate with the Profiler.
- The NAC Collector HA pair is added as a single entry in the Profiler and communicates to the virtual IP address of the CAS. This needs to be configured as a client connection.
- Only one of the collectors are actively collecting endpoint profile information and sending it to the Profiler server.
- The name of the collector must be the same on both the active and standby collector.
- For the NetTrap Collector Module, SNMP traps for MAC Notification, linkup/linkdown status should be sent to the virtual IP address of the NAC Server.
- For the NetWatch collector module, both distribution switches must span traffic going to and coming from the access switches to both the active and standby collectors/servers.

NAC Collector Modules

The Cisco NAC Profiler server houses the database that contains all of the endpoint information gathered from the associated collectors including device type, location, and behavioral attributes. In addition, the Profiler Server presents the web-based interfaces and communicates with the NAC Manager to keep the device's filters list current and relevant. There are also forwarder modules that serve as middleware and facilitate secure communications between the Profiler server and the collectors. The Profiler server also provides a module that can receive and analyze data from other sources such as NetFlow records exported from NetFlow-enabled infrastructure devices (e.g., routers) or other NetFlow collectors. This information is combined with the information gathered from the collectors and is used to further profile the network attached endpoints.

The Cisco NAC Profiler Collectors reside on the same appliance with the Cisco NAC Appliance server and consists of a number of software modules that discover information about the network attached endpoints including a network mapping module (NetMap), an SNMP trap receiver/analyzer (NetTrap), a passive network analysis module (NetWatch), and an active inquiry module (NetInquiry). The major functions of the collector are to gather all of the data about the endpoints communicating to/through the NAC server, and to minimize and aggregate the information that is sent over the network to the Profiler server.

Table 5-8 summarizes the functions of the collector.

Table 5-8 Collector Modules

Module Name	Purpose and functionality
NetMap	SNMP module that queries network devices for the following types of information: • System • Interface • Bridge • 802.1x • Routing and IP
NetTrap	Reports link state changes and new MAC notifications
NetWatch	Passive network traffic analyzer

Table 5-8 Collector Modules (continued)

NetInquiry	Active profiling module that can be used with TCP open port and some application rules
NetRelay	Receives and processes NetFlow export packets directly from switches or other NetFlow data sources

It is not recommended to enable all the collector modules on the collector. Rather, only enable the ones that are needed. Otherwise, it might overload the collector. The following summarizes the recommended mandatory and optional modules that should be enabled.

Mandatory Collector Modules (Recommended)

- *NetTrap*—This module listens for SNMP traps sent by switches for new-mac notification or Link Up/Down notifications. This module sends all new MAC addresses to Profiler for profiling. This feature is defined per switch on the SNMP-Server configuration command line on Cisco IOS.
- *NetMap*—This module sits on the Collector and is responsible for doing SNMP polling of the access switches that the users connect to at timed intervals. The Collector SNMP polls the remote switches for specific MIB information with read access to the switch. This polling provides things like mac-address to port information, interfaces, link status, dot1x information, system information, and so forth.
- *NetWatch (SPAN)*—NetWatch module can listen on a SPAN destination port of a switch and send the ingested traffic information back to the Profiler. A NAC server requires an additional interface on each NAC server to collect this data. This module is essential because profiler is based primarily on DHCP information passed by devices and some other application traffic matching.

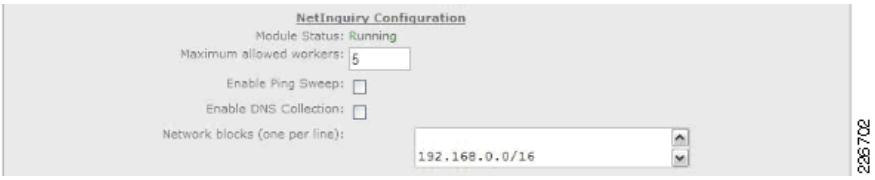
Optional Collector Modules

- *NetRelay*—(Netflow) is configured on each router on a per interface basis and the destination is the virtual management IP address of the NAC Server. A Netflow agent sits on the NAC Server and parses the Netflow information based on your traffic rules and networks configured on the Profiler.
- *NetInquiry*—This is a passive and active mechanism based on things like TCP Open ports. For example, the NAC Server does a SYN/ACK and then drops the connection in order to poll a particular subnet range or ranges for open TCP ports. If there is a response, it sends the information to the Profiler with the IP address and TCP port polled.

For a routed-access campus design, it is recommended that all three mandatory modules and the passive mechanism of the NetInquiry module be enabled. The passive mechanism of the NetInquiry module allows to restrict the information the collector will process based on a list of subnet ranges entered. In the case of the campus design, the subnet ranges should include the subnet ranges for the authentication, access and voice VLANs on the access switches and the subnet range for the DHCP server. It is not recommended to enable the active mechanism of NetInquiry. This can overload the NAC server with extra processing and hardware resources like memory and CPU utilization if not configured properly.

The screenshot in Figure 5-13 depicts the configuration of the passive mechanism of the NetInquiry module

Figure 5-13 Passive Mechanism of NetInquiry



Note Leave ping sweep and DNS collection disabled; u se this as a last resort. Ping sweep and DNS collection triggers pings and nslookups on the range of IP subnets added under **Network block** (see Figure 5-13). This is not recommended and rarely used.

SPAN or NetFlow can be used, based on the deployment and customer requirements, but only one or the other is recommended on a NAC server due to the amount of traffic that is sent to the collector modules and the other NAC functionalities that the NAC server has to perform. With NetFlow, vital informational pieces can be lost about devices (for example, DHCP vendor information, URL destinations, web client info, and web server information). In the case of the campus design where the collectors are connected to the distribution switches, SPANing the ports that are connected to the access switches will show all information coming from the access layer. In this case SPAN provides more information and NetFlow information would not be needed and would only create more overhead with the duplicate information. NetFlow is more suited for situations where SPAN would not provide all the information such as switches at remote sites.

For detailed instructions for configuring the NAC Profiler server and NAC Collectors in a Layer-3 OOB NAC design, refer to the *NAC Profiler and NAC SERVER Collectors in a Layer 3 Out-of-Band Configuration Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a30ad7.shtml

Threat Mitigated in the Enterprise Campus

Table 5-9 Enterprise Campus Threat Mitigation Features

	IP Spoofing	Botnets	DoS/DDoS	Layer 2 Attacks	Unauthorized Access	Spyware, Malware, Adware	Network Abuse	Data Leakage	Visibility	Control
Host-based Intrusion Prevention Systems (CSA)		Yes	Yes		Yes	Yes		Yes	Yes	Yes
Edge Filtering	Yes		Yes		Yes		Yes			Yes

Table 5-9 Enterprise Campus Threat Mitigation Features (continued)

VLAN Segregation	Yes		Yes	Yes	Yes					Yes
IPS		Yes	Yes	Yes		Yes	Yes			Yes
NAC				Yes	Yes	Yes	Yes		Yes	Yes
IBNS				Yes	Yes		Yes			Yes
Port Security			Yes	Yes	Yes					Yes
DHCP Snooping	Yes		Yes		Yes					Yes
IP Source Guard	Yes		Yes	Yes						Yes
Dynamic ARP Inspection			Yes	Yes	Yes					Yes