Community College and Vocational Education (CCVE) Design Overview

March 5, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: 78-xxxxx-xx

Community College and Vocational Education (CCVE) Design Overview

CONTENTS

CHAPTER 1 **Community College Reference Design Solution Overview** 1-1

Executive Summary 1-1

The Community College Environment 1-1

External Influences that Impact Community College Education 1-2

Vision for 21st Century Learning in Community College Education 1-2

Community College Challenges 1-3

Cisco Community College Reference Design 1-4

Community College Reference Design Service Fabric 1-4

High Availability 1-4

Differentiated Services 1-5

Access Layer Flexibility 1-7

Security 1-9

Network Security 1-9

Security Management 1-10

Secure Access Control 1-10

Mobility 1-11

Unified Communication 1-12

Network Management 1-13

Unified Communications Management 1-13

TelePresence Network Management 1-14

Performance Assurance 1-14

Routing and Switching Management 1-14

Identity Management 1-14

Video, Cable, and Content Delivery Management 1-14

Virtual Learning Environment 1-14

Secure Remote Access for Faculty and Students 1-15

Virtual Classroom 1-16

Online Collaborative Classroom Using WebEx Training Center 1-17

Review Streaming and Stored Video Using Video Portal 1-18

Operational Efficiencies 1-18

Network as a Platform 1-18

Data Center Optimization and Design 1-19

Facilities Management 1-20

Secure Connected Classroom 1-23

Classroom Connectivity to the Network 1-23

Network Admission Control for Guests and Students 1-23
Application and Network Control 1-24
Campus Safety and Security 1-25
IP-Based Video Surveillance 1-26
Communicate Campus Events and Emergencies with Digital Signage 1-26
IPICS for Emergency Collaboration 1-27
Conclusion 1-29

CHAPTER 2 **Community College Reference Design—Service Fabric Design Considerations** 2-1
Service Fabric Design Model 2-2
Main and Large Campus Design 2-2
Medium Campus Design 2-3
Small Campus Design 2-3
Building Profiles 2-3
Large Building Design 2-3
Medium Building Design 2-3
Small Building Design 2-4
Extra Small Building Design 2-4
Access Devices 2-4
LAN/WAN Design Considerations 2-4
LAN Design Considerations 2-4
Routing Protocol Selection Criteria 2-5
High Availability Design Considerations 2-5
Access Layer Design Considerations 2-5
LAN Service Fabric Foundational Services 2-6
WAN Design Considerations 2-6
WAN Transport 2-6
WAN Service Fabric Foundational Services 2-7
Security Design Considerations 2-7
Mobility 2-7
Unified Communications 2-8
Call Processing Considerations 2-8
Gateway Design Considerations 2-8
Dial Plan Considerations 2-9
Survivability Considerations 2-9

CHAPTER 3 **Community College LAN Design Considerations** 3-1
LAN Design 3-1
LAN Design Principles 3-3

Collapsed Core Campus Network Design 3-6

Community College LAN Design Models 3-7

Main College Campus Network Design Overview 3-9

Remote Large College Campus Site Design Overview 3-10

Remote Medium College Campus Site Design Overview 3-11

Remote Small College Campus Network Design Overview 3-12

Considering Multi-Tier LAN Design Models for Community Colleges 3-13

Campus Core Layer Network Design 3-13

Core Layer Design Option 1—Cisco Catalyst 6500-Based Core Network 3-14

Core Layer Design Option 2—Cisco Catalyst 4500-Based Campus Core Network 3-15

Core Layer Design Option 3—Cisco Catalyst 4500-Based Collapsed Core Campus Network 3-17

Campus Distribution Layer Network Design 3-18

Distribution Layer Design Option 1—Cisco Catalyst 6500-E Based Distribution Network 3-19

Distribution Layer Design Option 2—Cisco Catalyst 4500-E-Based Distribution Network 3-21

Distribution Layer Design Option 3—Cisco Catalyst 3750-E StackWise-Based Distribution Network 3-22

Campus Access Layer Network Design 3-23

Access Layer Design Option 1—Modular/StackWise Plus Access Layer Network 3-24

Access Layer Design Option 2—Fixed Configuration Access Layer Network 3-24

Community College Network Foundation Services Design 3-25

Network Addressing Hierarchy 3-25

Network Foundational Technologies for LAN Design 3-26

Designing the Core Layer Network 3-26

Designing the Campus Distribution Layer Network 3-30

Designing the Multilayer Network 3-31

Designing the Routed Access Network 3-32

Designing the Layer 3 Access Layer 3-34

Multicast for Application Delivery 3-35

Multicast Addressing Design 3-35

Multicast Routing Design 3-36

Multicast Routing Protocol Design 3-36

Designing PIM Rendezvous Point 3-36

Dynamic Group Membership Design 3-38

Designing Multicast Security 3-39

QoS for Application Performance Optimization 3-39

Community College LAN QoS Framework 3-40

Designing Community College LAN QoS Trust Boundary and Policies 3-43

Community College LAN QoS Best Practices 3-44

High-Availability in LAN Network Design 3-48

Community College LAN Design High-Availability Framework 3-48
Network Resiliency Best Practices 3-49
Device Resiliency Best Practices 3-50
Operational Resiliency Best Practices 3-52
Summary 3-53

CHAPTER 4 **Community College WAN Design Considerations 4-1**
WAN Design 4-1
WAN Transport 4-3
Private WAN Service 4-3
Internet Service 4-4
Metro Service 4-5
Leased-Line Service 4-7
WAN Aggregation Platform Selection in the Community College Reference Design 4-7
Main Campus WAN Aggregation Platform Selection 4-8
Remote Large Campus WAN Aggregation Platform Selection 4-10
Remote Medium Campus WAN Aggregation Platform Selection 4-10
Remote Small Campus WAN Aggregation Platform Selection 4-10
Network Foundation Services 4-11
Routing Design 4-11
QoS 4-13
Redundancy 4-16
Multicast 4-17
Summary 4-17

CHAPTER 5 **Community College Mobility Design Considerations 5-1**
Mobility Design 5-1
Accessibility 5-5
WLAN Controller Location 5-7
WLAN Controller Connectivity 5-8
Controller Connectivity to the Wired Network 5-9
Controller Connectivity to Wireless Devices 5-10
Access Points 5-20
Usability 5-27
Quality-of-Service 5-27
Guest Access 5-28
Traffic and Performance 5-32
Manageability 5-33
Reliability 5-36

Controller Link Aggregation 5-36
Controller Redundancy 5-39
AP Controller Failover 5-41
Community College Mission Relevancy 5-42
Safety and Security 5-42
Virtual Learning 5-43
Secure Connected Classrooms 5-44
Operational Efficiencies 5-44

CHAPTER 6 **Community College Security Design Considerations** 6-1
Security Design 6-1
Network Foundation Protection 6-5
Internet Perimeter Protection 6-7
Internet Border Router Security 6-10
Internet Firewall 6-10
Intrusion Prevention 6-13
E-Mail Security 6-14
Web Security 6-19
Data Center Protection 6-24
Network Access Security and Control 6-25
Cisco Catalyst Integrated Security Features 6-25
Cisco Identity-Based Network Services 6-26
IEEE 802.1X Protocol 6-26
802.1X and EAP 6-27
Impacts of 802.1X on the Network 6-27
802.1X in Community Colleges 6-28
Cisco NAC Appliance 6-28
NAC Appliance Components 6-29
NAC Appliance Modes and Positioning 6-31
NAC Deployment in the Community College Reference Design 6-35
Endpoint Protection 6-41
Community College Mission Relevancy 6-41
Virtual Learning Environments 6-41
Secure Connected Classrooms 6-42
Safety and Security 6-42
Operational Efficiencies 6-43

CHAPTER 7 **Community College Unified Communications Design Considerations** 7-1

Unified Communications Design 7-1
LAN Design 7-2
Layer 2 Access 7-2
Spanning Tree Protocol (STP) 7-3
Routed Access 7-3
Call Processing 7-4
Clustering over the IP WAN 7-6
PSTN Trunk Sizing 7-11
Calculating Traffic 7-11
Dial Plan Considerations 7-13
SRST 7-14
Community College Mission Relevancy 7-14
Virtual Learning Environment 7-14
Secure Connected Classrooms 7-14
Safety and Security 7-15
Operational Efficiencies 7-15

APPENDIX A **Reference Documents** A-1

CHAPTER 1

Community College Reference Design Solution Overview

Executive Summary

The Cisco Community College reference design is a framework designed to assist Community Colleges in designing and implementing a network for the 21st century learning environment. The design is created around solving complex business challenges that these institutions face. At its foundation is the network service fabric, which is a collection of features and technologies that serve to provide a highly available network that understands and adapts to the different services that it facilitates. The Cisco Community College reference design supports business solutions that utilize the service fabric were created to help these institutions:

- Create a 21st century virtual learning environment to enable highly interactive and collaborative learning and teaching experiences while delivering any content, anytime, anywhere, to any device.
- Increase operational efficiencies by using the network as a platform and optimizing data center design to extend cost reduction, improve utilization of under-used network capacity, and add flexibility to organizations through business process improvements.
- Design and implement secure connected classrooms that serve the educational needs of students and faculty by leveraging network and application control.
- Provide safety and security on campus by utilizing a platform architecture that proactively protects students, faculty, and staff.
- Allow for facilities management to interact with building controls, measure power consumption, and control energy output to reduce energy cost and carbon footprint, creating greener and more energy efficient campuses.

The Community College Environment

In the United States, community colleges, sometimes called junior colleges, technical colleges, or city colleges, are primarily two-year public institutions providing higher education and lower-level tertiary education, granting certificates, diplomas, and associate degrees. Traditionally, after graduating from a community college, some students transfer to a four-year liberal arts college or university for two to three years to complete a bachelor's degree.

External Influences that Impact Community College Education

Current economic conditions, a rise in continuing education enrollment, and the addition of courses for traditional secondary schools have all led to a substantial increase in enrollment at community colleges.

The worldwide recession has led to a dramatic reduction in funding for institutions of higher learning, which in turn have increased tuition rates. Increased tuition costs, as well as the reduction of available income due to the unprecedented high unemployment rate worldwide, have led students that would typically attend a traditional institution of higher learning to turn to community colleges as a lower cost educational option. This allows the student to begin a post-secondary education at a community college to attain a lower level degree, while having the option to continue on to an institution of higher learning to earn a traditional undergraduate degree at a later date.

Continuing education for adults has also been on the rise. Adults who have lost their jobs have been attending community colleges to augment their existing skill set or to take workforce development programs to retrain for another profession. The addition of distance learning as an option for working adults has also contributed to the rise in enrollment for continuing education students.

Secondary school students have also been a factor in the increased enrollment of community colleges. As the children of the baby boomers enter their college years, the competition to get into top-rated institutions has increased. One tool that secondary school students use to stand out from the crowd of applicants is to demonstrate their academic prowess at a college level by attending and passing community college courses while in secondary school.

Vision for 21st Century Learning in Community College Education

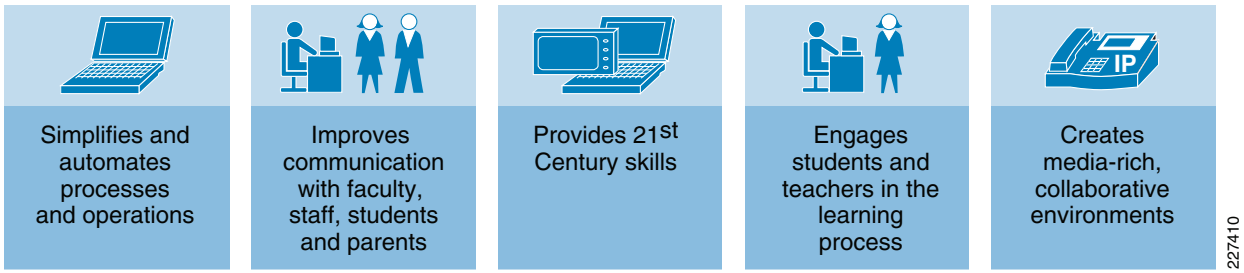
The 21st century learning environment will be an environment where anyone, from anywhere, at anytime can access community college resources. The traditional classroom will be extended by the use of online communities of learning. Students will be able to access their course work online, receive instruction by attending class either in person or remotely, and be able to retrieve the instruction at a later time through audio and video recordings augmented by online instructor and class notes.

This style of learning requires a collaborative environment in which instructors and students are not bound by geographic distances; students will be able to work together remotely to seamlessly complete projects and course work.

21st century learning will also be ecologically friendly by reducing the need to expand brick and mortar schools and commuting to campus to attend class. In addition, buildings and infrastructure optimized to reduce energy usage will all help reduce green house gasses and lead to greener and more energy efficient campuses.

Security, whether physical or logical, will become increasingly important in the 21st century learning environment. Security elements will be ubiquitous across traditional and virtual campuses and will work in concert to provide a safer environment for all students, faculty, and staff. See Figure 1-1.

Figure 1-1 Characteristics of a 21st Century School



Community College Challenges

In the United States from 2000 to 2006, there was a 10 percent growth in overall enrollment at two-year institutions, according to the most recent figures from the Department of Education. During the 2006-2007 academic years, 6.2 million students were enrolled in the country's 1,045 community colleges, 35 percent of all postsecondary pupils that year, according to a new National Center for Education Statistics study. Though full national figures for the 2007-2008 academic year are not yet available and most colleges only have estimates for their enrollments this fall, many colleges are projecting increases of around 10 percent over last fall.

This increased enrollment presents new challenges for delivering educational course work. The demand for instruction is increasing at a pace that does not allow the brick and mortar campus to expand quickly enough to handle growth. Community colleges have turned to online learning as the predominant method of handling this growth. While online learning has helped to handle the increase demand, it has been criticized for lacking the face-to-face experience that traditional learning provides, as well as lower than traditional passing rates for students. Community colleges are faced with the task of delivering a true virtual learning environment that delivers experiences that are comparable to the traditional environment. They must also allow for secure remote working environment for faculty and staff.

While community colleges are growing, their funding (like institutions of higher learning) is also being cut, so they have to do more with less. Operational efficiencies are being streamlined to allow community colleges to produce the same quality of education with fewer resources.

The rapid and expansive adoption of technology by students has led community colleges to offer connected classrooms and laboratories. Allowing the student to be connected to the network from the classroom or lab while receiving lecture has the benefits of mutual use of online resources, but it also requires community colleges to ensure that their networks are protected and that only authorized users are allowed access. Additionally, they must be able to control the use of applications and resources that reside on the network.

Since the incidents at Columbine and Virginia Tech, campus safety and security have become paramount to all educational institutions. Creating a safe campus is a major challenge for all community. They must employ the right tools to ensure the safety of the students, faculty, and staff. The safety and security systems in place must allow campus safety personnel to respond immediately and effectively in the case of an incident. A safe campus environment is a key differentiator for student and faculty recruitment and is an integral part of the community that welcomes local citizens and contributes positively to the area in which it resides.

As the world changes and becomes "greener", educational institutions are put in the position of leading that cause. Students are overwhelmingly concerned about greenhouse gasses as well as energy usage. The facility managers of community colleges must be able to strike the right balance between conducting business and optimizing energy use.

Budget reductions, increased enrollment, and limited staff are business constraints that impact the ability of community colleges to effectively address these challenges. A well thought out plan that optimizes resources, minimizes costs, and allows for flexibility in implementation is needed to allow community colleges to achieve the vision of 21st century learning.

Cisco Community College Reference Design

The Cisco Community College reference design is a framework designed around the vision, challenges, and constraints that community colleges face. Cisco has employed a business down approach in this design. The first step in creating the Community College reference design was to understand the vision that these institutions have for 21st century learning. Next, we identified the challenges that these institutions are facing. After understanding the vision and challenges, we recognized the business constraints that shape these institutions' ability to adopt solutions to address the challenges. Finally, we selected the best technologies, features, and equipment that allow these institutions to solve these challenges within the business constraints.

The Community College reference design is composed of the following solutions:

- Community College Reference Design Service Fabric
- Virtual Learning Environment
- Operational Efficiencies
  - Data Center Design
  - Facilities Management
- Secure Connected Classroom
- Campus Safety and Security

Community College Reference Design Service Fabric

The service fabric is the foundational network on which all solutions and services build. It comprises local and wide area networking equipment, security appliances, unified communications hardware as well as network, security, and mobility services that all work in concert to provide the fundamental network building block that all solutions and services use.

High Availability

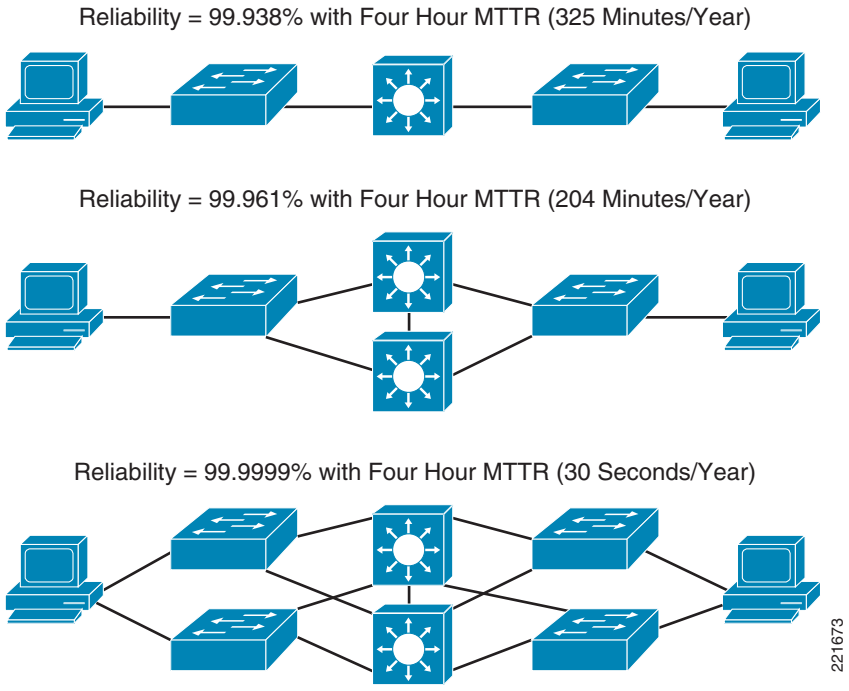
The high availability technologies used in the Cisco Community College reference design allow network equipment to eliminate the effects of any unplanned link or network failures by understanding the typology of the infrastructure and using that information to immediately re-route network traffic without the need to relearn (reconverge) the network. The use of these technologies allows critical service communications to remain unaffected by network outages.

The service fabric is designed to provide nonstop communications with resiliency throughout all the layers of the network. Many elements of the network must be correctly designed and implemented to ensure a highly available network.

Network resiliency is achieved by the careful design and implementation of network paths, devices, and power:

- *Path resiliency*—End-to-end resilient paths are required (Figure 1-2).
- *Device resiliency*—Resilient devices are usually preferred over resilient components within a single device. While resilient components within a single device are valuable, the best availability is usually achieved with completely separate devices (and paths).
- *Power resiliency*—Power diversity is another area that must be addressed because resilient devices attached to a single power source are vulnerable to simultaneous failure. For example, resilient core switches should have at least two unique power sources. Otherwise, a single power failure will bring down both core switches. Alternatively, backup power could be implemented. These types of mundane issues are very important when creating a highly available service fabric.

Figure 1-2 End-to-End Resilient Paths



Differentiated Services

Certain network services demand more from the network than others. For example, voice communications do not work if parts of the conversation drop out. Video conferencing is not useful if the picture keeps freezing. Additionally, a professor's use of the network to conduct class should take precedence over a student surfing the Web. Finally, if there are more traffic demands than the network can handle, the network should be able to make decisions as to which traffic is most important. The ability to understand, mark, shape, and limit traffic is embedded into the Cisco Community College reference design using Cisco's extensive array of quality-of-service (QoS) technologies.

There is some debate in the networking industry about the need to deploy QoS in campus architectures due to ample amounts of bandwidth and the rarity of congestion. However, during network attacks or a partial outage, this situation can change dramatically. It has been shown that QoS can serve as a vital tool to maintain the performance of priority applications and traffic during a degraded network condition.

The following are some reasons why QoS is important in the campus portion of the network:

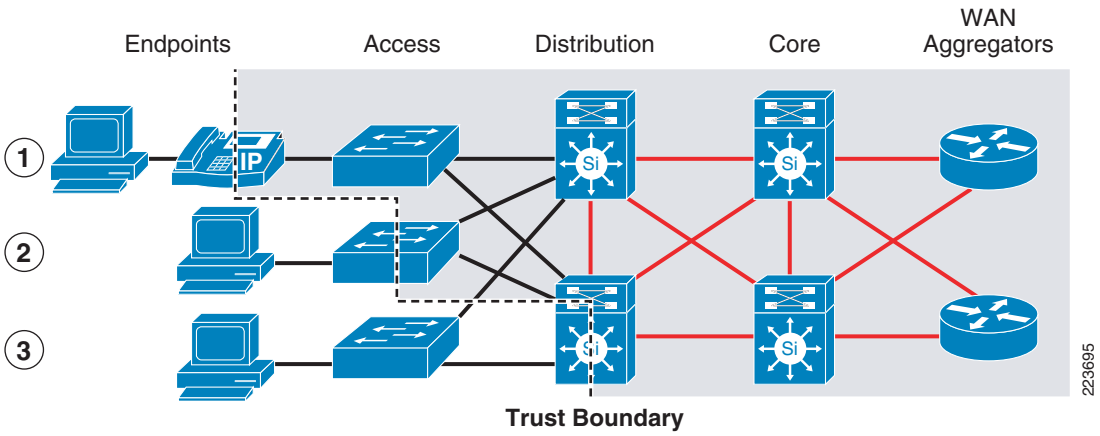
- The introduction of 10Gbps (and higher) link speeds is creating greater mismatches between high-speed and low-speed links in the campus. This increases the need to buffer and prioritize traffic.
- Well-known applications ports, like HTTP, are being used by a large number of applications. There is a need to distinguish between high-priority and low-priority traffic using the same port numbers to make sure priority traffic is transmitted.
- Prioritized traffic, like voice and video, must continue to flow even during a network attack or during a partial failure in the network. Attack traffic often masquerades as legitimate traffic using well-known port numbers. There is a need to distinguish between legitimate and bogus traffic by inspecting data packets more deeply.

The following principles should guide QoS deployments:

- Classify and mark traffic as close to the network edge as possible. This is called creating a *trust boundary*. Traffic crossing the trust boundary is considered “trusted” and the QoS markings are adhered to in the rest of the network.
- Police/rate-limit traffic as close to the source as possible. It is most efficient to drop unwanted traffic as close to the source as possible, rather than transmitting it further into the network before dropping it.
- Perform QoS functions in hardware rather than software. Software-based QoS functions can easily overwhelm the CPU of networking devices. High-speed networks require hardware-based QoS functions.

Figure 1-3 summarizes key QoS functions and where they should be performed.

Figure 1-3 QoS Functions



1. Optimal Trust Boundary: Trusted Endpoint
2. Optimal Trust Boundary: Untrusted Endpoint
3. Suboptimal Trust Boundary

Access Layer Flexibility

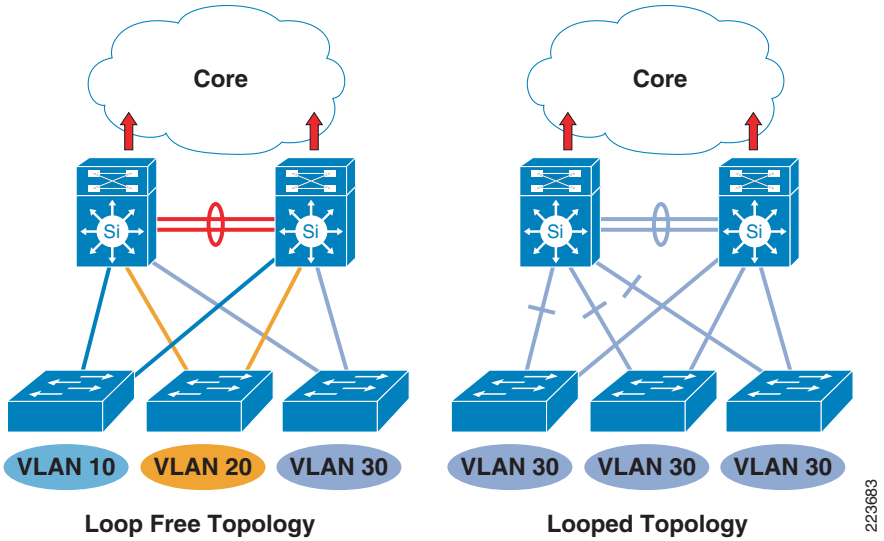
In a hierarchical network design, the core and distribution layers can reconverge in less than 1 second after most types of failures. The access layer typically has longer convergence times due to the inherent deficiencies of a flat Layer-2 architecture. Bridging loops, broadcast storms, and slow reconvergence are examples of access layer problems that reduce end-to-end availability. Spanning tree typically takes up to 1 minute to recover from a link or system outage, which is far too long to support real-time mission critical applications or provide 99.999 percent availability. There are several design changes and software features that can be implemented to improve availability in the access layer.

Currently, there are three different ways to design the access-layer control plane. Although all three of them use the same physical layout, however they differ in performance and availability.

The traditional multi-tier network is designed where all access switches run in Layer 2 mode between the access and the distribution, while they run in Layer 3 mode between distribution and the core. Cross-connects between distribution switches are usually Layer 2 links. When not optimized, this model is dependent on spanning tree, with all its inherent limitation, to detect and recover from network failures. As mentioned, load balancing of resilient uplinks is not possible because spanning tree usually blocks one uplink. HSRP, VRRP, or GLBP must be used to provide First Hop Routing Protocol (FHRP) resiliency. While deficiencies are evident in the traditional multi-tier approach, design changes and feature enhancements are available to greatly enhance availability and performance.

The current multi-tier best practice is to create unique VLANs on each access switch as shown in Figure 1-4. The best practice design offers several benefits. First, a loop-free topology is created. This means spanning tree does not impact reconvergence times. Traffic is load balanced across two active uplinks, achieving maximum throughput and minimum failover times. This loop-free topology also reduces the risk of broadcast storms and unicast flooding.

Figure 1-4 Best Practice Multi-Tier Has Unique VLANs on each Access Switch



One disadvantage of the best-practice multi-tier design is the requirement to redesign the VLAN and IP addressing scheme: unique IP subnet(s)/VLAN(s) per switch. This can be a significant challenge in large mature networks. The routed access model discussed below has this same drawback.

The routed access layer design is an improvement over the traditional multi-tier, as the name implies this design pushes routing into the access layer switches and creates an end-to-end routed infrastructure. Several important benefits are gained:

- Spanning tree issues are virtually eliminated.
- Reconvergence times for the end-to-end network can be reduced to 1 second or less.
- Reconvergence times become more predictable with the elimination of spanning tree.
- Resilient uplinks can be fully utilized.
- HSRP/VRRP is no longer needed to provide host resiliency. This simplifies configuration, management, and troubleshooting.
- Troubleshooting is accomplished using well-known Layer 3 tools, such as traceroute, ping, etc.
- Network layout, naming, and VLAN numbering can become standardized across buildings and campuses.

A drawback to the routed access model is the requirement to have separate IP subnets and VLANs on every access switch. This is in contrast to the traditional multi-tier model where a user VLAN can span several switches. However, the convergence times of the routed access layer are much less than that of flat Layer 2 networks.

Employing a hybrid access-layer design allows the network administrator to leverage their existing Layer 2 network while giving them the flexibility to implement and slowly migrate their existing network to a routed access layer design model. Advantages of a routed access design include the following:

- Prevention of loops without the need of multiple complex Layer 2 technologies such as spanning tree protocol.
- High availability and ease of network troubleshooting and management by leveraging well-known Layer 3 troubleshooting tools and technologies.

Security

Building a secure Community College reference design is paramount to the community college environment. Community Colleges have to balance network access given to students, guests, faculty and staff with protecting critical data and personal information of students and staff. The Community College reference design approaches security as described in the following subsections.

Network Security

Build a network security infrastructure that inherently detects and blocks invasive software attacks and intruder access.

Firewalls

- Combines firewall, VPN, and optional content security and intrusion prevention to distribute network security across your operations
- Provides threat defense and highly secure communications services to stop attacks before they affect business continuity
- Reduces deployment and operational costs while delivering comprehensive network security for networks of all sizes

Intrusion Prevention

- Identifies, classifies, and stops malicious traffic, including worms, spyware, adware, viruses, and application abuse
- Delivers high-performance, intelligent threat detection and protection over a range of deployment options
- Uses reputation filtering and global inspection to give businesses actionable intelligence and prevent threats with confidence
- Promotes business continuity and helps businesses meet compliance needs

E-mail and Web Security

Reduce costly downtime associated with E-mail-based spam, viruses, and web threats.

E-mail Security Appliances

- Fights spam, viruses, and blended threats to protect organizations of all sizes with industry-leading security capabilities
- Prevents data leaks, enforces compliance, and protects reputation and brand assets
- Reduces downtime, simplifies administration of community college mail systems, and eases the technical support burden

Web Security Appliances

- Integrates industry-leading web-usage controls, reputation filtering, malware filtering, and data security
- Takes advantage of Cisco Security Intelligence Operations (SIO) and global threat correlation technology to help optimize threat detection and mitigation

- Combines multiple layers of web security technology to combat complex and sophisticated web-based threats
- Supports built-in management capabilities to simplify administration and provide visibility into threat-related activity

Security Management

Simplify the configuration, monitoring, and management of your Cisco security capabilities.

Cisco IronPort Security Management Appliances

- Simplifies security management across Cisco IronPort E-mail and web security products
- Delivers centralized reporting, message tracking, and spam quarantine for the E-mail security appliances
- Provides centralized web policy management for web security appliances
- Allows for delegated administration of web access policies and custom URL categories

Cisco Security Manager

- Facilitates the configuration and management of Cisco firewalls, VPNs, IPS sensors, and integrated security services
- Ideal for controlling large or complex deployments of Cisco network and security devices
- Supports role-based access control and an approval framework for proposing and integrating changes
- Delivers flexible device management options, including policy-based management and methods for deploying configuration changes

Cisco Security Monitoring, Analysis and Response System

- Identifies threats by learning the topology, configuration, and behavior of the network environment
- Facilitates troubleshooting and identifying attacks or vulnerabilities for a wide range of enterprise networks
- Visually characterizes an attack path, identifies the threat source, and makes precise recommendations for threat mitigation
- Simplifies incident management and response through integration with Cisco Security Management software

Secure Access Control

Enforce network security policies; help secure user and host access control, and control network access based on dynamic conditions and attributes.

Network Admission Control Appliance

- Enforces network security policies on all devices by allowing access only to compliant and trusted devices

- Blocks access by noncompliant devices and limits the potential damage from emerging security threats and risks
- Reduces virus, worm, and unwanted access threats by promoting efficiency and integrating with other Cisco products

Cisco Secure Access Control System

- Controls network access based on dynamic conditions and attributes through an easy-to-use management interface
- Meets evolving access requirements with rule-based policies for flexibility and manageability
- Simplifies management and increases compliance with integrated monitoring, reporting, and troubleshooting capabilities
- Adopts an access policy that takes advantage of built-in integration capabilities and distributed deployment

Mobility

Cisco Mobility and Wireless Solutions for Community Colleges give students and staff the freedom to be anywhere on campus and still perform all the tasks they would normally do in a classroom's, or an office's wired network. The solutions enable new network connections to PCs, laptops, PDAs, printers, video cameras, videoconferencing units, IP phones, and other devices, making school resources more widely available and improving collaboration among students, Faculty and Staff

Mobility products include the following:

- Cisco Aironet Access Points connect Wi-Fi devices to networks in a variety of wireless environments. Cisco Next-Generation Wireless solutions use 802.11n technology to deliver unprecedented reliability and up to nine times the throughput of 802.11a/b/g networks. Wi-Fi certified for interoperability with a variety of client devices, these access points support robust connectivity for both indoor and outdoor environments.
- Wireless LAN controllers simplify the deployment and operation of wireless networks, helping to ensure smooth performance, enhanced security, and maximum network availability. Cisco wireless LAN controllers communicate with Cisco Aironet access points over any Layer 2 or Layer 3 infrastructure to support systemwide wireless LAN (WLAN) functions such as the following:
  - Enhanced security with WLAN policy monitoring and intrusion detection
  - Intelligent radio frequency (RF) management
  - Centralized management
  - Quality of service (QoS)
  - Mobility services such as guest access, voice over Wi-Fi and location services

  Cisco wireless LAN controllers support 802.11a/b/g and the IEEE 802.11n draft 2.0 standard, so you can deploy the solution that meets your individual school requirements. From voice and data services to location tracking, Cisco wireless LAN controller products provide the control, scalability, security, and reliability you need to build highly secure, district-wide wireless networks.
- Cisco Wireless Location Appliance allows school districts to simultaneously track thousands of devices from within the WLAN infrastructure, bringing the power of a cost-effective, high-resolution location solution to critical applications such as the following:
  - **H**igh-value asset tracking

  - IT management
  - Location-based security

This easy-to-deploy solution smoothly integrates with Cisco WLAN Controllers and Cisco lightweight access points to track the physical location of wireless devices to within a few meters. This appliance also records historical location information that can be used for location trending, rapid problem resolution, and RF capacity management.

Unified Communication

Cisco Unified Communications solutions provide many solutions for community colleges that wish to take advantage of media-rich unified communications functionality. Each aspect of the total unified communications architecture provides opportunities for enhancing links within the higher education community. Functionality includes IP telephony, unified client software, presence, instant messaging, unified messaging, rich-media conferencing, mobility solutions, and application development.

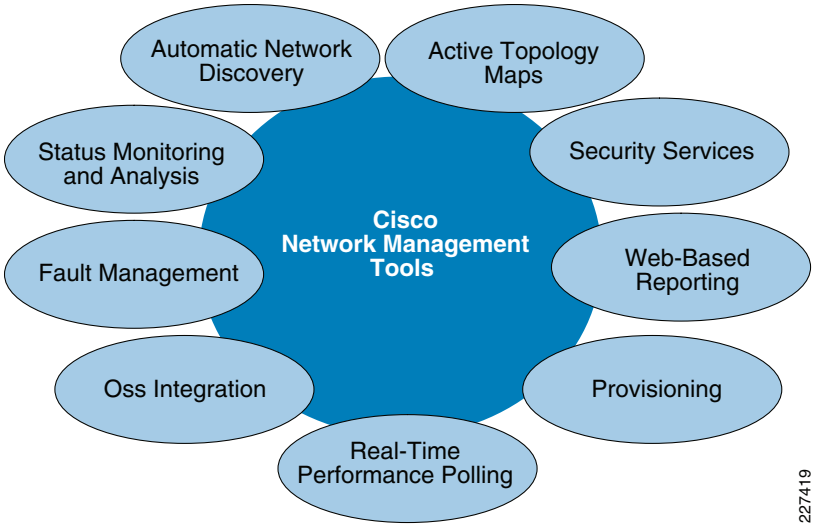
- *IP telephony*—At the foundation of the Cisco Unified Communications solution is its proven, industry-leading call processing system, Cisco Unified Communications Manager. This highly available, enterprise-class system delivers call processing, video, mobility, and presence services to IP phones, media processing devices, VoIP gateways, mobile devices, and multimedia applications. The system can scale to one million users across 1000 sites or more or 60,000 users within a single clustered system. Built-in resiliency keeps service reliable. Cisco also offers several unified communications platforms for small community colleges. All of these standards-based systems work with an array of third-party phones and dual-mode devices. The systems also provide integration with existing desktop applications such as calendar solutions, E-mail, enterprise resource planning (ERP) systems, and customer relationship management (CRM) software. Cisco unified communications capabilities can also be extended to a variety of mobile phones, including those that run Symbian, Blackberry, and Windows Mobile operating systems.
- *Unified client software*—Cisco offers several rich-media client applications that improve productivity and simplify processes. Available on Microsoft Windows and Mac OS environments as well as mobile operating systems, these clients support a range of applications, including voice, presence/messaging, unified messaging, video, and conferencing. Communications functionality has also been unified with applications from industry partners. For example, call control and presence can be launched and managed from within Microsoft Outlook through a Cisco Unified Personal Communicator widget or toolbar.
- *Presence and instant messaging*—Cisco presence solutions based on Session Initiation Protocol (SIP) or (SIMPLE) provide SIP presence and proxy services to deliver IM and click-to-call features. Through the presentation of dynamic presence information, presence solutions allow users to check the availability of colleagues in real time, reducing “phone tag” and improving productivity. Cisco presence and instant messaging solutions work in conjunction with Cisco Unified Communications Manager and support Cisco Unified Personal Communicator, Cisco IP phones, Cisco IP Phone Messenger, WebEX Connect, IBM Sametime clients, and Microsoft clients.
- *Unified messaging*—Cisco unified messaging solutions easily integrate with existing environments and provide flexible deployment options to meet each organization’s individual needs. The broad range of easy-to-manage solutions includes products tailored for small, medium-sized, and very large organizations, with feature-rich functionality aligned intelligently with business requirements.
- *Rich-media conferencing*—Cisco conferencing solutions help remote workers and teams communicate more effectively to save time and reduce costs. Integrated voice, video, and Web conferences can be set up and attended in a single step from IP phones, instant messaging clients, Web browsers, and Microsoft Outlook and IBM Lotus Notes calendars.

- *Mobility solutions*—Cisco Unified Communications extends rich call control and collaboration services to facilitate easy collaboration among mobile workers on campus or on the move. By anchoring communications in the network, Cisco Mobile Unified Communications solutions connect different mobile worker types and workspaces, provide a consistent collaboration experience regardless of location, maintain business continuity and compliance, and take advantage of least-cost routing of mobile communications over the education network. Cisco Mobile Unified Communications solutions support a wide range of popular handheld platforms, enabling workers to communicate quickly and easily using their familiar mobile equipment.
- *Application development*—Community colleges may operate in unique educational environments that require specialized applications. To meet these needs, Cisco provides a versatile service creation platform, enabling institutions and partners to rapidly and easily develop and deliver innovative media-rich and Web-rich applications. The platform also allows organizations to easily blend unified communications capabilities with existing business process systems.

Network Management

As community colleges implement more services and their networks become more instrumental as the platform for 21st century learning, the need to understand how the network is operating, what issues it is experiencing, and how those issues are impacting students, faculty, and staff become critical. Network management tools (see Figure 1-5) have been developed to help the IT staff understand the status and operation of service fabric and the services that are in operation in the network. This section discusses some of the specific network management options available to community colleges.

Figure 1-5 Cisco Network Management Tools



Unified Communications Management

The broad range of products in the Cisco Unified Communications portfolio provide enormous flexibility for applications, rich media collaboration, call control and messaging, and IP communications. Networks that deliver data, voice, video and rich media applications require unified, system-level management.

TelePresence Network Management

Cisco TelePresence integrates advanced audio, high-definition video and interactive elements with the power of the underlying network to deliver an immersive, face-to-face experience for collaboration. Cisco TelePresence network management is essential to the Cisco TelePresence experience.

Performance Assurance

Cisco network management products can help network administrators effectively manage network resources, plan for changes in resource usage, and resolve problems before they affect users. Quick access to configuration menus and easy-to-read performance reports on data, voice, and video traffic helps network operators to monitor trends, plan capacity, and optimize performance.

Routing and Switching Management

Cisco network management products support more than 400 types of Cisco devices with detailed reporting, monitoring, and configuration. They can save network administrators time and effort with improved inventory and configuration management, rapid software deployment, and simplified troubleshooting.

Identity Management

The ever-increasing number of methods for accessing networks makes security breaches and uncontrolled user access a primary concern. Network operators can use Cisco network management products with identity management features to protect systems and information through internal trust and identity policies, access control, and compliance features. The result is security assurance and protection of company profits and assets.

Video, Cable, and Content Delivery Management

Designed to be ready for advanced applications, Cisco network management products help ensure high performance and high availability, leading to higher subscriber satisfaction. With Cisco network management products, subscribers can access next-generation services such as IP telephony, video on demand, and interactive gaming.

Virtual Learning Environment

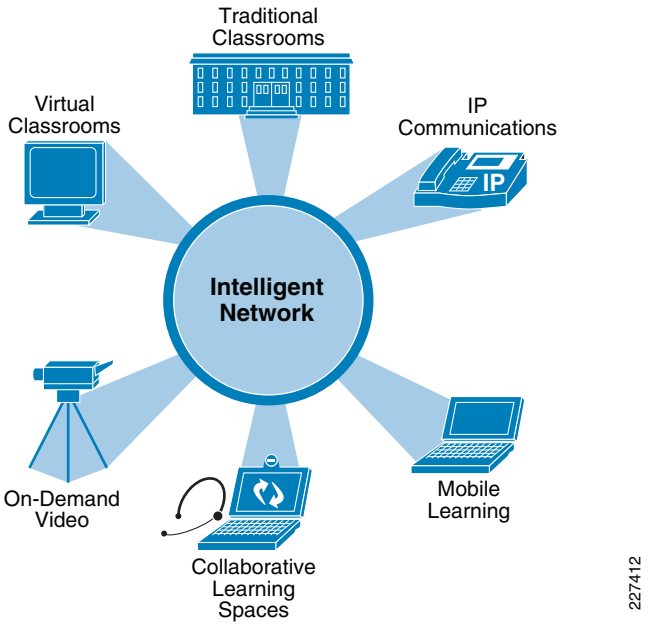
One of the key challenges that face community colleges is extending their learning environments beyond the campus to allow for online/distance learning, professor collaboration, and anytime/anywhere access for students to obtain course and educational materials. This virtual learning environment is key in allowing community to continue to grow at current rates and enhance the learning experience.

Cisco has several offerings for the virtual learning environment:

- Secure remote access
- Virtual classroom
- WebEx training center
- Video portal

See Figure 1-6.

Figure 1-6 21st Century Learning Environment



Secure Remote Access for Faculty and Students

Secure remote access is a way for community colleges to extend the network using secure remote access to anyone, anytime, anywhere, with virtually any device, in order to increase productivity and reduce costs. Secure remote access allows you to deliver network access safely and easily to a wide range of users and devices.

Cisco Secure Remote Access is a comprehensive and versatile remote access solution that supports the widest range of connectivity options, endpoints, and platforms to meet the changing and diverse remote access needs of community colleges.

The Secure Remote Access solution gives IT administrators a single point of control to assign granular access based on both user and device. It provides both full and controlled client-based network access to Web-based applications and network resources for a highly secure, flexible, remote access deployment.

Benefits include the following:

- Web-based access without preinstalled desktop software:
  - Facilitates customized remote access based on user and security requirements
  - Reduces desktop interaction and support costs
- Threat-protected Virtual Private Network (VPN) access:
  - Protects against viruses, worms, spyware, and hackers by integrating network and endpoint security in the Cisco Secure Sockets Layer (SSL) VPN platform
  - Eliminates the need for additional security equipment and management infrastructure
- Multiple VPN support from a single platform:
  - Supports both IP Security (IPSec) and SSL connectivity
  - Supports unified management of remote access and site-to-site VPN services to help reduce costs and management complexity

Virtual Classroom

Communication, collaboration, and learning are the fundamental building blocks of higher education. Students expect to use the latest technologies and many prefer dynamic online content to static printed materials. Distance learning and e-learning enable community colleges to deliver more engaging content to both on-campus and remote students, creating a new and potentially significant revenue stream.

Enhancing education through video and rich media elements can:

- Provide anywhere, anytime learning experiences not traditionally available to all students
- Offer a better way to present abstract ideas, making them easier to understand
- Eliminate the barriers of time, distance, and resources
- Permit faculty, staff, and students worldwide to function as if they were in the same room

Cisco's Virtual Classroom solution is an integrated learning and administrative environment that enables academic excellence and administrative efficiencies. The virtual classroom strategy focuses on the implementation of a network platform that can enable highly interactive and collaborative learning and teaching learning experiences while delivering any content, anytime, anywhere, to any device. As a result, Cisco's goal is to provide a scalable a solution that provides educational institutions with the necessary technology to solve business problems and address important issues, such as increasing student participation and graduation rates, in a cost effective and successful manner.

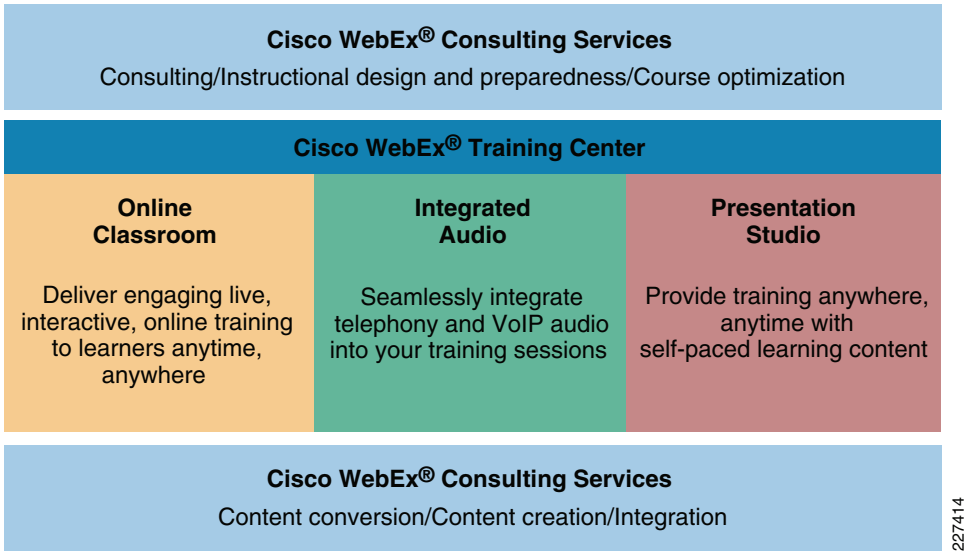
The Virtual Classroom solution is composed of campus-hosted technologies:

- Unified Communications
- TelePresence
- Video over IP technologies
- Wide area application services

The Virtual Classroom solution is designed to allow educational institutions to expand the reach of their offerings, both in a geographic and time-based manner. By using Web, video, and audio collaboration and scalable content delivery technologies, educational institutions can now reach students that are unable to physically attend class. Additionally, instructors and professors can record and edit pre-existing content into the recorded sessions and then post those content objects for the students to download to various devices, such as a mobile device. As a result, the schools can now scale their assets beyond their physical presence, such as subject matter expert or sign language teacher, to other classrooms and locations. Lastly, the ability to record the classroom events allows the student to also refer back to earlier classes for review or playback a class they missed.

Online Collaborative Classroom Using WebEx Training Center

Figure 1-7 Online Collaborative Classroom Using WebEx Training Center



WebEx Training Center is a Cisco web-hosted solution designed to facilitate online instruction for anywhere, anytime learning experiences. Features include the following:

- The ability to capture each student's attention with live, interactive instruction:
  - Share presentations, stream multimedia, and live video.
  - Connect online learners with remote computers, applications, and simulations before, during, or after live training sessions.
  - Pass control to attendees to demo applications.
- Encourage, improve, and track interaction:
  - Enhance and test retention with features like polling, testing, and breakout sessions.
  - Extend the reach of your educational facilities to students across the globe.
  - Simplify session registration and track attendance.
  - Record sessions and offer them on demand.
- Extend the reach of your institution while reducing costs:
  - Connect with more learners more often, while you eliminate travel and venue costs.
  - Charge for classes and online certification programs to turn your training center into a profit center.
  - Manage costs and pay as you go for an affordable, predictable monthly fee.

WebEx solutions are software delivered as a service (SaaS). Therefore community colleges do not need to worry about providing servers, maintenance, or support. Those items are handled as part of the subscription service.

Some advantages of SaaS:

- Performance and reliability for your critical communications.
- Keep sessions as private and safe as you need with exceptional security.

- No need to handle maintenance and upgrades.

Review Streaming and Stored Video Using Video Portal

Students can browse, search, and view digital media content interactively at the desktop with the Cisco Video Portal. An integrated component of the Cisco Digital Media System for Cisco Desktop Video, the Cisco Video Portal is a sophisticated video playback portal that uses standard Web technologies to deliver compelling live Webcasts and on-demand video to your audiences. Platform independent, the Cisco Video Portal fits easily into the existing network and infrastructure of community colleges.

The Cisco Video Portal features include:

- Customizable interface, program guide, and keyword search
- Personalized and featured playlists
- Advanced player controls—Full-screen video playback, fast forward, rewind
- Slide synchronization with video
- Submission and management of questions during live Webcasts
- Video sharing
- Secure log in and access to user-specific content based on Active Directory/LDAP
- Support for major video formats—Windows Media, Flash, MPEG-4/H.264, QuickTime
- Detailed content and user access reporting—Who, what, when, and how often

With the Cisco Digital Media Manager, the look and feel of the Cisco Video Portal can be customized to reflect the image of the educational institution.

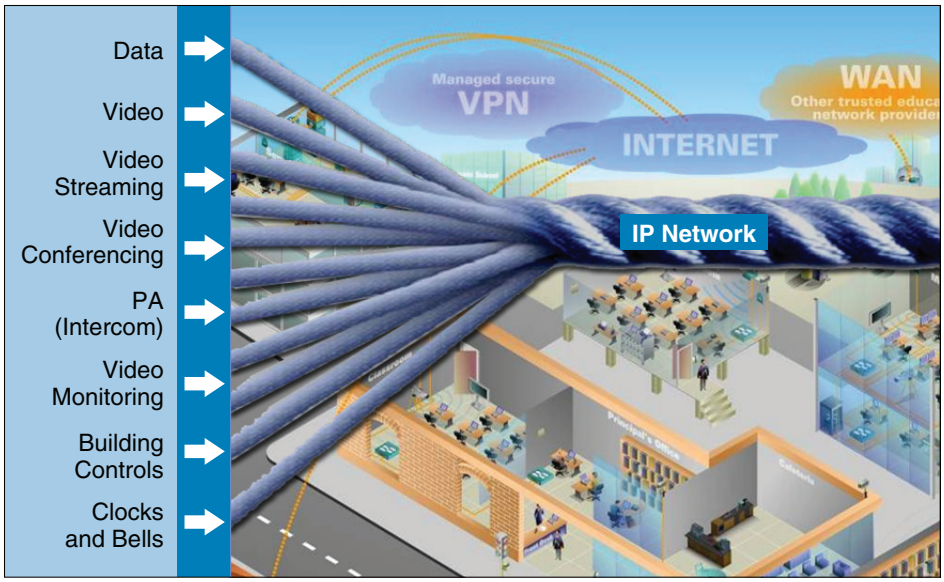
Operational Efficiencies

Community colleges are faced with the daunting task of doing more with less, facing explosive growth as budgets are reduced due to funding cuts. The Cisco Community College reference design leverages the use of the network as a platform to deliver an expanded array of education services and data center optimization as a means for creating operational efficiencies to reduce costs and capitalize on under-utilized network capacity.

Network as a Platform

The concept of using the network as a platform is the next phase in the evolution of network convergence. In the past, there was an effort to consolidate voice, video, and data networks onto a single IP network to allow organizations to reduce the cost of communication and take advantage of under-used network capacity. The network as a platform extends that concept beyond voice, video, and data services to allow for any IP-based service to use the network, wired or wireless, to extend cost reduction, improve utilization of under-used network capacity, and add flexibility to organizations through business process improvements. See Figure 1-8.

Figure 1-8 Network as a Platform



The network infrastructure or fabric must be able to understand the requirements of these non-traditional services and remain flexible and adaptable to their needs (discussed in detail later in this document). While the concept of adding non-traditional services like building controls and contextual awareness on top of an existing network seems like an easy task, the reality is that the underlying service fabric must be designed to accommodate and differentiate those services, especially as those services travel alongside others.

Data Center Optimization and Design

Cisco data center networking best practices give customers guidance and assistance in developing the data center network architecture most appropriate to meet changing IT requirements. These best practices augment the Cisco data center network architecture technologies and solutions to help IT architects and data center professionals take a phased approach to building and operating a comprehensive network platform for their next-generation data centers. By taking advantage of Cisco data center networking best practices, IT professionals can build a data center-class network, deploy solutions more quickly with lower risk, facilitate technology evolution and upgrades, and help ensure that IT staff are equipped with the right skills and expertise.

The benefits of data center optimization and design include the following:

- *Build and maintain a data center-class network*—Use validated and documented data center network solution designs to plan and implement networks that can achieve the stability and scalability required for mission critical data centers. By using proven best practices, community colleges can minimize downtime and accelerate recovery from disruptions. These designs also provide a robust foundation that customers or Cisco Advanced Services can use to make customizations to meet specific requirements.
- *Deploy solutions more quickly, with less risk and complexity*—Use Cisco data center best practices and designs to reduce the time, cost, and investment required for pre-production testing. Tried and tested designs help avoid the risks associated with technology disruptions, security exposure, non-scalable designs, and inappropriate software selection.

- *Facilitate technology evolution and upgrades*—The data center network is evolving to meet the challenges associated with cost, business alignment, resilience, and facilities concerns such as power and cooling. Cisco data center network best practices are constantly updated to incorporate these changes, so that customers can adopt them in a timely manner, with minimal risk.
- *Accelerate knowledge transfer*—The expertise and skills required to design and maintain increasingly sophisticated integrated data center networks are provided through constant training and knowledge transfer programs and infrastructure services. These programs include specialized Cisco CCIE® training such as the storage specialization, data center training labs, Cisco Press® books, Cisco Networkers, and executive briefing sessions.

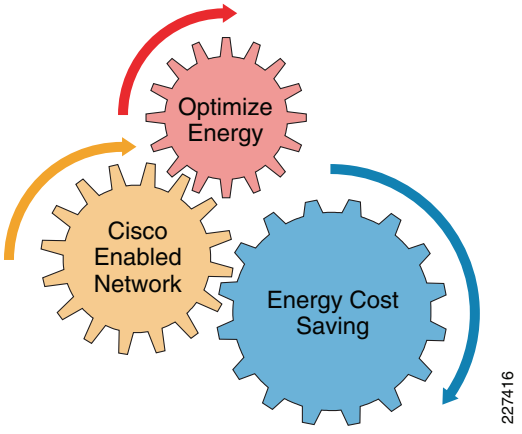
Facilities Management

In response to energy costs, environmental concerns, and government directives, there is an increased need for sustainable and "green" IT operations at community colleges. Methods to measure power consumption and control energy output are now the focus of businesses worldwide, with all customers looking for a method to reduce energy costs and implement increased efficient operation.

Cisco EnergyWise is a new energy management architecture that allows IT operations and facilities to measure and fine-tune power usage to realize significant cost savings. Cisco EnergyWise focuses on reducing power utilization on all devices connected to a Cisco network ranging from Power-over-Ethernet (PoE) devices such as IP phones and wireless access points to IP-enabled building and lighting controllers. It uses an intelligent network-based approach, allowing IT and building facilities operations to understand, optimize, and control power across an entire campus infrastructure, potentially affecting any powered device.

This section illustrates how community colleges can use Cisco EnergyWise with a network enabled by Cisco to better understand the power footprint of their organization and optimize to reduce energy costs (see Figure 1-9).

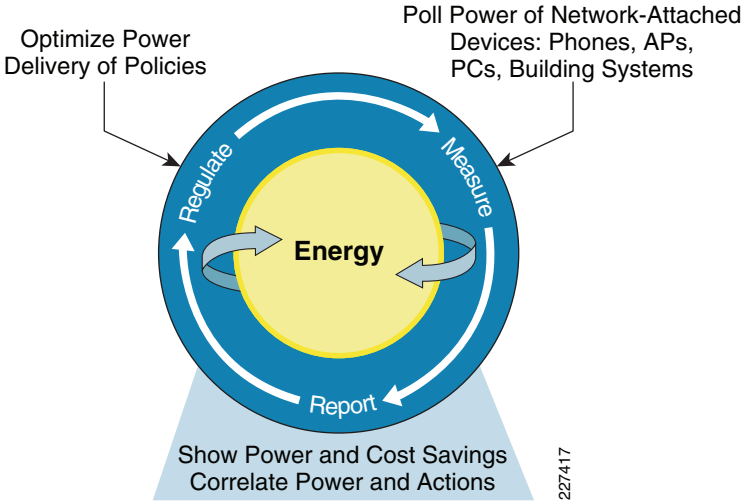
Figure 1-9 Cisco EnergyWise Optimize and Cost Saving



Cisco EnergyWise is an energy management architecture designed to measure power consumption and optimize power usage, resulting in effective delivery of power across the campus. Community college IT professionals can quickly optimize the power consumed in a building and the result is immediate cost saving with a clear return on investment.

Cisco EnergyWise measures current power consumption, can automate and take actions to optimize power levels, and can advise how much power is being consumed to demonstrate cost saving. After power consumption is understood, regulation using Cisco EnergyWise network protocols provides command and control of power usage. Energy consumed per location can easily be found with a realistic view of power consumed per wiring closet, building floor, or campus building (see Figure 1-10).

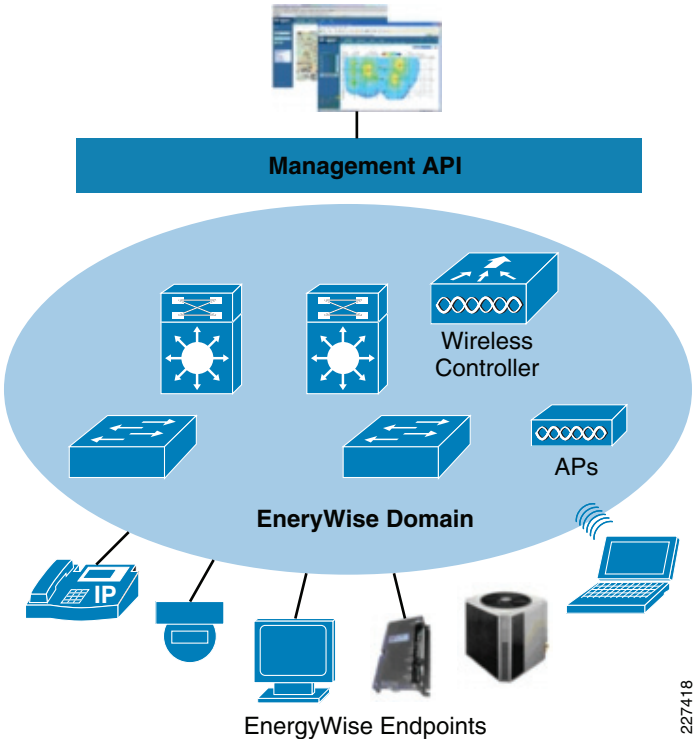
Figure 1-10 Cisco EnergyWise Optimized Power Delivery and Verification



The Cisco EnergyWise network is used to intelligently and proactively manage power consumption and consistently enforce policies to provide lower energy consumption. Cisco EnergyWise has the ability to monitor, manage, and reduce energy use by creating visibility to how electricity is consumed and create the ability to turn devices from always on to always available based on business needs. Cisco EnergyWise offers orchestration and coordinated power management utilizing the Cisco network for scalability and communication. For example, when an staff member enters a building, a series of events can take place enhancing efficient building operation. An employee's badge access might trigger the office phone to power up, wireless access point coverage to be assured, computers to boot up, and temperature of the office to be brought to a proper value. As a result, the user of Cisco EnergyWise is saving energy by powering off components when they are not needed.

In many cases, individual management systems are dedicated to each type of device in a building, with management systems for building controls, another for phones, and another for access points. Today a large number of systems need to be integrated together to perform orchestration of events for power management. Disparate system integration is difficult to achieve and not always used. Cisco EnergyWise network wide policies can control device power management, eliminating the need for a myriad of systems to integrate and coordinate with each other. Orchestration is a primary benefit for the above scenarios and it is the Cisco network acting as a proxy of information that allows systems to communicate in a synchronized fashion that reduces complexity and costs, assuring power saving. Figure 1-11 depicts a typical Cisco network enabled by Cisco EnergyWise, including the management layer and endpoints.

Figure 1-11 Network Enabled by Cisco EnergyWise



The cost savings realized by using Cisco EnergyWise are significant. In many countries the government mandates saving energy for the business and proof of saving energy can provide financial incentives. As compared to today's typical campus building or branch, the savings realized by just controlling IT power devices is significant.

The Cisco Network Building Mediator ("Mediator") is the industry's first solution that extends the network as a platform to transform the way buildings are built, operated, and experienced. The Mediator:

- Enables energy reduction across global operations
- Takes advantage of Cisco's expertise in collaboration, convergence, and security to foster sustainable energy use
- Provides flexible integration of new technologies that deliver energy efficiency, clean energy, and environmental stewardship

The Mediator collects data from the building, IT, energy supply, and energy demand systems, which use different protocols. The Mediator then normalizes the data into a common data representation. This enables the Mediator to perform any-to-any protocol translation and to provide information to the end user in a uniform presentation.

This network-based framework creates a common, standards-based, open platform that allows campus applications, cloud services, and building/IT systems to communicate. The Mediator is protocol-agnostic and extends the network to serve as an effective foundation for sustainability management. The Mediator provides the following benefits:

- Reduced total cost of ownership (TCO)
- Simplified management of energy and facilities
- Flexible integration of building, IT, and clean technology systems
- Enhanced uptime and resiliency with networking technology

- Secure, high-quality delivery of concurrent building and IT services
- Future proofed investment with third-party applications and cloud services

The Mediator provides a network-based framework that interconnects four key systems: building, IT, energy supply, and energy demand. The integration of these disparate systems onto an IP network leads to a truly converged, energy-efficient building.

The Mediator's strategy is built on:

- *Any-to-any connectivity*—Building, IT, and "green" technologies
- *End-to-end management*—Efficiency, conservation, and decarburization
- *Extensible platform*—Third-party applications and cloud services

Secure Connected Classroom

Classroom Connectivity to the Network

Providing connectivity to students while attending class is the foundation of 21st century learning, however it also poses many problems for community colleges. They must ensure that the person accessing the network should be allowed on the network and that the computer connecting to the network is free of viruses and other ailments that might adversely impact the network or others users. Secondly, while connectivity is provided, all steps should be taken to ensure the person connected is using the network for educational purposes and not illegal activities, such as sharing copyrighted material. Some community colleges chose to restrict the student to only access certain network resources while in class.

The density of wireless users in one location can also be problematic. Wireless designs must take into consideration the number of users, radio interference, and network utilization. The Community College reference design addresses these challenges is a variety of ways.

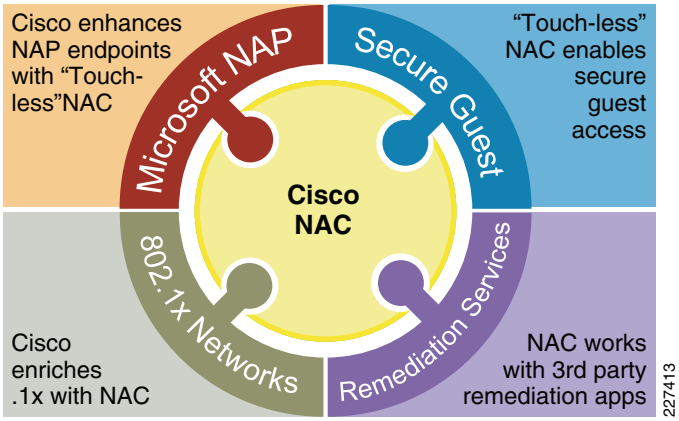
Network Admission Control for Guests and Students

Network admission control allows community colleges to stop unauthorized or noncompliant devices and users from propagating threats into the network. Cisco Network Admission Control (NAC) enforces your institution's security policies and posture on all devices and users seeking network access.

Current business mechanisms such as Web 2.0, social networking, and cloud computing increase the likelihood of sensitive data residing outside of controlled devices. Traditional security products designed to protect closed environments with well-defined security boundaries are not effective in the new Web 2.0 environment.

Cisco NAC prevents loss of sensitive information by giving institutions a powerful, role-based method of allowing only compliant and authorized access and improving network resiliency. With Cisco NAC, only compliant and trusted endpoints—from PCs to printers, IP phones, and PDAs—are allowed onto the network, thereby limiting the potential damage from emerging security threats and risks.

Figure 1-12 Cisco Network Admission Control



Application and Network Control

Cisco NAC helps reduce the potential loss of sensitive information by enabling organizations to verify a user's privilege level before granting network access. When that access is granted, the user is placed into a "role." Using role-based access control, community colleges can define security policies based on the role of the person using the network. For example, if a student connects to the network in a classroom, they can be put in a "student" role, which can then control where they can go and what they can use on the network, internally or externally.

As students, faculty, and staff carry their laptops to external locations, it is critical that the security protection on each endpoint device is up to date. The security policy is applied when an endpoint device attempts to connect to the internal network. Cisco NAC provides comprehensive policy enforcement and support. Cisco NAC integrates with a wide range of endpoint security applications. It supports built-in policies for more than 350 applications from leading antivirus and other security and management software solution providers. Many user-friendly capabilities, such as silent remediation and auto-remediation, help bring devices into compliance without causing user impact.

Cisco NAC helps community colleges provide secured guest access and assigns internal user access based on a user's role in the organization. Secure guest access allows visitors and guests to utilize the network without sacrificing the network security of the community college.

Cisco NAC provides full integration with wireless, VPN, and 802.1X and can be implemented in a single-sign-on (SSO) manner to maximize security benefits and minimize user impact.

Controlling peer-to-peer and instant messaging applications present several challenges, especially in the community college environment. Peer-to-peer applications, such as Gnutella and BitTorrent, are often used to share copyrighted material, such as music and movies, and instant messaging applications, like yahoo IM or AIM, can be used in the education environment as a way to pass notes in class. Both can be a challenge to control as often they will use common application ports such as port 80, which is also used to connect to Web pages, so just turning off the port is not an option. Educational institutions need to be able to look deeper inside the packet that is going across the network to ensure that these ports are not being used to circumvent security policies. Cisco has several ways of inspecting this traffic to ensure security compliance.

Campus Safety and Security

Cisco physical security solutions provide broad network-centric capabilities in video surveillance, IP cameras, electronic access control, and ground breaking technology that converges voice, data, and physical security in one modular appliance. Our connected physical security solution enables community colleges use the IP network as an open platform to build more collaborative and integrated physical security systems while preserving their existing investments in analog-based technology. As customers converge their physical security infrastructures and operations and begin using the IP network as the platform, they can gain significant value through rapid access to relevant information and interoperability between other IP-centric systems. This creates a higher level of situational awareness and allows intelligent decisions to be made more quickly.

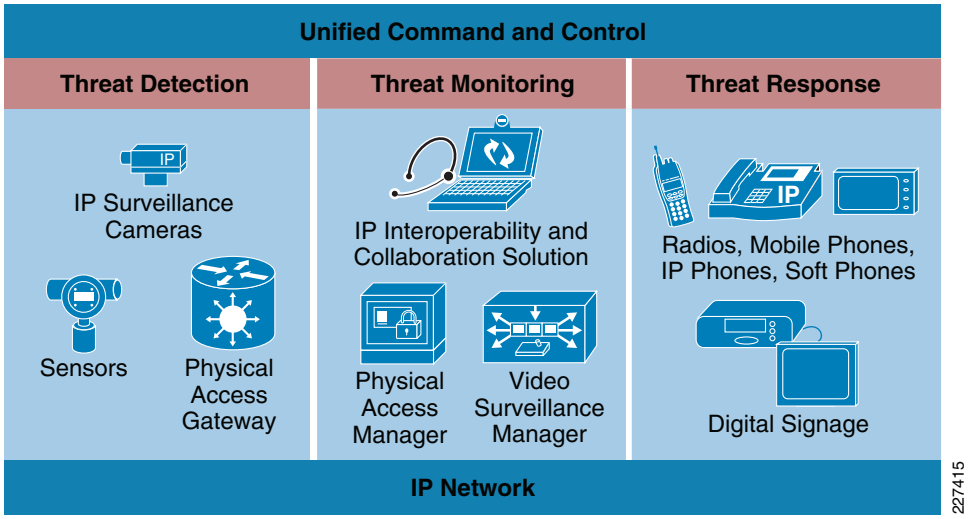
Cisco enables customers to build cost-effective, modular physical security solutions that are both best in class and interoperable. Cisco physical security products support the company's vision of a single unified security product suite that enables integration with all security operations within the IP network and with many non-security applications. Using the network as an open, scalable platform for integrating security provides community colleges with several benefits, such as operational flexibility, greater protection capabilities, lower cost of ownership, and reduced risk.

The Cisco Open Platform for Safety and Security is a platform architecture that proactively protects students, faculty, and staff through a scalable, tested network design. The architecture provides a more complete common operating picture, improves decision and response cycle times, and takes advantage of the network to expand the range and effectiveness of your emergency operations teams.

The platform takes advantage of a converged, IP network and provides the following benefits:

- Increases student, faculty, and staff safety and security through emergency notification and early warning
- Improves risk mitigation by facilitating continuity of operations (COOP), crisis management, all-hazards incident response, as well as facilities and critical infrastructure protection
- Reduces cost of operations
- Overcomes interoperability issues

Figure 1-13 Unified Command and Control



IP-Based Video Surveillance

Every day, you strive to make your schools as safe as possible. You develop plans, deploy systems, and train your staff on how to prevent, deter, detect, and respond to safety incidents. And you are doing a great job. Statistics show that community colleges continue to reduce the number of safety incidents.

For many decades, video surveillance has been a key component of the safety and security groups of community colleges. As an application, video surveillance has demonstrated its value and benefits countless times by:

- Providing real-time monitoring of a facility's environment, people, and assets
- Recording events for subsequent investigation, proof of compliance, and audit purposes

As security risks increase, the need to visually monitor and record events in an institution's environment has become even more important. Moreover, the value of video surveillance has grown significantly with the introduction of motion, heat, and sound detection sensors as well as sophisticated video analytics. Video surveillance can be integrated with and complement access control policies, providing video corroboration of access credential use.

These systems are realized through an open, standards-based, IP-network-centric functional and management architecture. As a network-centric company, Cisco has enabled the migration of many applications and systems onto a converged infrastructure. As a global enterprise organization, Cisco has developed and adopted a network-centric system architecture that meets the extensive requirements for a world-class video surveillance system.

The Cisco video surveillance architecture provides several benefits:

- Increased reliability and availability
- Greater utility (any camera to any monitoring or recording device for any application)
- Increased accessibility and mobility
- Multivendor video surveillance system "best of breed" interoperability
- The ability to enhance other building management system capabilities through improved interoperability

Communicate Campus Events and Emergencies with Digital Signage

Traditionally, campuses have advertised events on posters tacked to bulletin boards around campus. The drawbacks of paper-based communications include clutter, out-of-date information, the time needed to constantly put up and take down posters, and paper waste.

Cisco Digital Signage provides more timely and eye-catching communications that can be scheduled to appear in different parts of the campus. Install the networked digital signs in high-traffic areas such as the entrances to buildings, student union, and faculty lounge areas, then display information about campus events and up-to-date emergency alerts and instructions. Assign any staff person, not necessarily an IT staff member, to use the interface to schedule content. You can even deliver different content to different signs—for example, promoting plays in the Theater Department building and advertising specials in the book store.

Popular uses of digital signage in community colleges include:

- Emergency notifications and instructions
- Event announcements, such as sports, guest speakers, registration/drop deadlines, etc.
- Classroom changes
- Student and staff group training

- Advertising in bookstores and stadiums
- Way finding
- Information for major events, such as graduation or donor recognition receptions
- Room scheduling

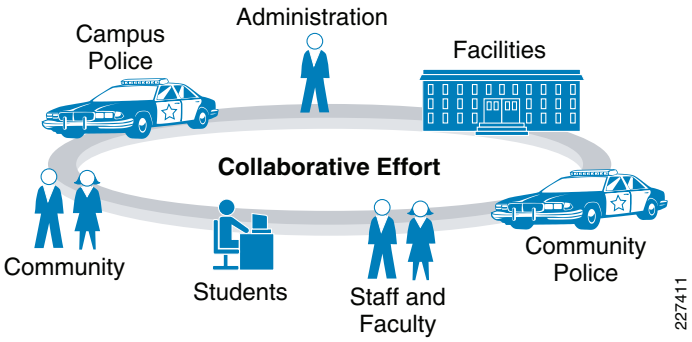
IPICS for Emergency Collaboration

An emergency by definition is a chaotic event. Whether the emergency is a motor vehicle accident, a crime in progress, or a natural disaster that strikes a wide area, those who are responsible for responding require real-time, accurate information in order to effectively manage the event. Responding agencies—traditional first responders (police, fire, and emergency medical services), allied agencies (such as power utilities or other enterprises), or nongovernmental organizations such as the Red Cross and Red Crescent—need to work efficiently together to mitigate the effects of the incident.

Push-to-talk (PTT) Land Mobile Radio (LMR) systems have been the backbone of emergency response for decades. Unfortunately, one of the problems of LMR has been a legacy of incompatibility. Radios that do not use the same frequencies, LMR vendor-proprietary enhancements to established standards, and high infrastructure costs have led to a fractured LMR landscape that prevents effective coordination. Agencies that may have to work together may not be able to talk to each other. According to a report prepared by COMCARE, the United States alone has more than 100,000 emergency response agencies, most of which cannot easily communicate with each other or the public.

Another challenge is that responders now need to communicate with devices other than LMR systems, including Sprint/Nextel Push-To-Talk (PTT) phones, IP phones, and PCs. Technology is no longer an optional or a luxury item for emergency response. In an increasing number of cases, technology is vital to the situational awareness, span of control, scalability, and efficiency of incident response. However, incompatible communications technologies also build barriers that complicate interagency collaboration. Organizations must be able to break down these communications silos to realize the full benefit of their technology investments and to operate efficiently.

Figure 1-14 Campus Safety



Cisco IPICS provides simple, scalable, comprehensive communications interoperability that encompasses radio networks, IP and non-IP networks, telephones, cell phones, and PC clients. Benefits of the Cisco IPICS solution include:

- *PTT everywhere*—By extending PTT and voice services from the LMR networks to IP networks, Cisco IPICS provides communications interoperability between wired and wireless networks.

- *Flexible and efficient operations and incident management*—Cisco IPICS provides an easy-to-use, Web-based interface for managing users, user groups, and radio channels across multiple networks and operational domains. Resources can be quickly added and then removed when no longer necessary, allowing graceful escalation and de-escalation based on the incident scope.
- *One-click activation of predefined policies*—Cisco IPICS Policy Engine, new in Cisco IPICS, enables administrators to create policies that define standard operating procedures—including talk group establishment and user notification—and then activate those policies with a single click. Notification methods can include radio, cell phone, public switched telephone network (PSTN) phone, Cisco Unified IP phone, Cisco IPICS Push-to-Talk Management Center (PMC) Client, pager, E-mail, or Short Message Service (SMS) text message. (Some methods require a Simple Mail Transfer Protocol [SMTP] gateway.) The agency defines policies using an intuitive, Web-based interface.
- *Customization*—Cisco IPICS can be customized to meet organizations' individual requirements. As an organization's needs change over time, Cisco IPICS can adapt with them.
- *Low cost and investment protection*—Cisco IPICS enables comprehensive communications interoperability at a fraction of the cost of replacing existing radio systems. By capitalizing on existing communications networks and devices, Cisco IPICS avoids the expense of unnecessary upgrades to existing radio networks. Furthermore, by enabling a graceful migration to IP networks and services, Cisco IPICS protects what can be a significant investment in traditional radio networks and devices. Agencies can also eliminate the expense of purchasing radios for office personnel by using the Cisco IPICS PMC Client for PCs and laptops or the Cisco IPICS Phone Client for IP phones.
- *Unified command and control*—Dispatchers and incident commanders can manage operations from one or more locations using the Web-based Cisco IPICS Administration Console.
- *Standards compliance*—Cisco IPICS takes advantage of industry-standard hardware and a proven IP architecture to create a framework for interoperable voice, video, and data communications. Organizations that currently use multiple wireless devices, including PTT, cellular, and wireless LAN (WLAN), can smoothly migrate to Cisco IPICS, which provides the infrastructure and feature set needed to achieve wide-ranging business and service goals. A standards-based solution also gives organizations the flexibility to add communications devices from any vendor.

Controlling physical access into buildings, rooms, and labs traditionally meant the use of an independent security network. The Cisco Physical Access Control solution is scalable and flexible, able to manage from one to several thousand doors. With this solution, institutions can combine modules to customize solutions and to manage the entire system remotely. In addition, this physical access solution easily integrates with Cisco's Video Surveillance solution and can use IP network services.

The Cisco Physical Access Gateway is an intelligent, distributed processing networking edge device module that connects door hardware, such as locks and readers, to the network. Accessory modules are available to handle additional doors and input/outputs.

The Cisco Physical Access Manager is the management application is used to configure hardware, monitor activity, enroll users, and integrate with IT applications and data stores. The data it collects can easily be shared with other security devices using the Cisco Open Platform for Safety and Security to create a holistic security view of the campus.

Conclusion

The Cisco Community College reference design is built upon a highly resilient and flexible service fabric to provide community colleges with design solutions to solve business problems. It provides solutions that enable a 21st century learning environment, allowing for highly interactive and collaborative learning and teaching experiences while delivering any content, anytime, anywhere to any device.

To learn more about the Cisco Community College reference design, refer to the following URL: http://www.cisco.com/go/education

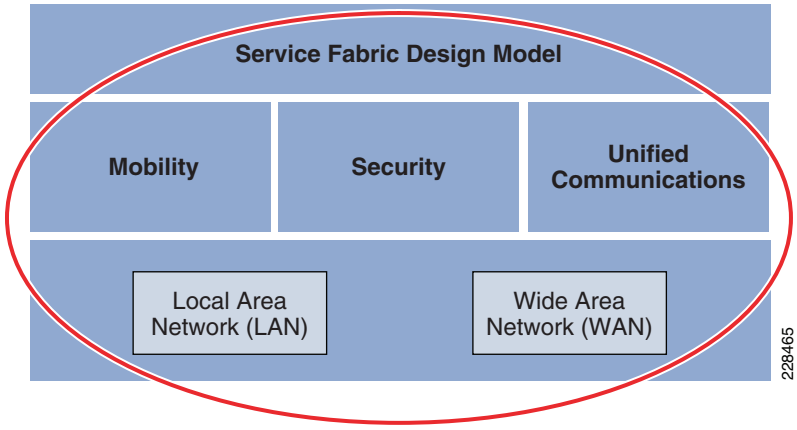
CHAPTER 2

Community College Reference Design—Service Fabric Design Considerations

The service fabric is the foundational network which all Community College services, applications, and solutions use to interact and communicate with one another. Service fabric is the most important component of the Community College reference design. If it fails, all applications, solutions, and technologies employed in the Community College reference design will also fail. Like the foundation of a house, the service fabric must be constructed in a fashion that supports all the applications and services that will ride on it. Additionally, it must be aware of what is type of traffic is transversing and treat each application or service with the right priority based on the needs and importance of that application.

The service fabric is made up of four distinct components local and wide area network (LAN/WAN), security, mobility, and unified communications. Each of these critical foundation components must be carefully designed and tuned to allow for a secure environment that provides business continuity, service awareness and differentiation, as well as access flexibility. See Figure 2-1.

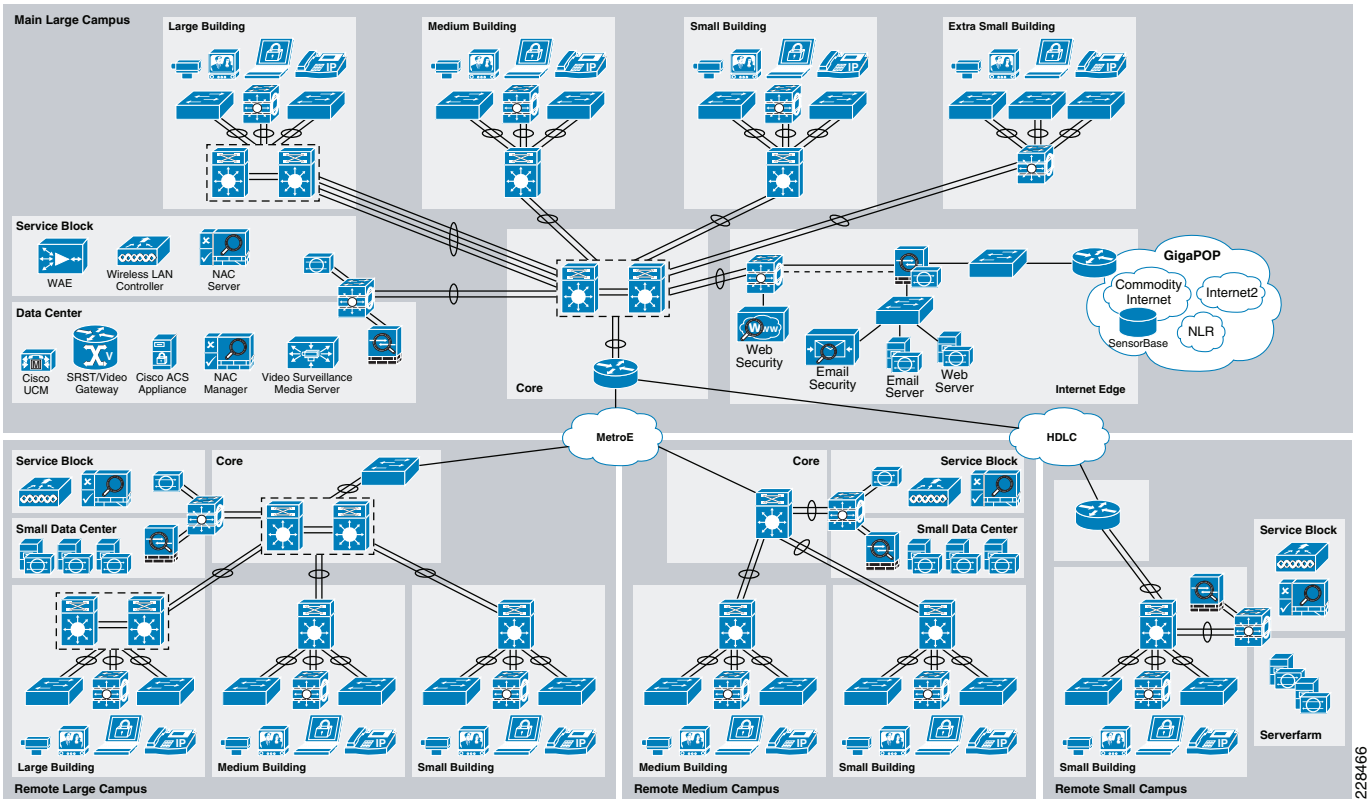
Figure 2-1 Service Fabric Foundation Network



Service Fabric Design Model

The model used for the Community College reference design service fabric is based around the desire to represent as many community college environments as possible. To do that a modular design is used, represented by campuses and buildings of varying sizes (see Figure 2-2). The campuses are made up of one or more building, depending on the campus size profile; buildings are also sized with the determining factor being the number of users or connections to the network in that building as well as physical size. When representing a classroom, an average size of 35 students per classroom or lab is used. Additionally, it is expected that half of all network can be accessed via wireless. This approach allows the network architect to essentially build their own community college environment by mixing the different campus and building profiles provided.

Figure 2-2 Community College Reference Design Overview



Main and Large Campus Design

The main and large campus designs are meant to represent significantly sized campuses containing the largest student, faculty, and staff populations. The profile of the main/large campus is made up of six buildings, the buildings range in size from large to extra small. The buildings will connect back to the resilient core via multiple 10Gb Ethernet links. The core will also connect to a data center design and service block. The large campus will connect to the main campus via a 1Gb Metro Ethernet link. The main campus and large campus are almost identical, with the exception that the main campus is

connected to outside entities such as the Internet, Internet2 (I2), regional networks, and the National Lambda Rail using the Internet edge components, and will also have all other campuses within its community college system connecting to it.

Medium Campus Design

The medium campus design is targeted at community colleges campuses that have approximately 3 buildings ranging in size from medium to small. The buildings will connect to the medium campus core via multiple 10Gb links, and the core will also connect to a small data center and service block. The medium campus is connected to the main campus via a 100mb Metro Ethernet link. This link interconnects the medium campus to the other campuses as well as external networks such as the Internet and I2.

Small Campus Design

The small campus profile represents a campus made up of just one building; in this case, the core and distribution networks are collapsed into one. The small campus is connected to the main campus via a fractional DS3 with a 20mb bandwidth rating. This link interconnects the small campus to the other campuses as well as external networks such as the Internet and I2.

Building Profiles

There are four building profiles: large, medium, small, and extra small. All buildings have access switches that connect users. The buildings also have distribution switches that connect the access switches together as well as connect the building itself to the core network.

Large Building Design

The large building is designed for 1600 Ethernet access ports ranging in bandwidth from 100mb to 1Gb. The ports are distributed over four different floors, each floor having 400 access ports. There are 80 wireless access points using the IEEE 802.1 ABGN standards, there are 20 access points per floor; additionally, there are 6 outdoor mesh access points to cover the outdoor skirt of the building. The large building is made up of 80 classrooms, 30 professor offices, 10 administrative offices, and 40 college professionals collectively this represents 160 phones for the large building.

Medium Building Design

The medium building was designed for 800 Ethernet access ports ranging in bandwidth from 100mb to 1Gb. The ports are distributed over two different floors, each floor having 400 access ports. There are 40 wireless access points using the IEEE 802.11 ABGN standards, there are 20 access points per floor; additionally, there are four outdoor mesh access points to cover the outdoor skirt of the building. The medium building is made up of 40 classrooms, 15 professor offices, 5 administrative offices, and 20 college professionals collectively this represents 80 phones for the medium building.

Small Building Design

The small building is designed for 200 Ethernet access ports ranging in bandwidth from 100mb to 1Gb. The ports are all located on one floor. There are 10 wireless access points using the IEEE 802.1 ABGN standards; additionally, there are 2 outdoor mesh access points to cover the outdoor skirt of the building. The small building is made up of 10 classrooms, 8 professor offices, 2 administrative offices, and 10 college professionals collectively this represents 30 phones for the small building.

Extra Small Building Design

The extra small building is designed for 48 100mb Ethernet access ports. The ports are all located on one floor. There are 3 wireless access points using the IEEE 802.1 ABGN standards; additionally, there is 1 outdoor mesh access point to cover the outdoor skirt of the building. The extra small building is made up of 3 classrooms and 7 other phones, totaling 10 phones for the extra small building.

Access Devices

The devices that connect to the Cisco Community College reference design network include phones, cameras, displays, laptops, desktops, mobile phones, and personal devices (iPod, MP3, etc). Half of all the devices are expected to connect to the network using 802.11 ABGN wireless access.

The service fabric consists of four major components. The sections below provide a brief description of each of these components.

LAN/WAN Design Considerations

The service fabric LAN/WAN is made up of routers and switches deployed in a three-tier hierarchical model that use Cisco IOS to provide foundational network technologies needed to provide a highly available, application-aware network with flexible access.

LAN Design Considerations

Hierarchical network design model components:

- *Core layer*—The campus backbone consisting of a Layer-3 core network interconnecting to several distributed networks and the shared services block to access local and global information.
- *Distribution layer*—The distribution layer uses a combination of Layer-2 and Layer-3 switching to provide for the appropriate balance of policy and access controls, availability, and flexibility in subnet allocation and VLAN usage.
- *Access layer*—Demarcation point between network infrastructure and access devices. Designed for critical network edge functionality to provide intelligent application and device aware services.

Routing Protocol Selection Criteria

Routing protocols are essential for any network, because they allow for the routing of information between buildings and campuses. Selecting the right routing protocol can vary based on the end-to-end network infrastructure. The service fabric routers and switches support many different routing protocols that will work for community college environments. Network architects must consider all the following critical design factors when selecting the right routing protocol to be implemented throughout the internal network:

- *Network design*—Proven protocol that can scale in full-mesh campus network designs and can optimally function in hub-and-spoke WAN network topologies.
- *Scalability*—Routing protocol function must be network and system efficient that operates with a minimal number of updates, recomputation independent of number of routes in the network.
- *Rapid convergence*—Link state versus DUAL recomputation and synchronization. Network reconvergence also varies based on network design, configuration, and a multitude of other factors which are beyond the routing protocol.
- *Operational considerations*—Simplified network and routing protocol design that can ease the complexities of configuration, management, and troubleshooting.

High Availability Design Considerations

To ensure business continuity and prevent catastrophic network failure during unplanned network outage, it is important to identify network fault domains and define rapid recovery plans to minimize the application impact during minor and major network outages.

The service fabric design must ensures network survivability by following three major resiliency methods pertaining to most types of failures. Depending on the network system tier, role, and network service type the appropriate resiliency option should be deployed:

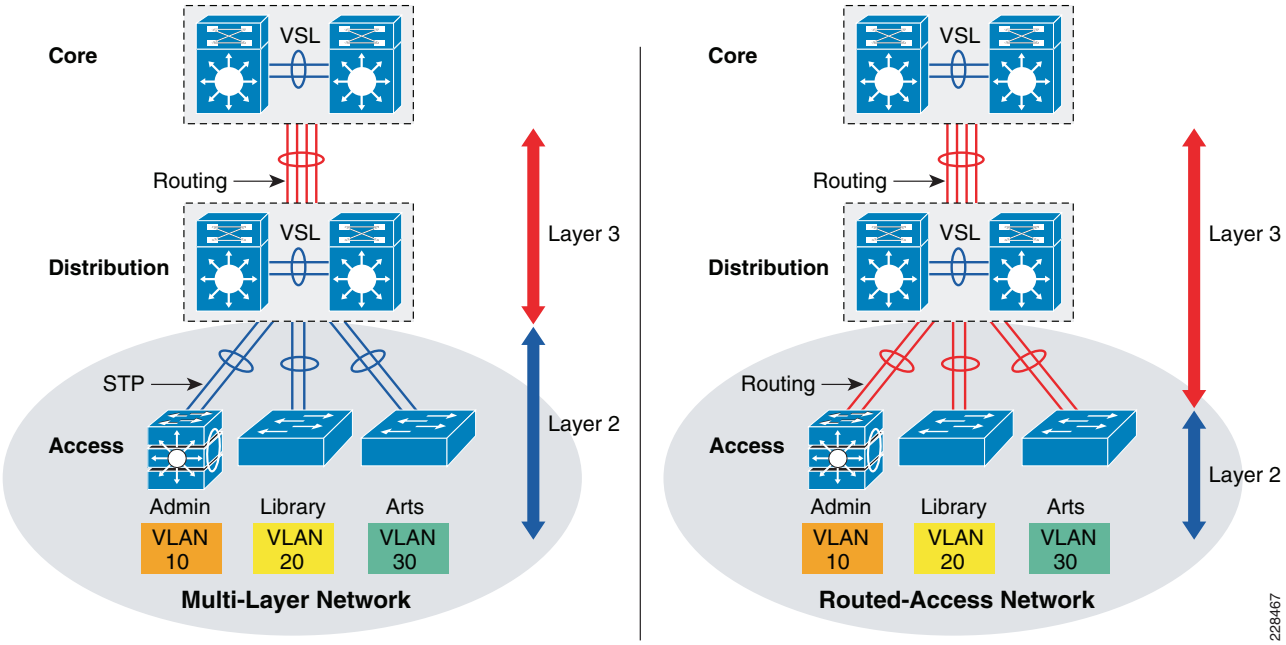
- *Link resiliency*—Provides redundancy during physical link failures (i.e., fiber cut, bad transceivers, incorrect cablings, etc.)
- *Device resiliency*—Protects network during abnormal node failure triggered by hardware or software (i.e., software crashes, non-responsive supervisor etc.)
- *Operational resiliency*—Enables higher level resiliency capabilities, providing complete network availability even during planned network outage conditions.

Access Layer Design Considerations

The access layer represents the entry into the network, consisting of wired and wireless access from the client to the network. The switch that the client connects to will ultimately connect up to the network distribution, and the layer of communication used here must be considered in any design. Traditional Layer 2 connectivity is prevalent in most networks today; however, it comes at some cost in administration, configuration, and timely resiliency. The emerging method of connectivity is a Layer 3 connection, commonly referred to as *routed-access*.

Performing the routing function in the access-layer simplifies configuration, optimizes distribution performances, and allows for the use of well known end-to-end troubleshooting tools. Implementing a Layer 3 access-layer in lieu of the traditional Layer 2 access replaces the required Layer 2 trunks with a single point-to-point Layer 3 link. Pushing Layer 3 function one tier down on Layer 3 access switches changes traditional multilayer network topology and the forwarding path. The implementing of a Layer 3 access does not require any physical or logical link reconfiguration or changes. See Figure 2-2.

Figure 2-3 Control Function in Multi-Layer and Routed-Access Network Design



At the network edge, Layer 3 access switches provides an IP gateway function and becomes a Layer-2 demarcation point to locally connected endpoints that could be logically segmented in multiple VLANs.

LAN Service Fabric Foundational Services

The service fabric uses essential foundational services to efficiently disseminate information that are used by multiple clients, as well as identify and prioritize different applications traffic based on their requirements. Designing the foundational services in a manner consistent with the needs of the community college system is paramount. Some of the key foundational services discussed include the following:

- Multicast routing protocol design considerations
- Designing QoS in campus network

WAN Design Considerations

WAN Transport

In order for campuses to communicate with one another and/or to communicate outside the community college system, network traffic must traverse over a WAN. WAN transport differs greatly from LAN transport due to the variables such as the type of connection used, the speed of the connection, and the distance of the connection. The service fabric design model covers the following WAN transport design considerations:

- MPLS/VPN
- Internet

- Metro Ethernet

WAN Service Fabric Foundational Services

Similar to the LAN, the WAN must deploy essential foundational services to ensure the proper transport and prioritization of community college services, the WAN Service Fabric Foundation Services considered are as follows:

- Routing protocol design
- Quality-of-service (QoS)
- WAN resiliency
- Multicast

Security Design Considerations

Security of the Community College reference design service fabric is essential. Without it, community college solutions, applications, and services are open to be compromised, manipulated, or shut down. The service fabric was developed with the following security design considerations:

- *Network Foundation Protection (NFP)*—Ensuring the availability and integrity of the network infrastructure, protecting the control and management planes.
- *Internet perimeter protection*— Ensuring safe connectivity to the Internet, Internet2 and National LambdaRail (NLR) networks and protecting internal resources and users from malware, viruses, and other malicious software. Protecting students, staff and faculty from harmful content. Enforcing E-mail and web browsing policies.
- *Data center protection*—Ensuring the availability and integrity of centralized applications and systems. Protecting the confidentiality and privacy of student, staff and faculty records.
- *Network access security and control*—Securing the access edges. Enforcing authentication and role-based access for students, staff and faculty residing at the main and remote campuses. Ensuring systems are up-to-date and in compliance with the CCVE institution's network security policies.
- *Network endpoint protection*—Protecting servers and school-controlled systems (computer labs, school-provided laptops, etc.) from viruses, malware, botnets, and other malicious software. Enforcing E-mail and web browsing policies for staff and faculty.

Each of these security design considerations are discussed in further detail in Chapter 6, "Community College Security Design Considerations."

Mobility

Mobility is an essential part of the community college environment. Most students will connect wirelessly to campus networks. Additionally, other devices will also rely on the mobile network. In designing the mobility portion of the service fabric, the following design criteria were used:

- *Accessibility*—Enables students, staff and guests to be accessible and productive, regardless of whether they are meeting in a study hall, at lunch with colleagues in the campus cafeteria, or simply enjoying a breath of fresh air outside a campus building. Provide easy, secure guest access to college guests such as alumni, prospective students, contractors, vendors and other visitors.

- *Usability*—In addition to extremely high WLAN transmission speeds made possible by the current generation of IEEE 802.11n technology, latency sensitive applications (such as IP telephony and video-conferencing) are supported over the WLAN using appropriately applied QoS. This gives preferential treatment to real-time traffic, helping to ensure that video and audio information arrives on time.
- *Security*—Segment authorized users and block unauthorized users. Extend the services of the network safely to authorized parties. Enforce security policy compliance on all devices seeking to access network computing resources. Faculty and other staff enjoy rapid and reliable authentication through IEEE 802.1x and Extensible Authentication Protocol (EAP), with all information sent and received on the WLAN being encrypted.
- *Manageability*—College network administrators must be able to easily deploy, operate, and manage hundreds of access points within multiple community college campus deployments. A single, easy to understand WLAN management framework is desired to provide small, medium and large community college systems with the same level of wireless LAN management scalability, reliability and ease of deployment that is demanded by traditional enterprise business customers.
- *Reliability*—Provide adequate capability to recover from a single-layer fault of a WLAN accessibility component or controller wired link. Ensure that wireless LAN accessibility is maintained for students, faculty, staff and visitors in the event of common failures.

Unified Communications

Call Processing Considerations

How calls are processed in the community college environment is an important design consideration, guidance on designing scalable and resilient call processing systems is essential for deploying a unified communications system. Some of the considerations include the following:

- *Scale*—The number of users, locations, gateways, applications, and so forth
- *Performance*—The call rate
- *Resilience*—The amount of redundancy

Gateway Design Considerations

Gateways provide a number of methods for connecting an IP telephony network to the Public Switched Telephone Network (PSTN). Several considerations for gateways include the following:

- PSTN trunk sizing
- Traffic patterns
- Interoperability with the call processing system

Dial Plan Considerations

The dial plan is one of the key elements of an unified communications system, and an integral part of all call processing agents. Generally, the dial plan is responsible for instructing the call processing agent on how to route calls. Specifically, the dial plan performs the following main functions:

- Endpoint addressing
- Path selection
- Calling privileges
- Digit manipulation
- Call coverage

Survivability Considerations

Voice communications are a critical service that must be maintained in the event of a network outage for this reason the service fabric must take survivability into consideration. Chapter 7, "Community College Unified Communications Design Considerations," describes how the service fabric design is equipped and designed to keep voice communications active in the event of an outage.

CHAPTER 3

Community College LAN Design Considerations

LAN Design

The community college LAN design is a multi-campus design, where a campus consists of multiple buildings and services at each location, as shown in Figure 3-1.

Figure 3-1 Community College LAN Design

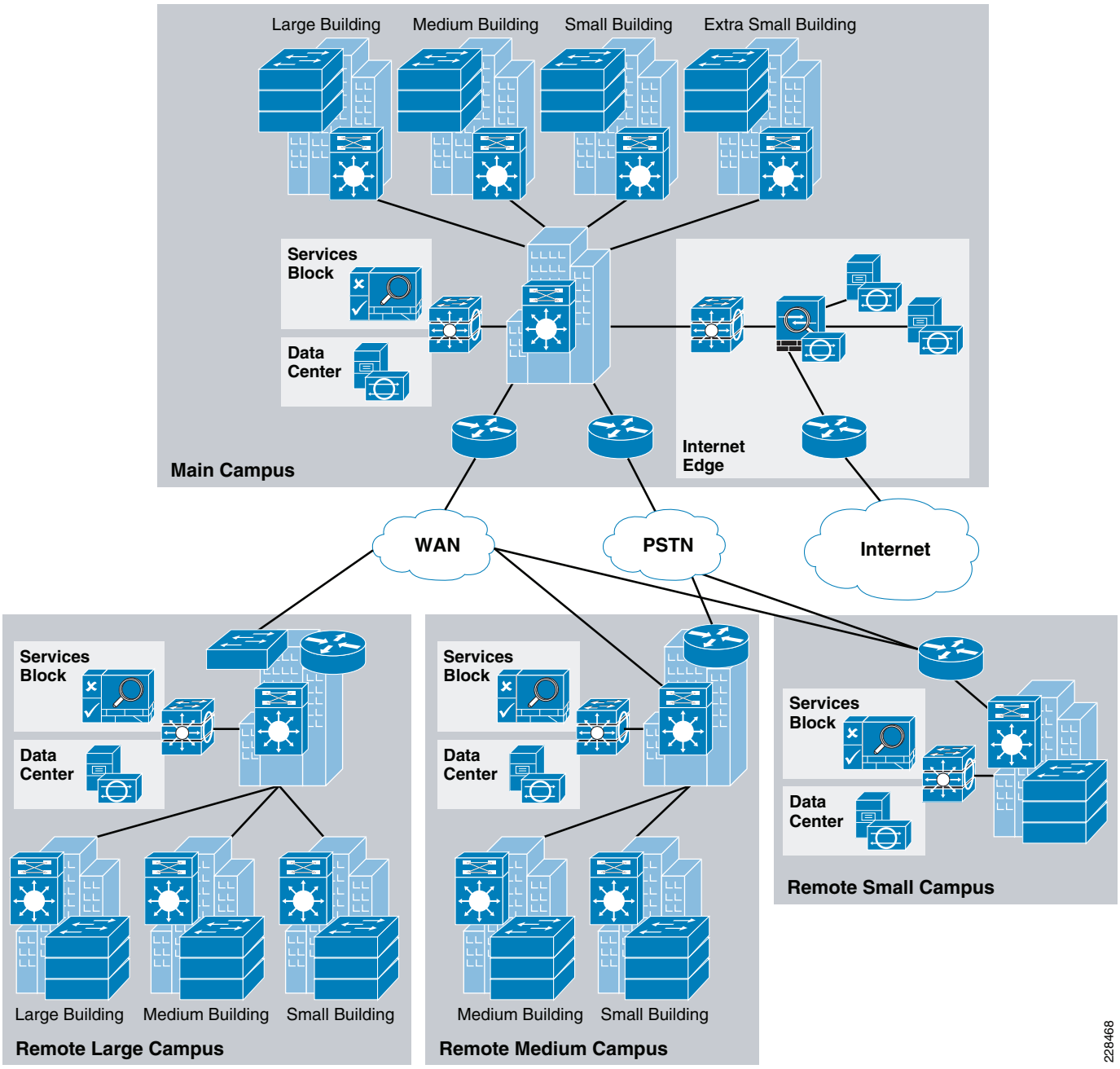
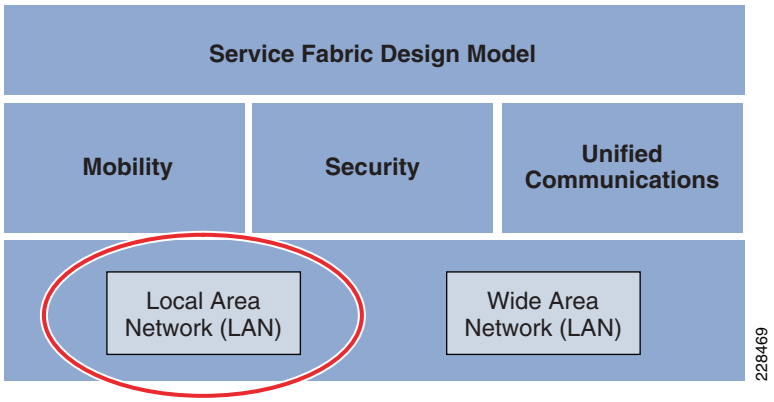


Figure 3-2 shows the service fabric design model used in the community college LAN design.

Figure 3-2 Community College LAN Design



This chapter focuses on the LAN component of the overall design. The LAN component consists of the LAN framework and network foundation technologies that provide baseline routing and switching guidelines. The LAN design interconnects several other components, such as endpoints, data center, WAN, and so on, to provide a foundation on which mobility, security, and unified communications (UC) can be integrated into the overall design.

This LAN design provides guidance on building the next-generation community college network, which becomes a common framework along with critical network technologies to deliver the foundation for the service fabric design. This chapter is divided into following sections:

- *LAN design principles*—Provides proven design choices to build various types of LANs.
- *LAN design model for the community college*—Leverages the design principles of the tiered network design to facilitate a geographically dispersed college campus network made up of various elements, including networking role, size, capacity, and infrastructure demands.
- *Considerations of a multi-tier LAN design model for community colleges*—Provides guidance for the college campus LAN network as a platform with a wide range of next-generation products and technologies to integrate applications and solutions seamlessly.
- *Designing network foundation services for LAN designs in community colleges*—Provides guidance on deploying various types of Cisco IOS technologies to build a simplified and highly available network design to provide continuous network operation. This section also provides guidance on designing network-differentiated services that can be used to customize the allocation of network resources to improve user experience and application performance, and to protect the network against unmanaged devices and applications.

LAN Design Principles

Any successful design or system is based on a foundation of solid design theory and principles. Designing the LAN component of the overall community college LAN service fabric design model is no different than designing any large networking system. The use of a guiding set of fundamental engineering design principles serves to ensure that the LAN design provides for the balance of availability, security, flexibility, and manageability required to meet current and future college and technology needs. This chapter provides design guidelines that are built upon the following principles to allow a community college network architect to build college campuses that are located in different geographical locations:

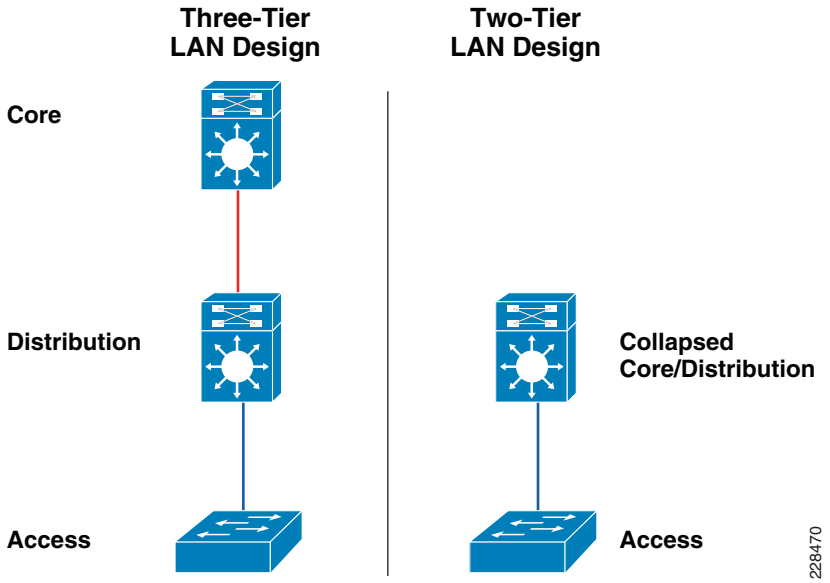
- *Hierarchical*

  - Facilitates understanding the role of each device at every tier
  - Simplifies deployment, operation, and management
  - Reduces fault domains at every tier
- *Modularity*—Allows the network to grow on an on-demand basis
- *Resiliency*—Satisfies user expectations for keeping network always on
- *Flexibility*—Allows intelligent traffic load sharing by using all network resources

These are not independent principles. The successful design and implementation of a college campus network requires an understanding of how each of these principles applies to the overall design. In addition, understanding how each principle fits in the context of the others is critical in delivering a hierarchical, modular, resilient, and flexible network required by community colleges today.

Designing the community college LAN building blocks in a hierarchical fashion creates a flexible and resilient network foundation that allows network architects to overlay the security, mobility, and UC features essential to the service fabric design model, as well as providing an interconnect point for the WAN aspect of the network. The two proven, time-tested hierarchical design frameworks for LAN networks are the three-tier layer and the two-tier layer models, as shown in Figure 3-3.

Figure 3-3 Three-Tier and Two-Tier LAN Design Models



The key layers are access, distribution and core. Each layer can be seen as a well-defined structured module with specific roles and functions in the LAN network. Introducing modularity in the LAN hierarchical design further ensures that the LAN network remains resilient and flexible to provide critical network services as well as to allow for growth and changes that may occur in a community college.

- *Access layer*

  The access layer represents the network edge, where traffic enters or exits the campus network. Traditionally, the primary function of an access layer switch is to provide network access to the user. Access layer switches connect to the distribution layer switches to perform network foundation technologies such as routing, quality of service (QoS), and security.

To meet network application and end-user demands, the next-generation Cisco Catalyst switching platforms no longer simply switch packets, but now provide intelligent services to various types of endpoints at the network edge. Building intelligence into access layer switches allows them to operate more efficiently, optimally, and securely.

- *Distribution layer*

  The distribution layer interfaces between the access layer and the core layer to provide many key functions, such as the following:

  - Aggregating and terminating Layer 2 broadcast domains
  - Aggregating Layer 3 routing boundaries
  - Providing intelligent switching, routing, and network access policy functions to access the rest of the network
  - Providing high availability through redundant distribution layer switches to the end-user and equal cost paths to the core, as well as providing differentiated services to various classes of service applications at the edge of network

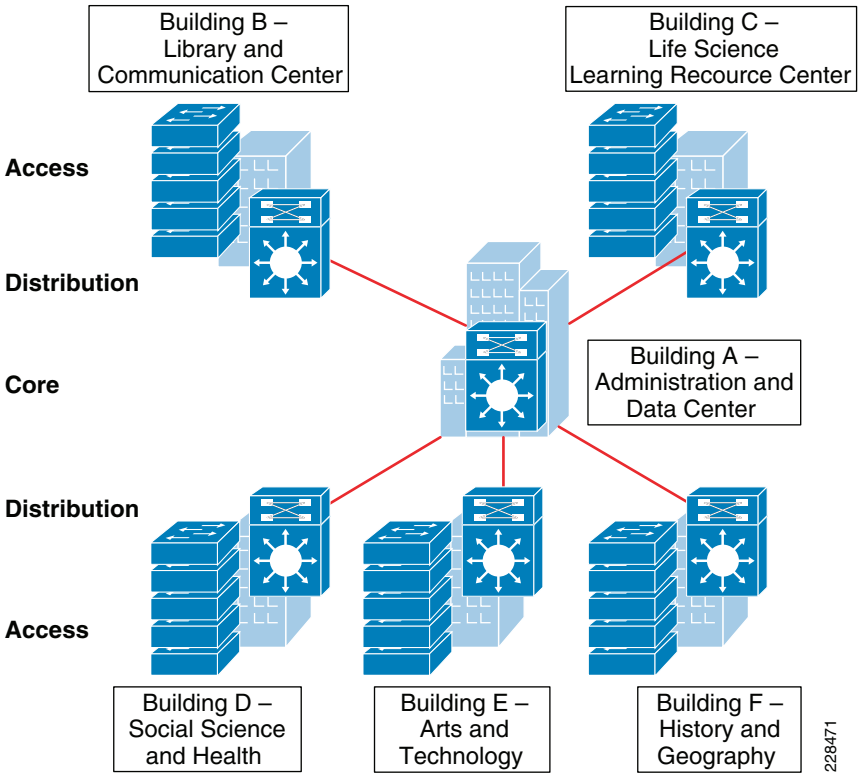
- *Core layer*

  The core layer is the network backbone that connects all the layers of the LAN design, providing for connectivity between end devices, computing and data storage services located within the data center and other areas, and services within the network. The core layer serves as the aggregator for all the other campus blocks, and ties the campus together with the rest of the network.

Note For more information on each of these layers, see the enterprise class network framework at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html.

Figure 3-4 shows a sample three-tier LAN network design for community colleges where the access, distribution, and core are all separate layers. To build a simplified, cost-effective, and efficient physical cable layout design, Cisco recommends building an extended-star physical network topology from a centralized building location to all other buildings on the same campus.

Figure 3-4 Three-Tier LAN Network Design Example



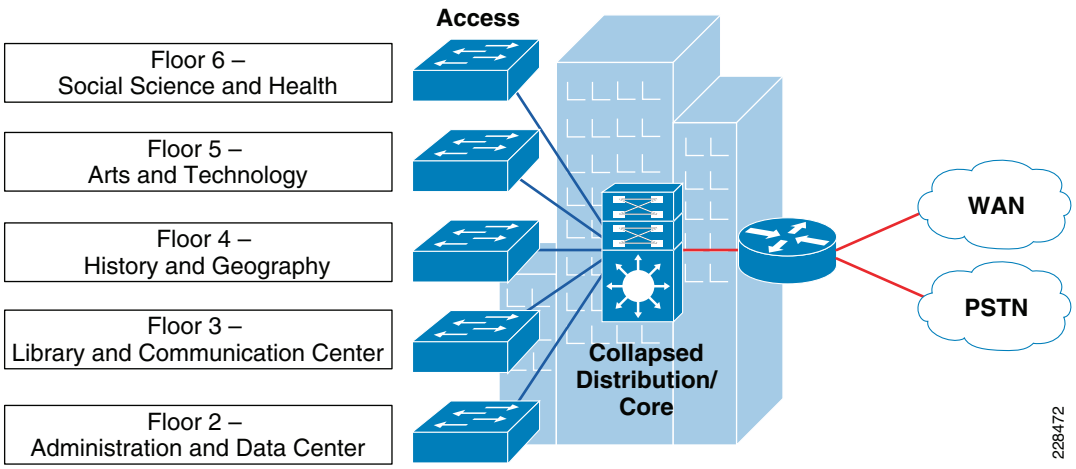
Collapsed Core Campus Network Design

The primary purpose of the core layer is to provide fault isolation and backbone connectivity. Isolating the distribution and core into separate layers creates a clean delineation for change control between activities affecting end stations (laptops, phones, and printers) and those that affect the data center, WAN, or other parts of the network. A core layer also provides for flexibility in adapting the campus design to meet physical cabling and geographical challenges. If necessary, a separate core layer can use a different transport technology, routing protocols, or switching hardware than the rest of the campus, providing for more flexible design options when needed.

In some cases, because of either physical or network scalability, having separate distribution and core layers is not required. In smaller locations where there are less users accessing the network or in college campus sites consisting of a single building, separate core and distribution layers are not needed. In this scenario, Cisco recommends the two-tier LAN network design, also known as the collapsed core network design.

Figure 3-5 shows a two-tier LAN network design example for a community college LAN where the distribution and core layers are collapsed into a single layer.

Figure 3-5 Two-Tier Network Design Example



If using the small-scale collapsed campus core design, the college network architect must understand the network and application demands so that this design ensures a hierarchical, modular, resilient, and flexible LAN network.

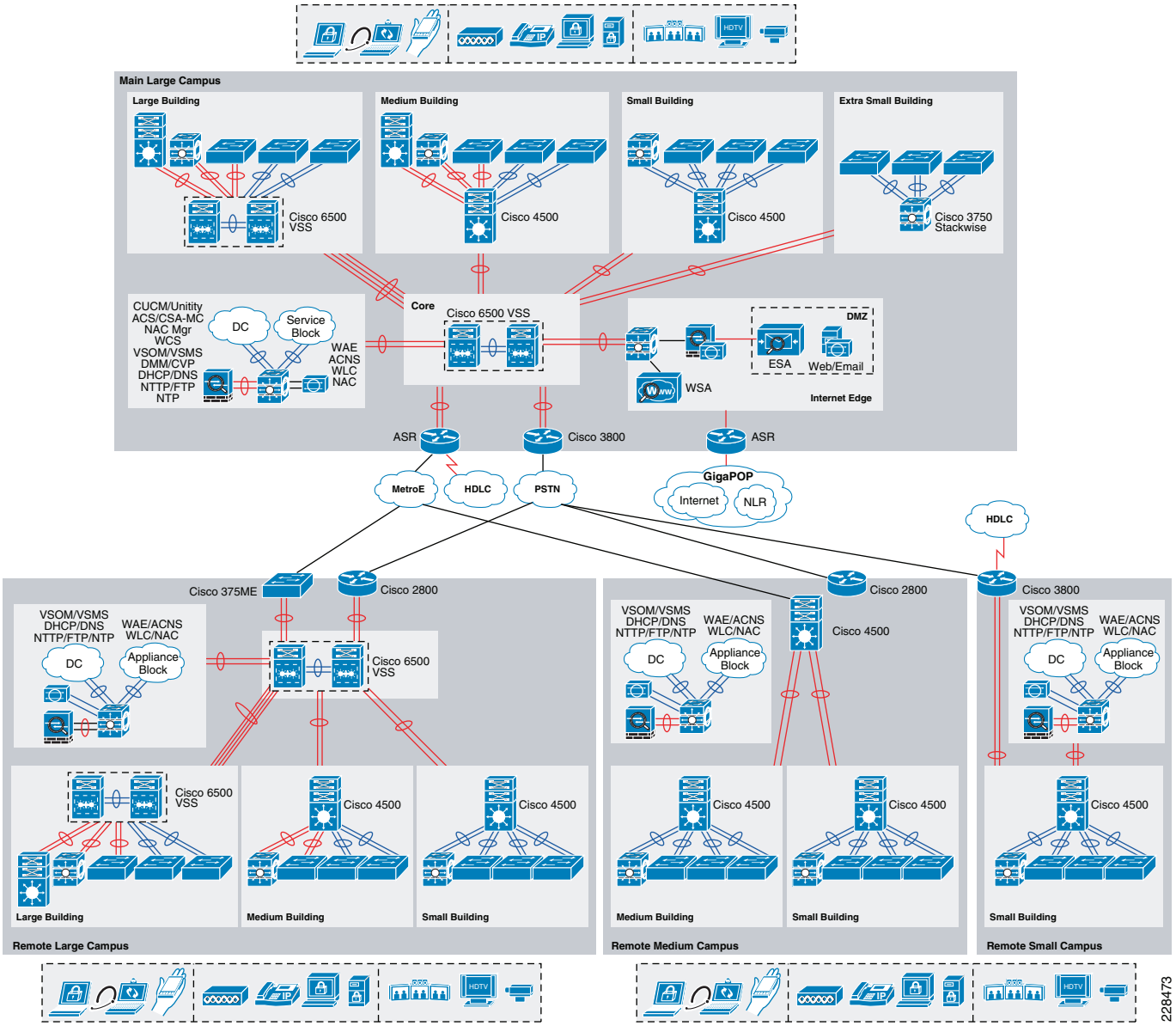
Community College LAN Design Models

Both LAN design models (three-tier and two-tier) have been developed with the following considerations:

- *Scalability*—Based on Cisco enterprise-class high-speed 10G core switching platforms for seamless integration of next-generation applications required for community colleges. Platforms chosen are cost-effective and provide investment protection to upgrade network as demand increases.
- *Simplicity*—Reduced operational and troubleshooting cost via the use of network-wide configuration, operation, and management.
- *Resilient*—Sub-second network recovery during abnormal network failures or even network upgrades.
- *Cost-effectiveness*—Integrated specific network components that fit budgets without compromising performance.

As shown in Figure 3-6, multiple campuses can co-exist within a single community college system that offers various academic programs.

Figure 3-6 Community College LAN Design Model



Depending on the number of available academic programs in a remote campus, the student, faculty, and staff population in remote campuses may be equal to or less than the main college campus site. Campus network designs for the remote campus may require adjusting based on overall college campus capacity.

Using high-speed WAN technology, all the remote community college campuses interconnect to a centralized main college campus that provides shared services to all the students, faculty, and staff, independent of their physical location. The WAN design is discussed in greater detail in the next chapter, but it is worth mentioning in the LAN section because some remote sites may integrate LAN and WAN functionality into a single platform. Collapsing the LAN and WAN functionality into a single Cisco platform can provide all the needed requirements for a particular remote site as well as provide reduced cost to the overall design, as discussed in more detail in the following section.

Table 3-1 shows a summary of the LAN design models as they are applied in the overall community college network design.

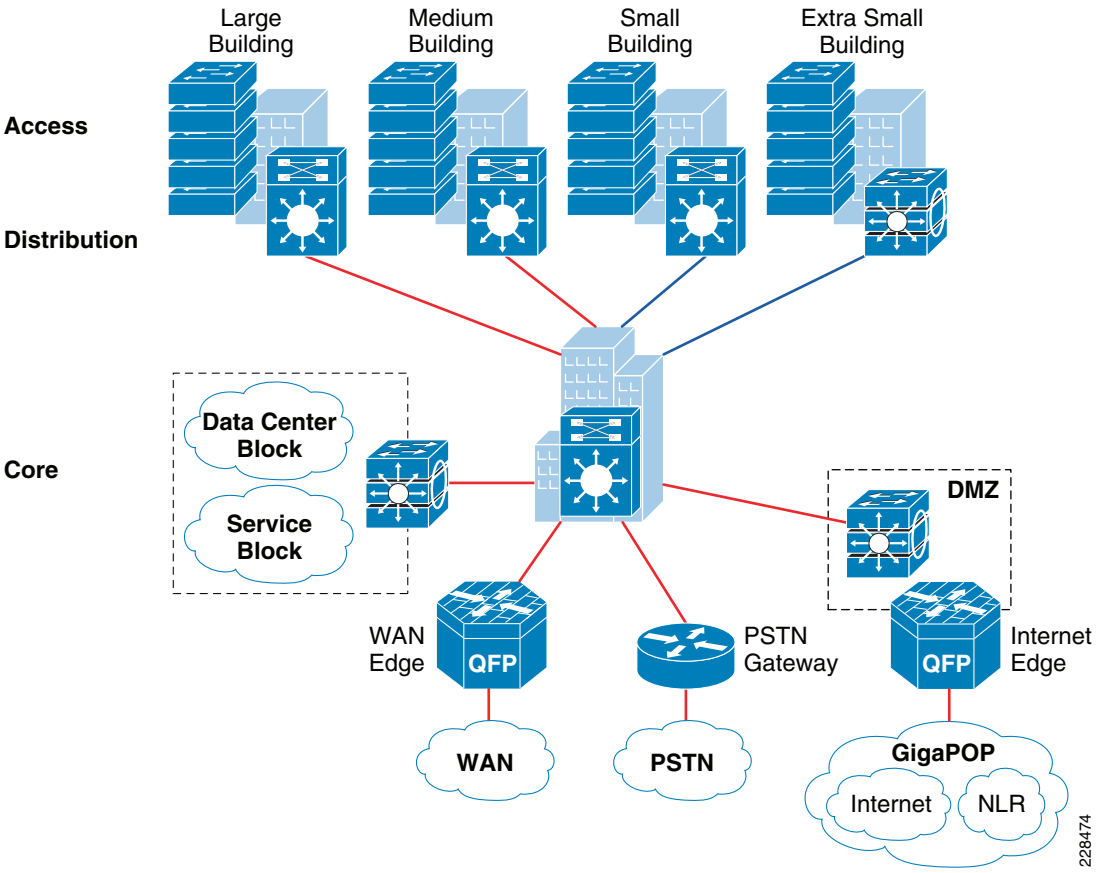
Table 3-1 Community College Recommended LAN Design Model

Community College Location	Recommended LAN Design Model
Main campus	Three-tier
Remote large campus	Three-tier
Remote medium campus	Three-tier with collapsed WAN edge
Remote small campus	Two-tier

Main College Campus Network Design Overview

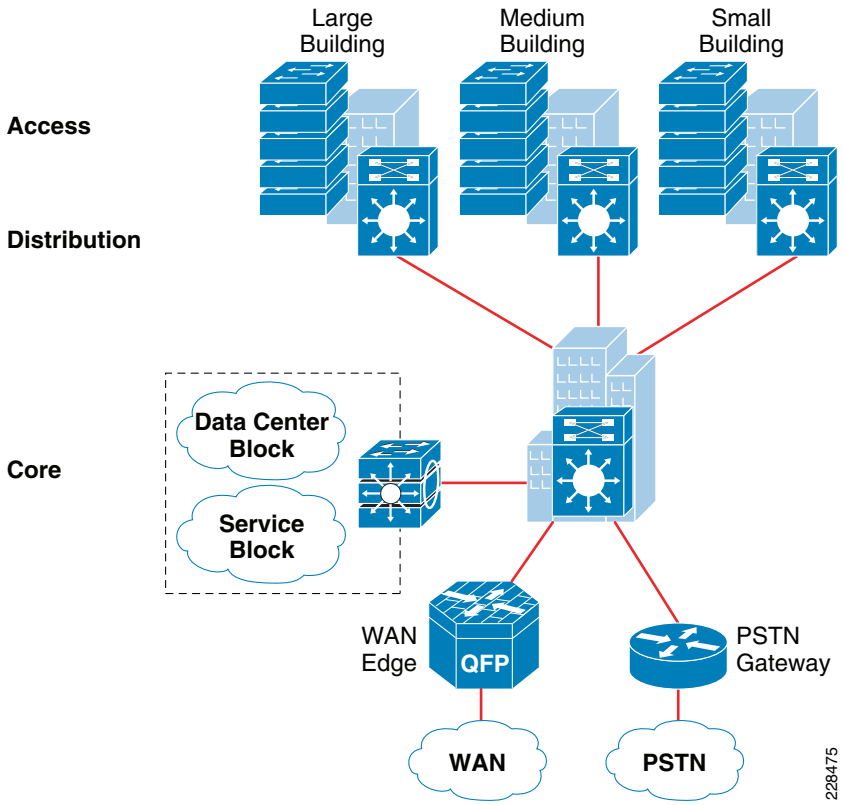
The main college campus in the community college design consists of a centralized hub campus location that interconnects several sizes of remote campuses to provide end-to-end shared network access and services, as shown in Figure 3-7.

Figure 3-7 Main College Campus Site Reference Design



The main college campus typically consists of various sizes of building facilities and various education department groups. The network scale factor in the main college campus site is higher than the remote college campus site, and includes end users, IP-enabled endpoints, servers, and security and network edge devices. Multiple buildings of various sizes exist in one location, as shown in Figure 3-8.

Figure 3-8 Main College Campus Site Reference Design



The three-tier LAN design model for the main college campus meets all key technical aspects to provide a well-structured and strong network foundation. The modularity and flexibility in a three-tier LAN design model allows easier expansion and integration in the main college network, and keeps all network elements protected and available.

To enforce external network access policy for each end user, the three-tier model also provides external gateway services to the students and staff for accessing the Internet as well as private education and research networks.

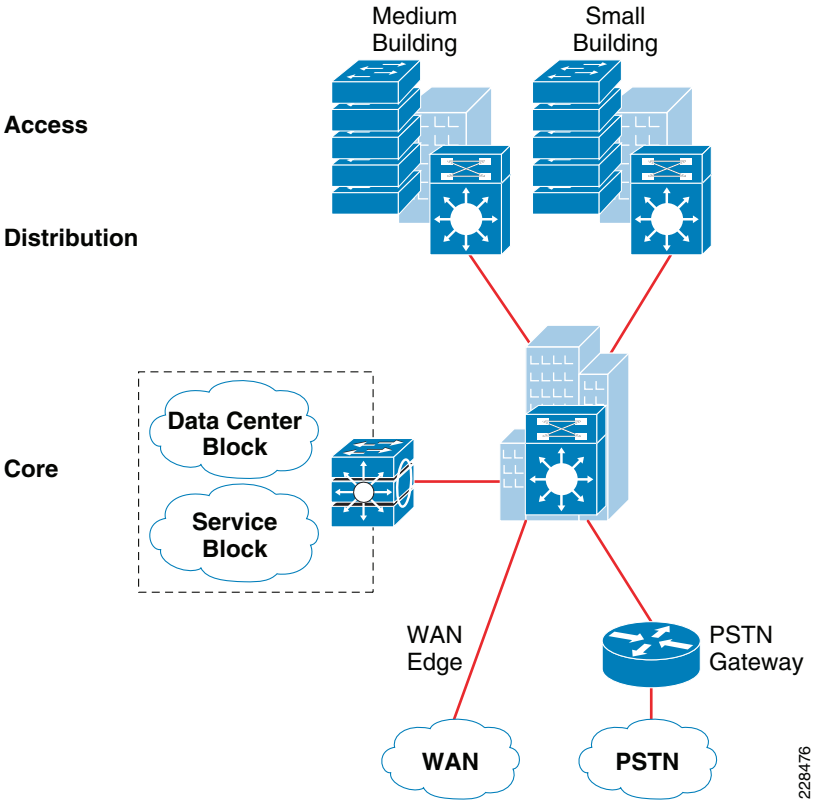
Note The WAN design is a separate element in this location, because it requires a separate WAN device that connects to the three-tier LAN model. WAN design is discussed in more detail in Chapter 4, "Community College WAN Design Considerations."

Remote Large College Campus Site Design Overview

From the location size and network scale perspective, the remote large college is not much different from the main college campus site. Geographically, it can be distant from the main campus site and requires a high-speed WAN circuit to interconnect both campuses. The remote large college can also be considered as an alternate college campus to the main campus site, with the same common types of applications, endpoints, users, and network services. Similar to the main college campus, separate WAN devices are recommended to provide application delivery and access to the main college campus, given the size and number of students at this location.

Similar to the main college campus, Cisco recommends the three-tier LAN design model for the remote large college campus, as shown in Figure 3-9.

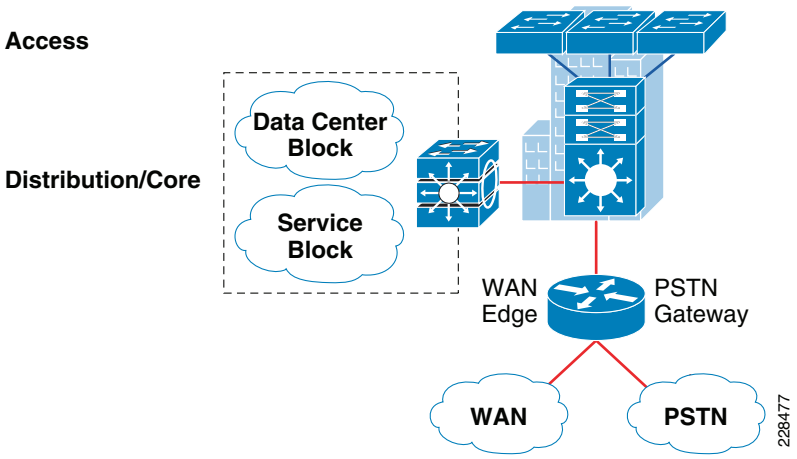
Figure 3-9 Remote Large College Campus Site Reference Design



Remote Medium College Campus Site Design Overview

Remote medium college campus locations differ from a main or remote large campus in that there are less buildings with distributed education departments. A remote medium college campus may have a fewer number of network users and endpoints, thereby reducing the need to build a similar campus network to that recommended for main and large college campuses. Because there are fewer students, faculty, and end users at this site as compared to the main or remote large campus sites, the need for a separate WAN device may not be necessary. A remote medium college campus network is designed similarly to a three-tier large campus LAN design. All the LAN benefits are achieved in a three-tier design model as in the main and remote large campus, and in addition, the platform chosen in the core layer also serves as the WAN edge, thus collapsing the WAN and core LAN functionality into a single platform. Figure 3-10 shows the remote medium campus in more detail.

Figure 3-10 Remote Medium College Campus Site Reference Design



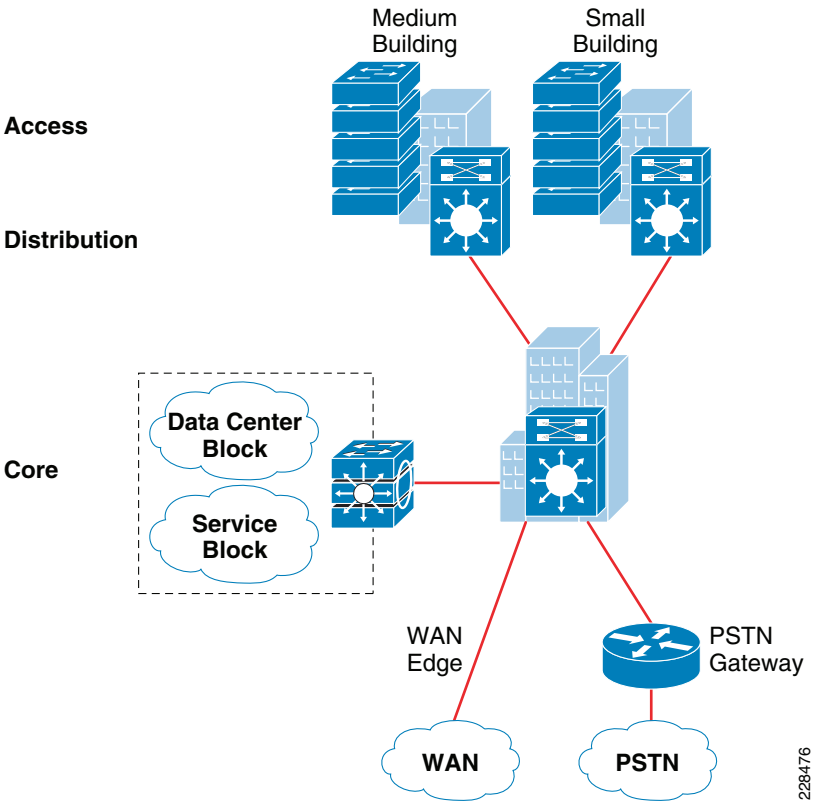
Remote Small College Campus Network Design Overview

The remote small college campus is typically confined to a single building that spans across multiple floors with different academic departments. The network scale factor in this design is reduced compared to other large college campuses. However, the application and services demands are still consistent across the community college locations.

In such smaller scale campus network deployments, the distribution and core layer functions can collapse into the two-tier LAN model without compromising basic network demands. Before deploying a collapsed core and distribution layer in the remote small campus network, considering all the scale and expansion factors prevents physical network re-design, and improves overall network efficiency and manageability.

WAN bandwidth requirements must be assessed appropriately for this remote small campus network design. Although the network scale factor is reduced compared to other larger college campus locations, sufficient WAN link capacity is needed to deliver consistent network services to student, faculty, and staff. Similar to the remote medium campus location, the WAN functionality is also collapsed into the LAN functionality. A single Cisco platform can provide collapsed core and distribution LAN layers. This design model is recommended only in smaller locations, and WAN traffic and application needs must be considered. Figure 3-11 shows the remote small campus in more detail.

Figure 3-11 Remote Small College Campus Site Reference Design



Considering Multi-Tier LAN Design Models for Community Colleges

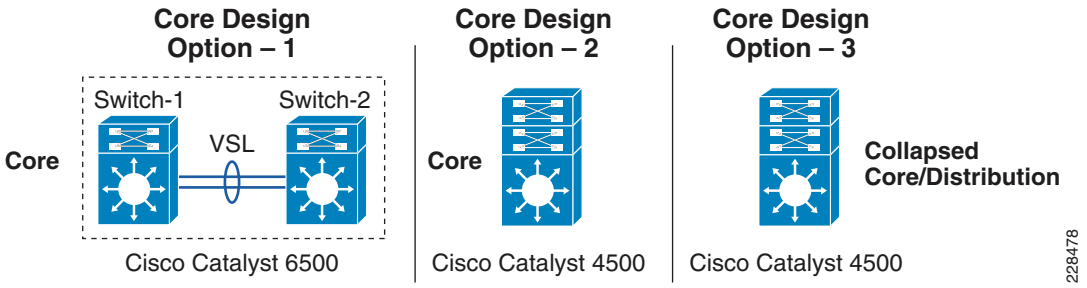
The previous section discussed the recommended LAN design model for each community college location. This section provides more detailed design guidance for each tier in the LAN design model. Each design recommendation is optimized to keep the network simplified and cost-effective without compromising network scalability, security, and resiliency. Each LAN design model for a community college location is based on the key LAN layers of core, distribution, and access.

Campus Core Layer Network Design

As discussed in the previous section, the core layer becomes a high-speed intermediate transit point between distribution blocks in different premises and other devices that interconnect to the data center, WAN, and Internet edge.

Similarly to choosing a LAN design model based on a location within the community college design, choosing a core layer design also depends on the size and location within the design. Three core layer design models are available, each of which is based on either the Cisco Catalyst 6500 Series or the Cisco Catalyst 4500 Series Switches. Figure 3-12 shows the three core layer design models.

Figure 3-12 Core Layer Design Models for Community Colleges



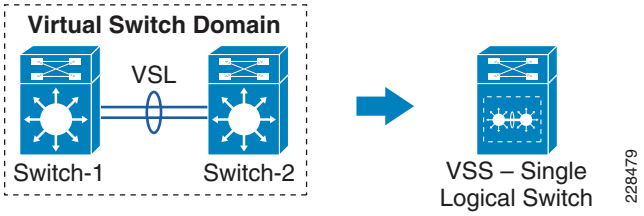
Each design model offers consistent network services, high availability, expansion flexibility, and network scalability. The following sections provide detailed design and deployment guidance for each model as well as where they fit within the various locations of the community college design.

Core Layer Design Option 1—Cisco Catalyst 6500-Based Core Network

Core layer design option 1 is specifically intended for the main and remote large campus locations. It is assumed that the number of network users, high-speed and low-latency applications (such as Cisco TelePresence), and the overall network scale capacity is common in both sites and thus, similar core design principles are required.

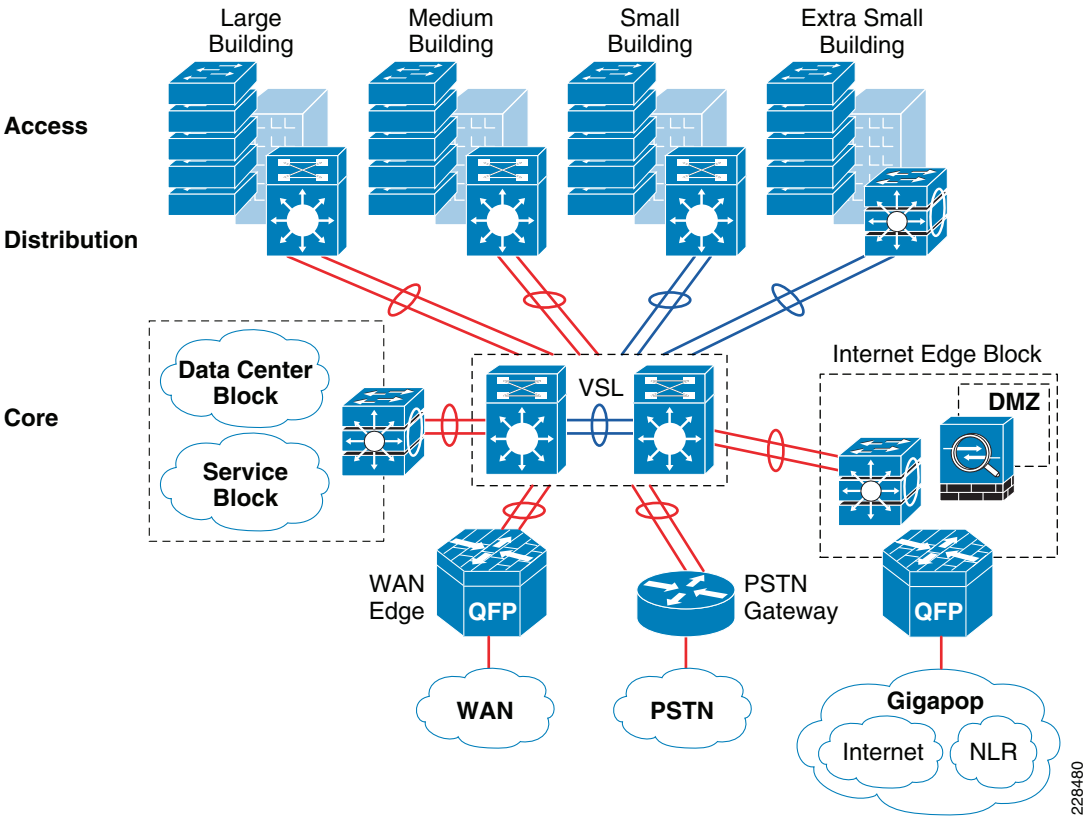
Core layer design option 1 is based on Cisco Catalyst 6500 Series switches using the Cisco Virtual Switching System (VSS), which is a software technology that builds a single logical core system by clustering two redundant core systems in the same tier. Building a VSS-based network changes network design, operation, cost, and management dramatically. Figure 3-13 shows the physical and operational view of VSS.

Figure 3-13 VSS Physical and Operational View



To provide end-to-end network access, the core layer interconnects several other network systems that are implemented in different roles and service blocks. Using VSS to virtualize the core layer into a single logical system remains transparent to each network device that interconnects to the VSS-enabled core. The single logical connection between core and the peer network devices builds a reliable, point-to-point connection that develops a simplified network topology and builds distributed forwarding tables to fully use all resources. Figure 3-14 shows a reference VSS-enabled core network design for the main campus site.

Figure 3-14 VSS-Enabled Core Network Design

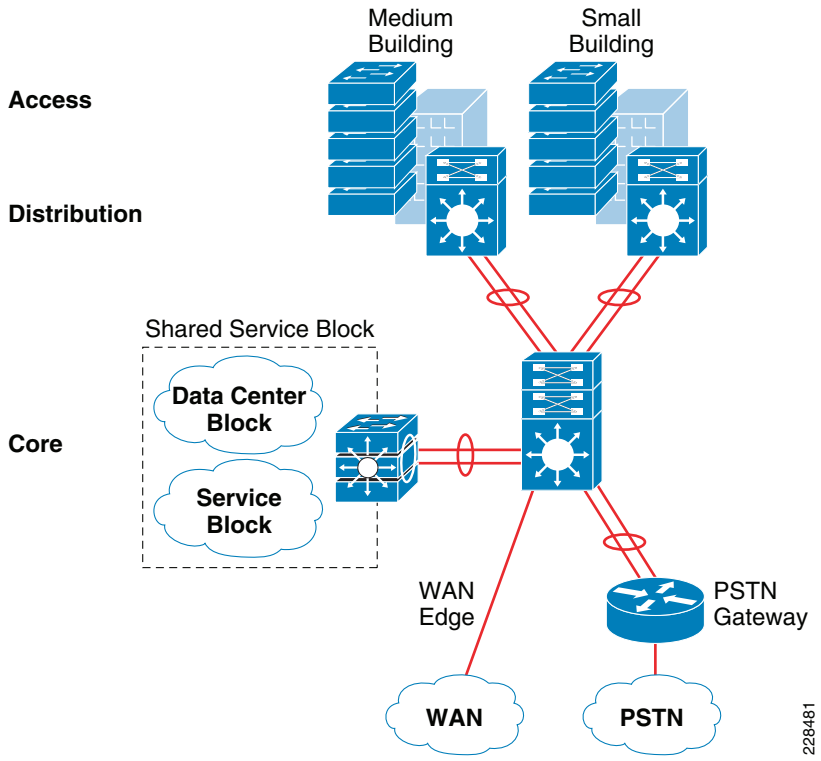


Note For more detailed VSS design guidance, see the *Campus 3.0 Virtual Switching System Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/VSS30dg/campusVSS_DG.html.

Core Layer Design Option 2—Cisco Catalyst 4500-Based Campus Core Network

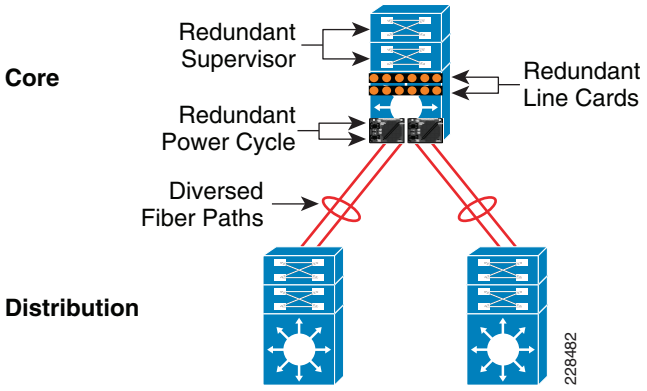
Core layer design option 2 is intended for a remote medium-sized college campus and is built on the same principles as for the main and remote large campus locations. The size of this remote site may not be large, and it is assumed that this location contains distributed building premises within the remote medium campus design. Because this site is smaller in comparison to the main and remote large campus locations, a fully redundant, VSS-based core layer design may not be necessary. Therefore, core layer design option 2 was developed to provide a cost-effective alternative while providing the same functionality as core layer design option 1. Figure 3-15 shows the remote medium campus core design option in more detail.

Figure 3-15 Remote Medium Campus Core Network Design



The cost of implementing and managing redundant systems in each tier may introduce complications in selecting the three-tier model, especially when network scale factor is not too high. This cost-effective core network design provides protection against various types of hardware and software failure and offers sub-second network recovery. Instead of a redundant node in the same tier, a single Cisco Catalyst 4500-E Series Switch can be deployed in the core role and bundled with 1+1 redundant in-chassis network components. The Cisco Catalyst 4500-E Series modular platform is a one-size platform that helps enable the high-speed core backbone to provide uninterrupted network access within a single chassis. Although a fully redundant, two-chassis design using VSS as described in core layer option 1 provides the greatest redundancy for large-scale locations, the redundant supervisors and line cards of the Cisco Catalyst 4500-E provide adequate redundancy for smaller locations within a single platform. Figure 3-16 shows the redundancy of the Cisco Catalyst 4500-E Series in more detail.

Figure 3-16 Highly Redundant Single Core Design Using the Cisco Catalyst 4500-E Platform



This core network design builds a network topology that has similar common design principles to the VSS-based campus core in core layer design option 1. The future expansion from a single core to a dual VSS-based core system becomes easier to deploy, and helps retain the original network topology and the management operation. This cost-effective single resilient core system for a medium-size college network meets the following four key goals:

- *Scalability*—The modular Cisco Catalyst 4500 chassis enables flexibility for core network expansion with high throughput modules and port scalability without compromising network performance.
- *Resiliency*—Because hardware or software failure conditions may create catastrophic results in the network, the single core system must be equipped with redundant system components such as supervisor, line card, and power supplies. Implementing redundant components increases the core network resiliency during various types of failure conditions using Non-Stop Forwarding/Stateful Switch Over (NSF/SSO) and EtherChannel technology.
- *Simplicity*—The core network can be simplified with redundant network modules and diverse fiber connections between the core and other network devices. The Layer 3 network ports must be bundled into a single point-to-point logical EtherChannel to simplify the network, such as the VSS-enabled campus design. An EtherChannel-based campus network offers similar benefits to an Multi-chassis EtherChannel (MEC)- based network.
- *Cost-effectiveness*—A single core system in the core layer helps reduce capital, operational, and management cost for the medium-sized campus network design.

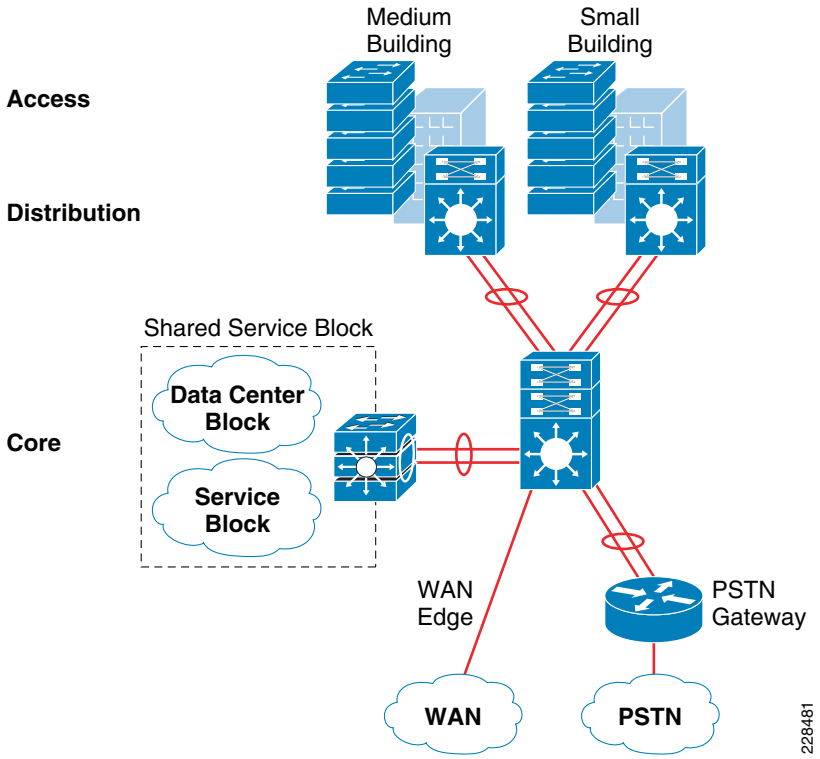
Core Layer Design Option 3—Cisco Catalyst 4500-Based Collapsed Core Campus Network

Core layer design option 3 is intended for the remote small campus network that has consistent network services and applications service-level requirements but at reduced network scale. The remote small campus is considered to be confined within a single multi-story building that may span academic departments across different floors. To provide consistent services and optimal network performance, scalability, resiliency, simplification, and cost-effectiveness in the small campus network design must not be compromised.

As discussed in the previous section, the remote small campus has a two-tier LAN design model, so the role of the core system is merged with the distribution layer. Remote small campus locations have consistent design guidance and best practices defined for main, remote large, and remote medium-sized campus cores. However, for platform selection, the remote medium campus core layer design must be leveraged to build this two-tier campus core.

Single highly resilient Cisco Catalyst 4500 switches with a Cisco Sup6L-E supervisor must be deployed in a centralized collapsed core and distribution role that interconnects to wiring closet switches, a shared service block, and a WAN edge router. The cost-effective supervisor version supports key technologies such as robust QoS, high availability, security, and much more at a lower scale, making it an ideal solution for small-scale network designs. Figure 3-17 shows the remote small campus core design in more detail.

Figure 3-17 Core Layer Option 3 Collapsed Core/Distribution Network Design in Remote Small Campus Location

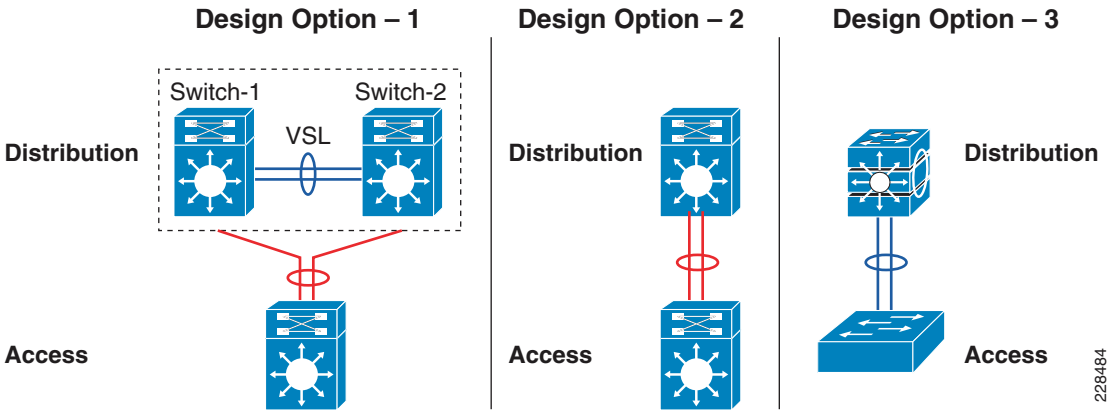


Campus Distribution Layer Network Design

The distribution or aggregation layer is the network demarcation boundary between wiring-closet switches and the campus core network. The framework of the distribution layer system in the community college design is based on best practices that reduce network complexities and accelerate reliability and performance. To build a strong campus network foundation with the three-tier model, the distribution layer has a vital role in consolidating networks and enforcing network edge policies.

Following the core layer design options in different campus locations, the distribution layer design provides consistent network operation and configuration tools to enable various network services. Three simplified distribution layer design options can be deployed in main or remote college campus locations, depending on network scale, application demands, and cost, as shown in Figure 3-18. Each design model offers consistent network services, high availability, expansion flexibility, and network scalability.

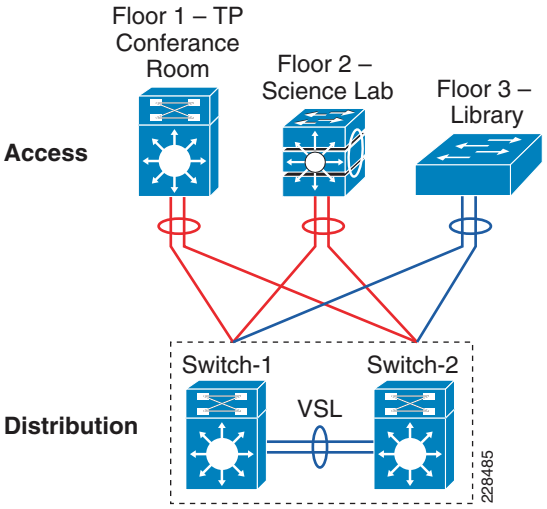
Figure 3-18 Distribution Layer Design Model Options



Distribution Layer Design Option 1—Cisco Catalyst 6500-E Based Distribution Network

Distribution layer design option 1 is intended for main campus and remote large campus locations, and is based on Cisco Catalyst 6500 Series switches using the Cisco VSS, as shown in Figure 3-19.

Figure 3-19 VSS-Enabled Distribution Layer Network Design



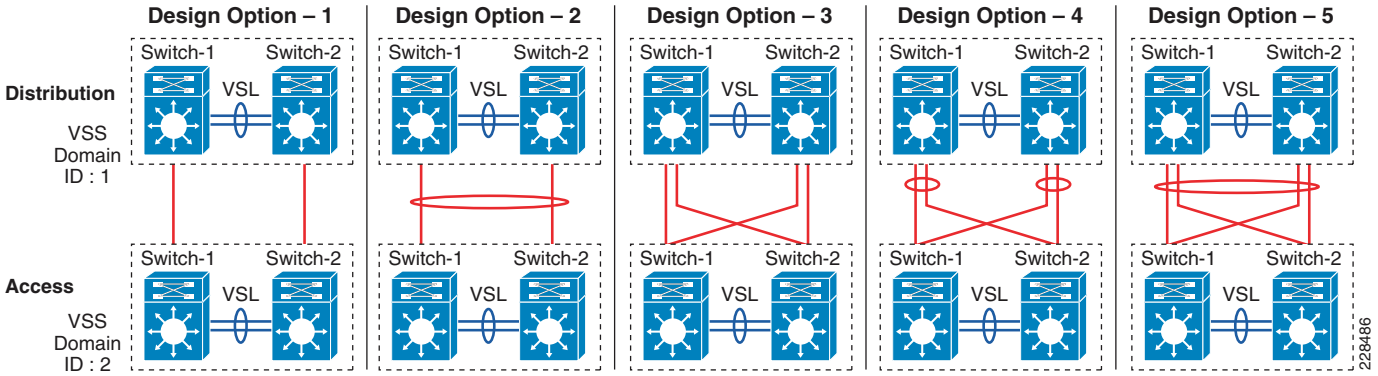
The distribution block and core network operation changes significantly when redundant Cisco Catalyst 6500-E Series switches are deployed in VSS mode in both the distribution and core layers. Clustering redundant distribution switches into a single logical system with VSS introduces the following technical benefits:

- A single logical system reduces operational, maintenance, and ownership cost.
- A single logical IP gateway develops a unified point-to-point network topology in the distribution block, which eliminates traditional protocol limitations and enables the network to operate at full capacity.
- Implementing the distribution layer in VSS mode eliminates or reduces several deployment barriers, such as spanning-tree loop, Hot Standby Routing Protocol (HSRP)/Gateway Load Balancing Protocol (GLBP)/Virtual Router Redundancy Protocol (VRRP), and control plane overhead.

- Cisco VSS introduces unique inter-chassis traffic engineering to develop a fully-distributed forwarding design that helps in increased bandwidth, load balancing, predictable network recovery, and network stability.

Deploying VSS mode in both the distribution layer switch and core layer switch provides numerous technology deployment options that are not available when not using VSS. Designing a common core and distribution layer option using VSS provides greater redundancy and is able to handle the amount of traffic typically present in the main and remote large campus locations. Figure 3-20 shows five unique VSS domain interconnect options. Each variation builds a unique network topology that has a direct impact on steering traffic and network recovery.

Figure 3-20 Core/Distribution Layer Interconnection Design Considerations



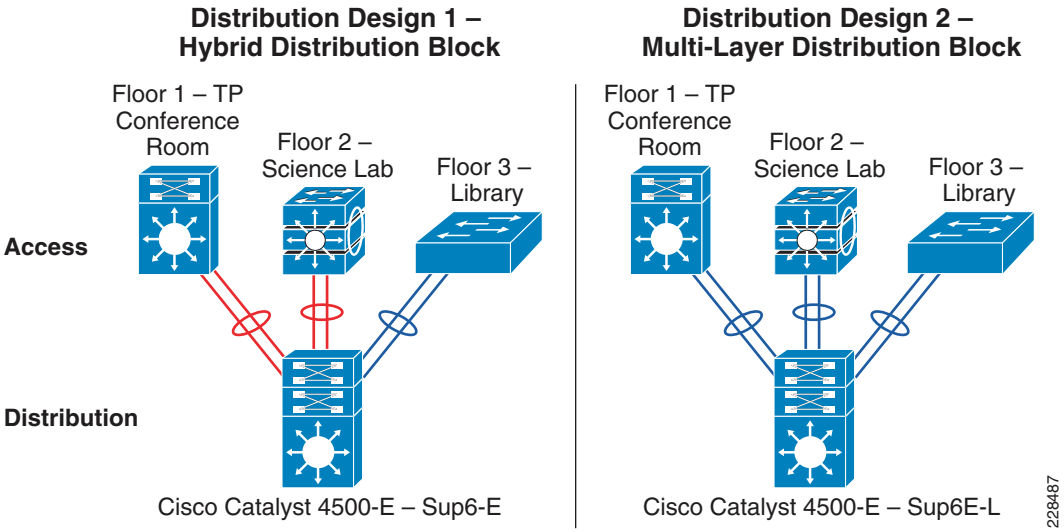
The various core/distribution layer interconnects offer the following:

- *Core/distribution layer interconnection option 1*—A single physical link between each core switch with the corresponding distribution switch.
- *Core/distribution layer interconnection option 2*—A single physical link between each core switch with the corresponding distribution switch, but each link is logically grouped to appear as one single link between the core and distribution layers.
- *Core/distribution layer interconnection option 3*—Two physical links between each core switch with the corresponding distribution switch. This design creates four equal cost multi-path (ECMP) with multiple control plane adjacency and redundant path information. Multiple links provide greater redundancy in case of link failover.
- *Core/distribution layer interconnection option 4*—Two physical links between each core switch with the corresponding distribution switch. There is one link direction between each switch as well as one link connecting to the other distribution switch. The additional link provides greater redundancy in case of link failover. Also these links are logically grouped to appear like option 1 but with greater redundancy.
- *Core/distribution layer interconnection option 5*—This provides the most redundancy between the VSS-enabled core and distribution switches as well as the most simplified configuration, because it appears as if there is only one logical link between the core and the distribution. Cisco recommends deploying this option because it provides higher redundancy and simplicity compared to any other deployment option.

Distribution Layer Design Option 2—Cisco Catalyst 4500-E-Based Distribution Network

Two cost-effective distribution layer models have been designed for the medium-sized and small-sized buildings within each campus location that interconnect to the centralized core layer design option and distributed wiring closet access layer switches. Both models are based on a common physical LAN network infrastructure and can be chosen based on overall network capacity and distribution block design. Both distribution layer design options use a cost-effective single and highly resilient Cisco Catalyst 4500 as an aggregation layer system that offers consistent network operation like a VSS-enabled distribution layer switch. The Cisco Catalyst 4500 Series provides the same technical benefits of VSS for a smaller network capacity within a single Cisco platform. The two Cisco Catalyst 4500-E-based distribution layer options are shown in Figure 3-21.

Figure 3-21 Two Cisco Catalyst 4500-E-Based Distribution Layer Options

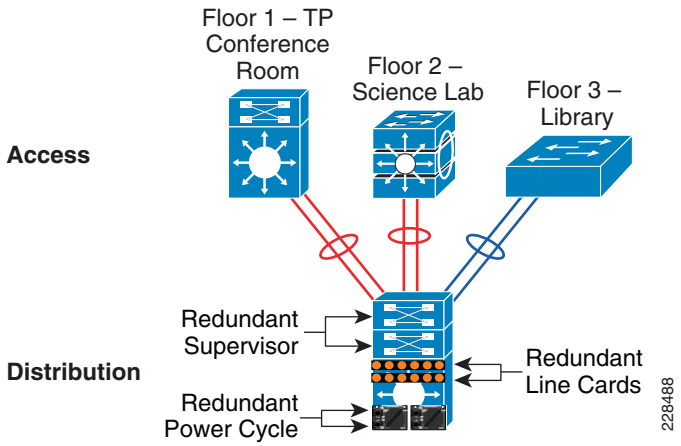


The hybrid distribution block must be deployed with the next-generation supervisor Sup6-E module. Implementing redundant Sup6-Es in the distribution layer can interconnect access layer switches and core layer switches using a single point-to-point logical connection. This cost-effective and resilient distribution design option leverages core layer design option 2 to take advantage of all the operational consistency and architectural benefits.

Alternatively, the multilayer distribution block option requires the Cisco Catalyst 4500-E Series Switch with next-generation supervisor Sup6E-L deployed. The Sup6E-L supervisor is a cost-effective distribution layer solution that meets all network foundation requirements and can operate at moderate capacity, which can handle a medium-sized college distribution block.

This distribution layer network design provides protection against various types of hardware and software failure, and can deliver consistent sub-second network recovery. A single Catalyst 4500-E with multiple redundant system components can be deployed to offer 1+1 in-chassis redundancy, as shown in Figure 3-22.

Figure 3-22 Highly Redundant Single Distribution Design



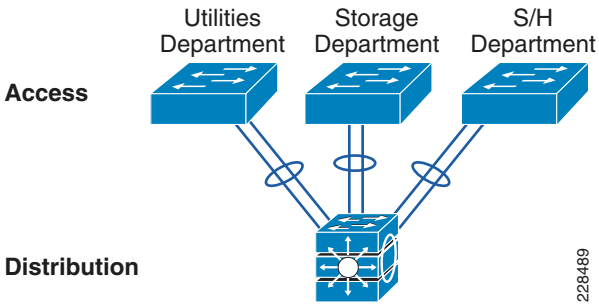
Distribution layer design option 2 is intended for the remote medium-sized campus locations, and is based on the Cisco Catalyst 4500 Series Switches. Although the remote medium and the main and remote large campus locations share similar design principles, the remote medium campus location is smaller and may not need a VSS-based redundant design. Fortunately, network upgrades and expansion become easier to deploy using distribution layer option 2, which helps retain the original network topology and the management operation. Distribution layer design option 2 meets the following goals:

- *Scalability*—The modular Cisco Catalyst 4500 chassis provides the flexibility for distribution block expansion with high throughput modules and port scalability without compromising network performance.
- *Resiliency*—The single distribution system must be equipped with redundant system components, such as supervisor, line card, and power supplies. Implementing redundant components increases network resiliency during various types of failure conditions using NSF/SSO and EtherChannel technology.
- *Simplicity*—This cost-effective design simplifies the distribution block similarly to a VSS-enabled distribution system. The single IP gateway design develops a unified point-to-point network topology in the distribution block to eliminate traditional protocol limitations, enabling the network to operate at full capacity.
- *Cost-effectiveness*—The single distribution system in the core layer helps reduce capital, operational, and ownership cost for the medium-sized campus network design.

Distribution Layer Design Option 3—Cisco Catalyst 3750-E StackWise-Based Distribution Network

Distribution layer design option 3 is intended for a very small building with a limited number of wiring closet switches in the access layer that connects remote classrooms or and office network with a centralized core, as shown in Figure 3-23.

Figure 3-23 Cisco StackWise Plus-enabled Distribution Layer Network Design



While providing consistent network services throughout the campus, a number of network users and IT-managed remote endpoints can be limited in this building. This distribution layer design option recommends using the Cisco Catalyst 3750-E StackWise Plus Series platform for the distribution layer switch.

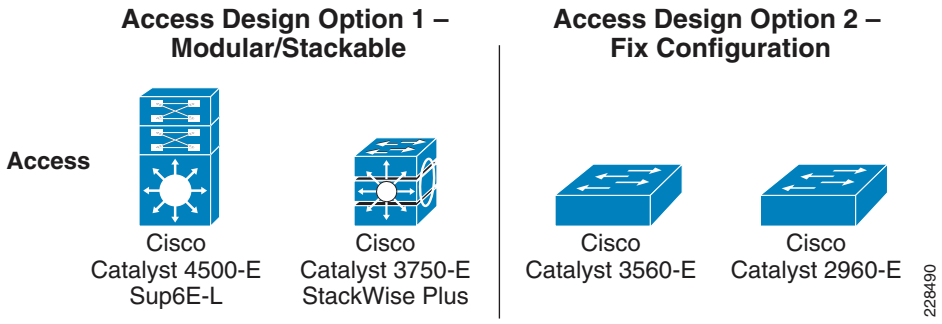
The fixed-configuration Cisco Catalyst 3750-E Series Switch is a multilayer platform that supports Cisco StackWise Plus technology to simplify the network and offers flexibility to expand the network as it grows. With Cisco StackWise Plus technology, the Catalyst 3750-E can be clustered into a high-speed backplane stack ring to logically build as a single large distribution system. Cisco StackWise Plus supports up to nine switches into single stack ring for incremental network upgrades, and increases effective throughput capacity up to 64 Gbps. The chassis redundancy is achieved via stacking, in which member chassis replicate the control functions with each member providing distributed packet forwarding. This is achieved by stacked group members acting as a single virtual Catalyst 3750-E switch. The logical switch is represented as one switch by having one stack member act as the master switch. Thus, when failover occurs, any member of the stack can take over as a master and continue the same services. It is a 1:N form of redundancy where any member can become the master. This distribution layer design option is ideal for the remote small campus location.

Campus Access Layer Network Design

The access layer is the first tier or edge of the campus, where end devices such as PCs, printers, cameras, Cisco TelePresence, and so on attach to the wired portion of the campus network. It is also the place where devices that extend the network out one more level, such as IP phones and wireless access points (APs), are attached. The wide variety of possible types of devices that can connect and the various services and dynamic configuration mechanisms that are necessary, make the access layer one of the most feature-rich parts of the campus network. Not only does the access layer switch allow users to access the network, the access layer switch must provide network protection so that unauthorized users or applications do not enter the network. The challenge for the network architect is determining how to implement a design that meets this wide variety of requirements, the need for various levels of mobility, the need for a cost-effective and flexible operations environment, while being able to provide the appropriate balance of security and availability expected in more traditional, fixed-configuration environments. The next-generation Cisco Catalyst switching portfolio includes a wide range of fixed and modular switching platforms, each designed with unique hardware and software capability to function in a specific role.

Community college campuses may deploy a wide range of network endpoints. The campus network infrastructure resources operate in shared service mode, and include IT-managed devices such as Cisco TelePresence and non-IT-managed devices such as student laptops. Based on several endpoint factors such as function and network demands and capabilities, two access layer design options can be deployed with college campus network edge platforms, as shown in Figure 3-24.

Figure 3-24 Access Layer Design Models



Access Layer Design Option 1—Modular/StackWise Plus Access Layer Network

Access layer design option 1 is intended to address the network scalability and availability for the IT-managed critical voice and video communication network edge devices. To accelerate user experience and college campus physical security protection, these devices require low latency, high performance, and a constant network availability switching infrastructure. Implementing a modular and Cisco StackWise Plus-capable platform provides flexibility to increase network scale in the densely populated campus network edge.

The Cisco Catalyst 4500-E with supervisor Sup6E-L can be deployed to protect devices against access layer network failure. Cisco Catalyst 4500-E Series platforms offer consistent and predictable sub-second network recovery using NSF/SSO technology to minimize the impact of outages on college business and IT operation.

The Cisco Catalyst 3750-E Series is the alternate Cisco switching platform in this design option. Cisco StackWise Plus technology provides flexibility and availability by clustering multiple Cisco Catalyst 3750-E Series Switches into a single high-speed stack ring that simplifies operation and allows incremental access layer network expansion. The Cisco Catalyst 3750-E Series leverages EtherChannel technology for protection during member link or stack member switch failure.

Access Layer Design Option 2—Fixed Configuration Access Layer Network

This entry-level access layer design option is widely chosen for educational environments. The fixed configuration Cisco Catalyst switching portfolio supports a wide range of access layer technologies that allow seamless service integration and enable intelligent network management at the edge.

The fixed configuration Cisco Catalyst 3560-E Series is a commonly deployed platform for wired network access that can be in a mixed configuration with critical devices such as Cisco IP Phones and non-mission critical endpoints such as library PCs, printers, and so on. For non-stop network operation during power outages, the Catalyst 3560-E must be deployed with an internal or external redundant power supply solution using the Cisco RPS 2300. Increasing aggregated power capacity allows flexibility to scale power over Ethernet (PoE) on a per-port basis. With its wire-speed 10G uplink forwarding capacity, this design reduces network congestion and latency to significantly improve application performance.

For a college campus network, the Cisco Catalyst 3560-E is an alternate switching solution for the multilayer distribution block design option discussed in the previous section. The Cisco Catalyst 3560-E Series Switches offer limited software feature support that can function only in a traditional Layer 2 network design. To provide a consistent end-to-end enhanced user experience, the Cisco Catalyst 2960-E supports critical network control services to secure the network edge,

intelligently provide differentiated services to various class-of-service traffic, as well as simplified management. The Cisco Catalyst must leverage the 1G dual uplink port to interconnect the distribution system for increased bandwidth capacity and network availability.

Both design options offer consistent network services at the campus edge to provide differentiated, intelligent, and secured network access to trusted and untrusted endpoints. The distribution options recommended in the previous section can accommodate both access layer design options.

Community College Network Foundation Services Design

After each tier in the model has been designed, the next step for the community college design is to establish key network foundation services. Regardless of the application function and requirements that community colleges demand, the network must be designed to provide a consistent user experience independent of the geographical location of the application. The following network foundation design principles or services must be deployed in each campus location to provide resiliency and availability for all users to obtain and use the applications the community college offers:

- Network addressing hierarchy
- Network foundation technologies for LAN designs
- Multicast for applications delivery
- QoS for application performance optimization
- High availability to ensure user experience even with a network failure

Design guidance for each of these five network foundation services are discussed in the following sections, including where they are deployed in each tier of the LAN design model, the campus location, and capacity.

Network Addressing Hierarchy

Developing a structured and hierarchical IP address plan is as important as any other design aspect of the community college network to create an efficient, scalable, and stable network design. Identifying an IP addressing strategy for the network for the entire community college network design is essential.

Note This section does not explain the fundamentals of TCP/IP addressing; for more details, see the many Cisco Press publications that cover this topic.

The following are key benefits of using hierarchical IP addressing:

- *Efficient address allocation*
  - Hierarchical addressing provides the advantage of grouping all possible addresses contiguously.
  - In non-contiguous addressing, a network can create addressing conflicts and overlapping problems, which may not allow the network administrator to use the complete address block.
- *Improved routing efficiencies*
  - Building centralized main and remote college campus site networks with contiguous IP addresses provides an efficient way to advertise summarized routes to neighbors.
  - Route summarization simplifies the routing database and computation during topology change events.

  - Reduces network bandwidth utilization used by routing protocols.
  - Improves overall routing protocol performance by flooding less messages and improves network convergence time.
- *Improved system performance*
  - Reduces the memory needed to hold large-scale discontiguous and non-summarized route entries.
  - Reduce higher CPU power to re-compute large-scale routing databases during topology change events.
  - Becomes easier to manage and troubleshoot.
  - Helps in overall network and system stability.

Network Foundational Technologies for LAN Design

In addition to a hierarchical IP addressing scheme, it is also essential to determine which areas of the community college design are Layer 2 or Layer 3 to determine whether routing or switching fundamentals need to be applied. The following applies to the three layers in a LAN design model:

- *Core layer*—Because this is a Layer 3 network that interconnects several remote locations and shared devices across the network, choosing a routing protocol is essential at this layer.
- *Distribution layer*—The distribution block uses a combination of Layer 2 and Layer 3 switching to provide for the appropriate balance of policy and access controls, availability, and flexibility in subnet allocation and VLAN usage. Both routing and switching fundamentals need to be applied.
- *Access layer*—This layer is the demarcation point between network infrastructure and computing devices. This is designed for critical network edge functions to provide intelligent application and device-aware services, to set the trust boundary to distinguish applications, provide identity-based network access to protected data and resources, provide physical infrastructure services to reduce greenhouse emission, and more. This subsection provides design guidance to enable various types of Layer 1 to 3 intelligent services, and to optimize and secure network edge ports.

The recommended routing or switching scheme of each layer is discussed in the following sections.

Designing the Core Layer Network

Because the core layer is a Layer 3 network, routing principles must be applied. Choosing a routing protocol is essential, and routing design principles and routing protocol selection criteria are discussed in the following subsections.

Routing Design Principles

Although enabling routing functions in the core is a simple task, the routing blueprint must be well understood and designed before implementation, because it provides the end-to-end reachability path of the college network. For an optimized routing design, the following three routing components must be identified and designed to allow more network growth and provide a stable network, independent of scale:

- *Hierarchical network addressing*—Structured IP network addressing in the community college LAN and/or WAN design is required to make the network scalable, optimal, and resilient.

- *Routing protocol*—Cisco IOS supports a wide range of Interior Gateway Protocols (IGPs). Cisco recommends deploying a single routing protocol across the community college network infrastructure.
- *Hierarchical routing domain*—Routing protocols must be designed in a hierarchical model that allows the network to scale and operate with greater stability. Building a routing boundary and summarizing the network minimizes the topology size and synchronization procedure, which improves overall network resource use and re-convergence.

Routing Protocol Selection Criteria

The criteria for choosing the right protocol vary based on the end-to-end network infrastructure. Although all the routing protocols that Cisco IOS currently supports can provide a viable solution, network architects must consider all the following critical design factors when selecting the right routing protocol to be implemented throughout the internal network:

- *Network design*—Requires a proven protocol that can scale in full-mesh campus network designs and can optimally function in hub-and-spoke WAN network topologies.
- *Scalability*—The routing protocol function must be network- and system-efficient and operate with a minimal number of updates and re-computation, independent of the number of routes in the network.
- *Rapid convergence*—Link-state versus DUAL re-computation and synchronization. Network re-convergence also varies based on network design, configuration, and a multitude of other factors that may be more than a specific routing protocol can handle. The best convergence time can be achieved from a routing protocol if the network is designed to the strengths of the protocol.
- *Operational*—A simplified routing protocol that can provide ease of configuration, management, and troubleshooting.

Cisco IOS supports a wide range of routing protocols, such as Routing Information Protocol (RIP) v1/2, Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS). However, Cisco recommends using EIGRP or OSPF for this network design. EIGRP is a popular version of an Interior Gateway Protocol (IGP) because it has all the capabilities needed for small to large-scale networks, offers rapid network convergence, and above all is simple to operate and manage. OSPF is popular link-state protocol for large-scale enterprise and service provider networks. OSPF enforces hierarchical routing domains in two tiers by implementing backbone and non-backbone areas. The OSPF area function depends on the network connectivity model and the role of each OSPF router in the domain. OSPF can scale higher but the operation, configuration, and management might become too complex for the community college LAN network infrastructure.

Other technical factors must be considered when implementing OSPF in the network, such as OSPF router type, link type, maximum transmission unit (MTU) considerations, designated router (DR)/backup designated router (BDR) priority, and so on. This document provides design guidance for using simplified EIGRP in the community college campus and WAN network infrastructure.

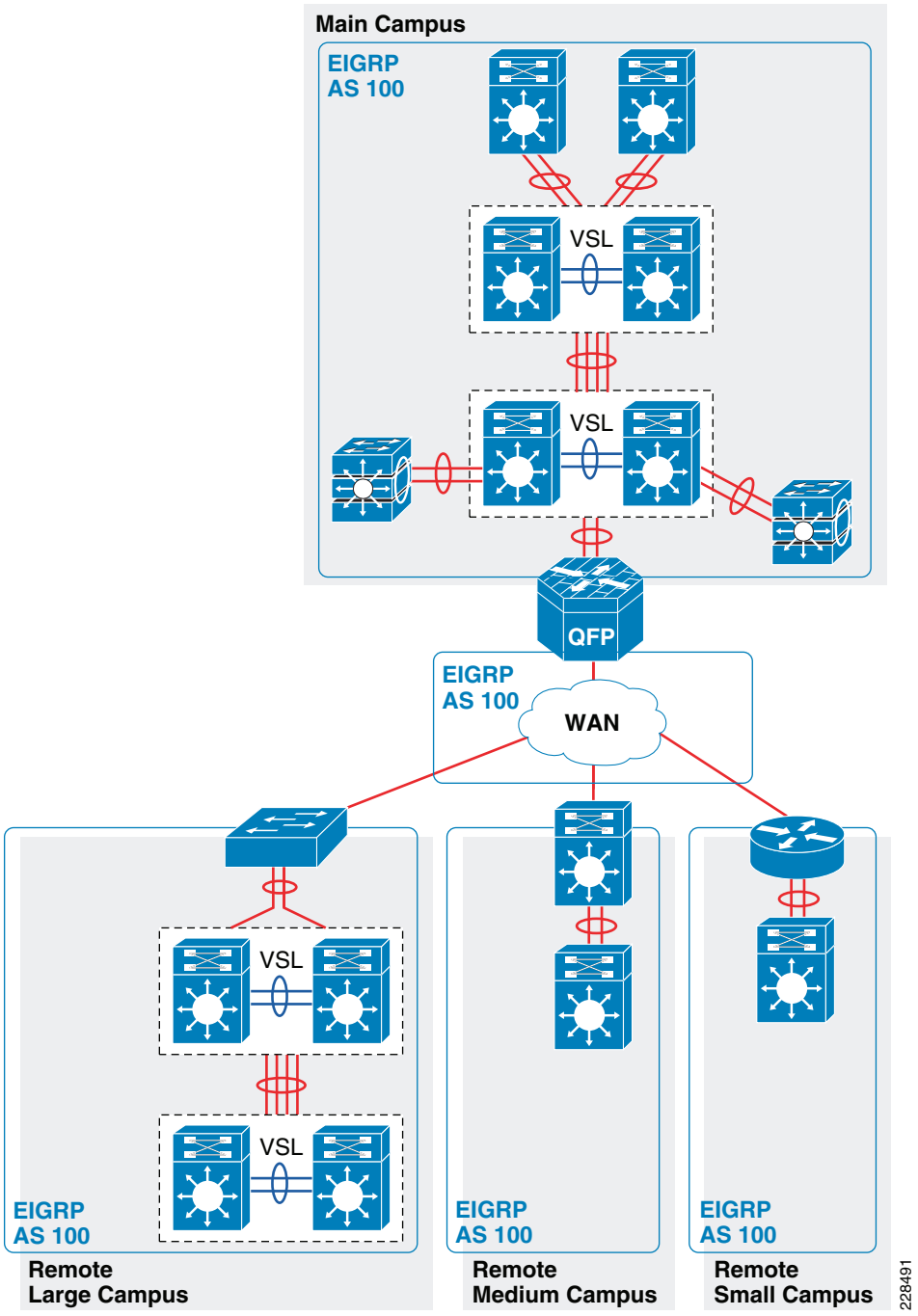
Note For detailed information on EIGRP and OSPF, see the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html.

Designing an End-to-End EIGRP Routing Network

EIGRP is a balanced hybrid routing protocol that builds neighbor adjacency and flat routing topology on a per autonomous system (AS) basis. Cisco recommends considering the following three critical design tasks before implementing EIGRP in the community college LAN core layer network:

- *EIGRP autonomous system*—The Layer 3 LAN and WAN infrastructure of the community college design must be deployed in a single EIGRP AS, as shown in Figure 3-25. A single EIGRP AS reduces operational tasks and prevents route redistribution, loops, and other problems that may occur because of misconfiguration.

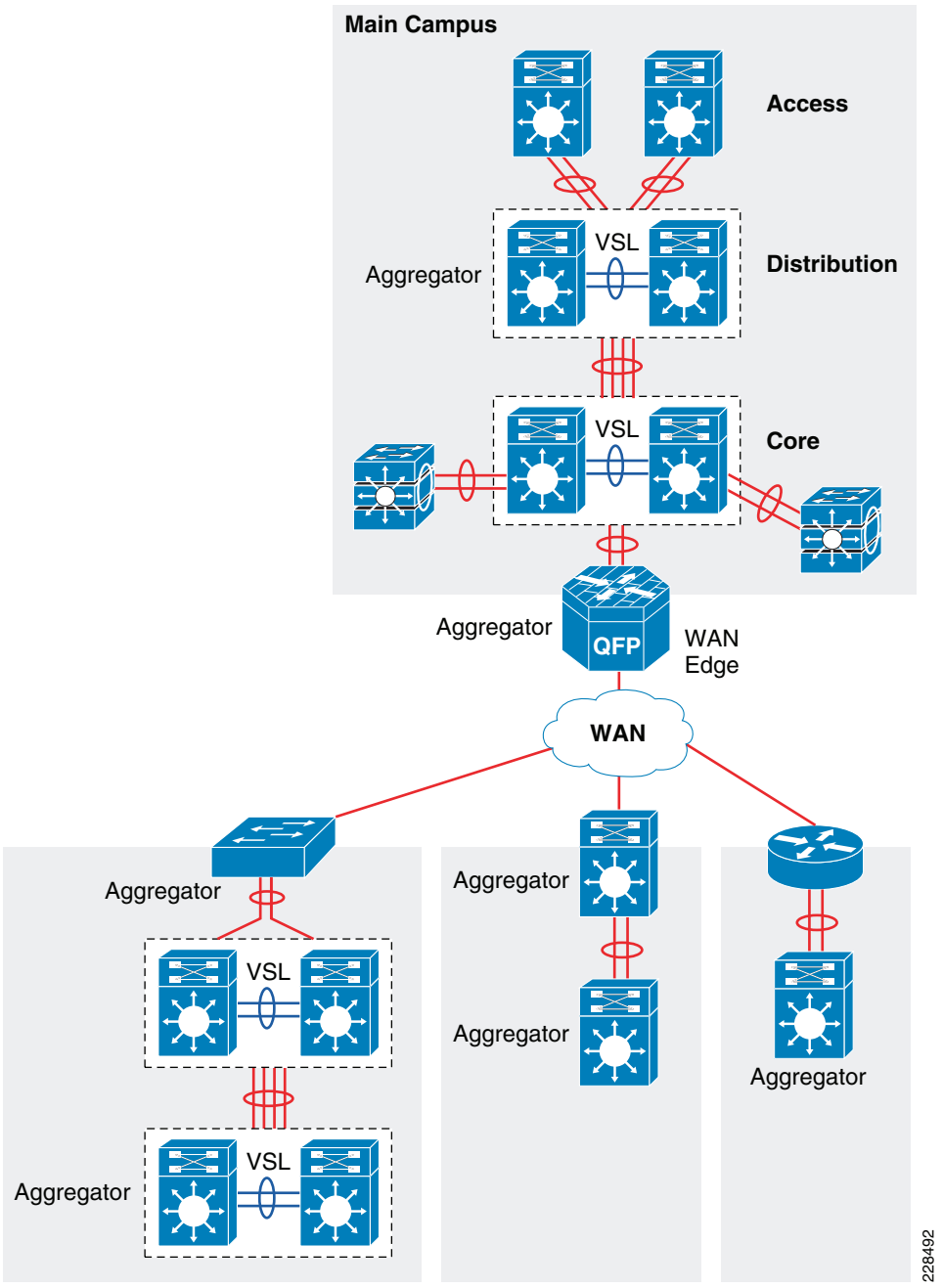
Figure 3-25 Sample End-to-End EIGRP Routing Design in Community College LAN Network



In the example in Figure 3-25, AS100 is the single EIGRP AS for the entire design.

- *EIGRP adjacency protection*—This increases network infrastructure efficiency and protection by securing the EIGRP adjacencies with internal systems. This task involves two subset implementation tasks on each EIGRP-enabled network devices:
  - Increases system efficiency—Blocks EIGRP processing with passive-mode configuration on physical or logical interfaces connected to non- EIGRP devices in the network, such as PCs. The best practice helps reduce CPU utilization and secures the network with unprotected EIGRP adjacencies with untrusted devices.
  - Network security—Each EIGRP neighbor in the LAN/WAN network must be trusted by implementing and validating the Message-Digest algorithm 5 (MD5) authentication method on each EIGRP-enabled system in the network.
- *Optimizing EIGRP topology*—EIGRP allows network administrators to summarize multiple individual and contiguous networks into a single summary network before advertising to the neighbor. Route summarization helps improve network performance, stability, and convergence by hiding the fault of an individual network that requires each router in the network to synchronize the routing topology. Each aggregating device must summarize a large number of networks into a single summary route. Figure 3-26 shows an example of the EIGRP topology for the community college LAN design.

Figure 3-26 EIGRP Route Aggregator Design



By default, EIGRP speakers transmit Hello packets every 5 seconds, and terminates EIGRP adjacency if the neighbor fails to receive it within 15 seconds of hold-down time. In this network design, Cisco recommends retaining default EIGRP Hello and Hold timers on all EIGRP-enabled platforms.

Designing the Campus Distribution Layer Network

This section provides design guidelines for deploying various types of Layer 2 and Layer 3 technology in the distribution layer. Independent of which implemented distribution layer design model is deployed, the deployment guidelines remain consistent in all designs.

Because the distribution layer can be deployed with both Layer 2 and Layer 3 technologies, the following two network designs are recommended:

- Multilayer
- Routed access

Designing the Multilayer Network

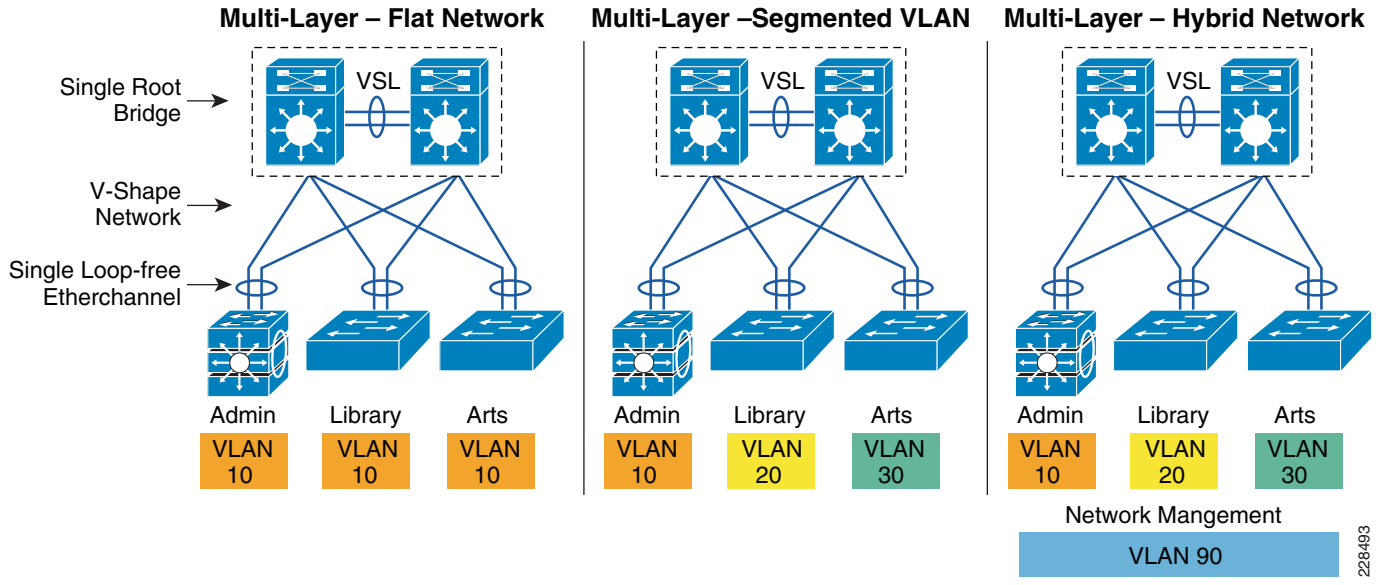
A multilayer network is a traditional, simple, and widely deployed scenario, regardless of network scale. The access layer switches in the campus network edge interface with various types of endpoints and provide intelligent Layer 1/2 services. The access layer switches interconnect to distribution switches with the Layer 2 trunk, and rely on the distribution layer aggregation switch to perform intelligent Layer 3 forwarding and to set policies and access control.

There are the following three design variations to build a multilayer network; all variations must be deployed in a V-shape physical network design and must be built to provide a loop-free topology:

- *Flat*—Certain applications and user access requires that the broadcast domain design span more than a single wiring closet switch. The multilayer network design provides the flexibility to build a single large broadcast domain with an extended star topology. Such flexibility introduces scalability, performance, and security challenges, and may require extra attention to protect the network against misconfiguration and miswiring that can create spanning-tree loops and de-stabilize the network.
- *Segmented*—Provides a unique VLAN for different education divisions and college business function segments to build a per-department logical network. All network communication between education and administrative groups passes through the routing and forwarding policies defined at the distribution layer.
- *Hybrid*—A hybrid logical network design segments VLAN workgroups that do not span different access layer switches, and allows certain VLANs (for example, that net management VLAN) to span across the access-distribution block. The hybrid network design enables flat Layer 2 communication without impacting the network, and also helps reduce the number of subnets used.

Figure 3-27 shows the three design variations for the multilayer network.

Figure 3-27 Multilayer Design Variations

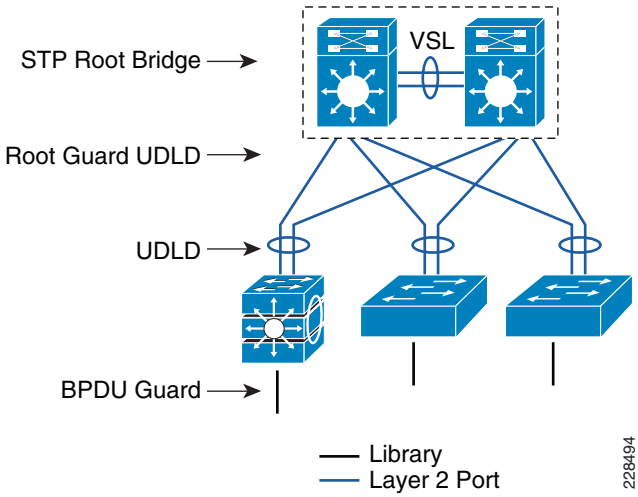


Cisco recommends that the hybrid multilayer access-distribution block design use a loop-free network topology, and span a few VLANs that require such flexibility, such as the management VLAN.

Ensuring a loop-free topology is critical in a multilayer network design. Spanning-Tree Protocol (STP) dynamically develops a loop-free multilayer network topology that can compute the best forwarding path and provide redundancy. Although STP behavior is deterministic, it is not optimally designed to mitigate network instability caused by hardware miswiring or software misconfiguration. Cisco has developed several STP extensions to protect against network malfunctions, and to increase stability and availability. All Cisco Catalyst LAN switching platforms support the complete STP toolkit suite that must be enabled globally on individual logical and physical ports of the distribution and access layer switches.

Figure 3-28 shows an example of enabling various STP extensions on distribution and access layer switches in all campus sites.

Figure 3-28 Protecting Multilayer Network with Cisco STP Toolkit

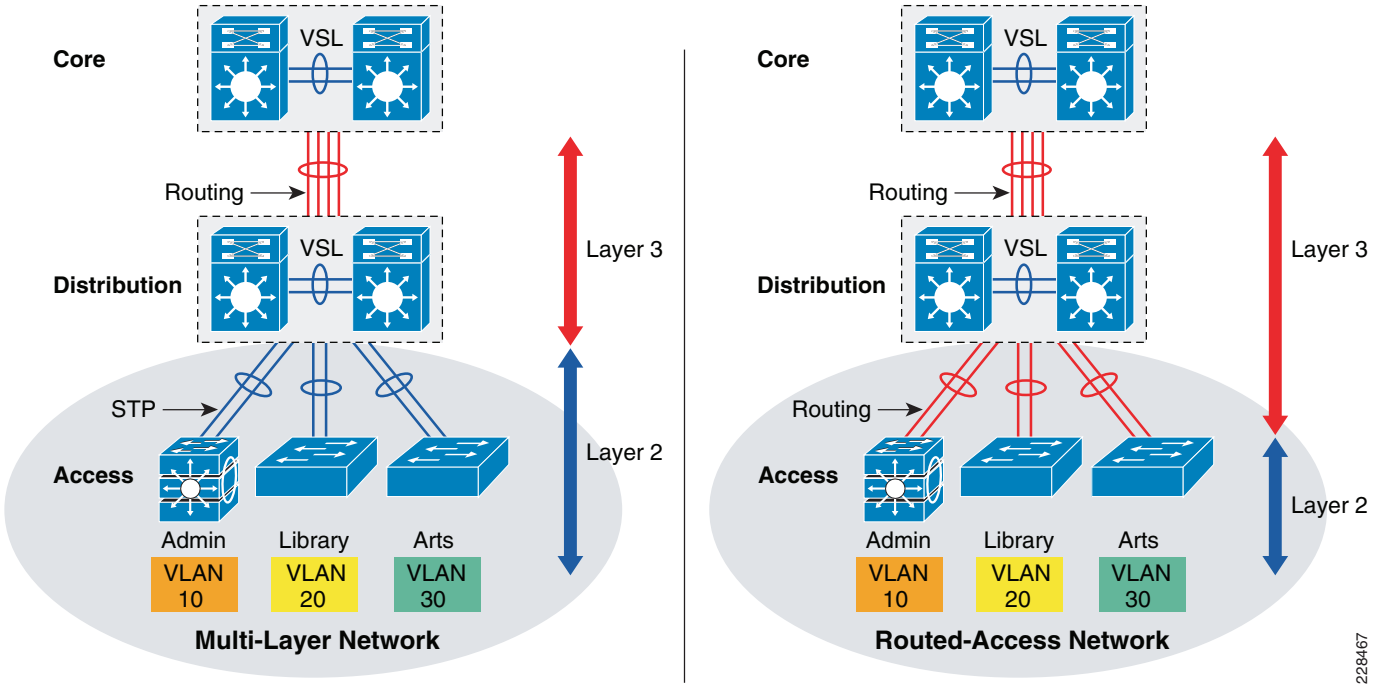


Note For additional STP information, see the following URL: http://www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_troubleshooting_technotes_list.html.

Designing the Routed Access Network

Routing functions in the access layer network simplify configuration, optimize distribution performances, and provide end-to-end troubleshooting tools. Implementing Layer 3 functions in the access layer replaces Layer 2 trunk configuration to a single point-to-point Layer 3 interface with a collapsed core system in the aggregation layer. Pushing Layer 3 functions one tier down on Layer 3 access switches changes the traditional multilayer network topology and forwarding development path. Implementing Layer 3 functions in the access switch does not require any physical or logical link reconfiguration; the access-distribution block can be used, and is as resilient as in the multilayer network design. Figure 3-29 shows the differences between the multilayer and routed access network designs, as well as where the Layer 2 and Layer 3 boundaries exist in each network design.

Figure 3-29 Layer 2 and Layer 3 Boundaries for Multilayer and Routed Access Network Design



Routed-access network design enables Layer 3 access switches to perform Layer 2 demarcation point and provide Inter-VLAN routing and gateway function to the endpoints. The Layer 3 access switches makes more intelligent, multi-function and policy-based routing and switching decision like distribution-layer switches.

Although Cisco VSS and a single redundant distribution design are simplified with a single point-to-point EtherChannel, the benefits in implementing the routed access design in community colleges are as follows:

- Eliminates the need for implementing STP and the STP toolkit on the distribution system. As a best practice, the STP toolkit must be hardened at the access layer.
- Shrinks the Layer 2 fault domain, thus minimizing the number of denial-of-service (DoS)/ distributed denial-of-service (DDoS) attacks.
- Bandwidth efficiency—Improves Layer 3 uplink network bandwidth efficiency by suppressing Layer 2 broadcasts at the edge port.
- Improves overall collapsed core and distribution resource utilization.

Enabling Layer 3 functions in the access-distribution block must follow the same core network designs as mentioned in previous sections to provide network security as well as optimize the network topology and system resource utilization:

- *EIGRP autonomous system*—Layer 3 access switches must be deployed in the same EIGRP AS as the distribution and core layer systems.
- *EIGRP adjacency protection*—EIGRP processing must be enabled on uplink Layer 3 EtherChannels, and must block remaining Layer 3 ports by default in passive mode. Access switches must establish secured EIGRP adjacency using the MD5 hash algorithm with the aggregation system.

- *EIGRP network boundary*—All EIGRP neighbors must be in a single AS to build a common network topology. The Layer 3 access switches must be deployed in EIGRP stub mode for a concise network view.

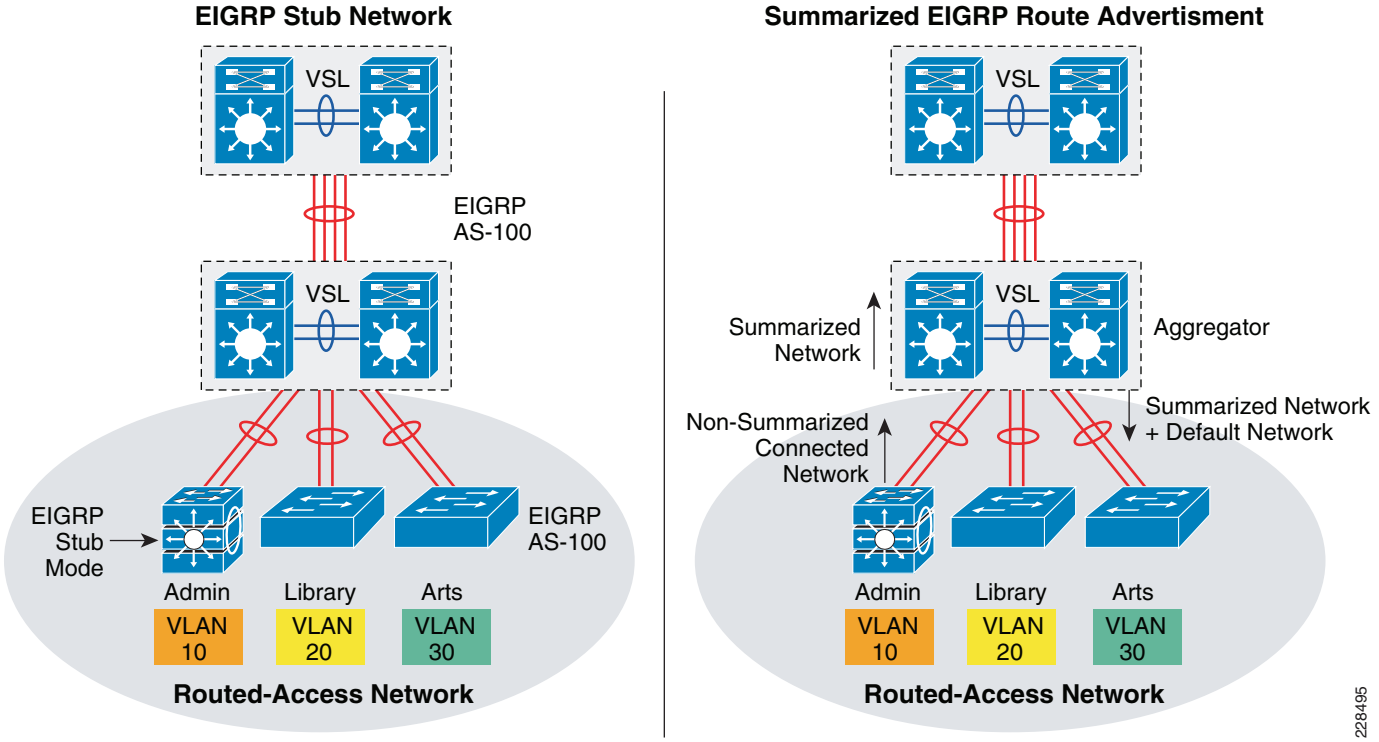
Designing the Layer 3 Access Layer

EIGRP creates and maintains a single flat routing topology network between EIGRP peers. Building a single routing domain in a large-scale campus core design allows for complete network visibility and reachability that may interconnect multiple campus components, such as distribution blocks, services blocks, the data center, the WAN edge, and so on.

In the three- or two-tier deployment models, the Layer 3 access switch must always have single physical or logical forwarding to a distribution switch. The Layer 3 access switch dynamically develops the forwarding topology pointing to a single distribution switch as a single Layer 3 next hop. Because the distribution switch provides a gateway function to rest of the network, the routing design on the Layer 3 access switch can be optimized with the following two techniques to improve performance and network reconvergence in the access-distribution block, as shown in Figure 3-30:

- Deploying the Layer 3 access switch in EIGRP stub mode
- Summarizing the network view with a default route to the Layer 3 access switch for intelligent routing functions

Figure 3-30 Designing and Optimizing EIGRP Network Boundary for the Access Layer



Multicast for Application Delivery

Because unicast communication is based on the one-to-one forwarding model, it becomes easier in routing and switching decisions to perform destination address lookup, determine the egress path by scanning forwarding tables, and to switch traffic. In the unicast routing and switching technologies discussed in the previous section, the network may need to be made more efficient by allowing certain applications where the same content or application must be replicated to multiple users. IP multicast delivers source traffic to multiple receivers using the least amount of network resources as possible without placing an additional burden on the source or the receivers. Multicast packet replication in the network is done by Cisco routers and switches enabled with Protocol Independent Multicast (PIM) as well as other multicast routing protocols.

Similar to the unicast methods, multicast requires the following design guidelines:

- Choosing a multicast addressing design
- Choosing a multicast routing protocol
- Providing multicast security regardless of the location within the community college design

Multicast Addressing Design

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. A range of class D address space is assigned to be used for IP multicast applications. All multicast group addresses fall in the range from 224.0.0.0 through 239.255.255.255. Layer 3 addresses in multicast communications operate differently; while the destination address of IP multicast traffic is in the multicast group range, the source IP address is always in the unicast address range. Multicast addresses are assigned in various pools for well-known multicast-based network protocols or inter-domain multicast communications, as listed in Table 3-2.

Table 3-2 Multicast Address Range Assignments

Application	Address Range
Reserved—Link local network protocols.	224.0.0.0/24
Global scope—Group communication between an organization and the Internet.	224.0.1.0 – 238.255.255.255
Source Specific Multicast (SSM)—PIM extension for one-to-many unidirectional multicast communication.	232.0.0.0/8
GLOP—Inter-domain multicast group assignment with reserved global AS.	233.0.0.0/8
Limited scope—Administratively scoped address that remains constrained within a local organization or AS. Commonly deployed in enterprise, education, and other organizations.	239.0.0.0/8

During the multicast network design phase, community college network architects must select a range of multicast sources from the limited scope pool (239/8).

Multicast Routing Design

To enable end-to-end dynamic multicast operation in the network, each intermediate system between the multicast receiver and source must support the multicast feature. Multicast develops the forwarding table differently than the unicast routing and switching model. To enable communication, multicast requires specific multicast routing protocols and dynamic group membership.

Multicast Routing Protocol Design

The community college LAN design must be able to build packet distribution trees that specify a unique forwarding path between the subnet of the source and each subnet containing members of the multicast group. A primary goal in distribution trees construction is to ensure that no more than one copy of each packet is forwarded on each branch of the tree. The two basic types of multicast distribution trees are as follows:

- *Source trees*—The simplest form of a multicast distribution tree is a source tree, with its root at the source and branches forming a tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).
- *Shared trees*—Unlike source trees that have their root at the source, shared trees use a single common root placed at a selected point in the network. This shared root is called a rendezvous point (RP).

The PIM protocol is divided into the following two modes to support both types of multicast distribution trees:

- *Dense mode (DM)*—Assumes that almost all routers in the network need to distribute multicast traffic for each multicast group (for example, almost all hosts on the network belong to each multicast group). PIM in DM mode builds distribution trees by initially flooding the entire network and then pruning back the small number of paths without receivers.
- *Sparse mode (SM)*—Assumes that relatively few routers in the network are involved in each multicast. The hosts belonging to the group are widely dispersed, as might be the case for most multicasts over the WAN. Therefore, PIM-SM begins with an empty distribution tree and adds branches only as the result of explicit Internet Group Management Protocol (IGMP) requests to join the distribution. PIM-SM mode is ideal for a network without dense receivers and multicast transport over WAN environments, and it adjusts its behavior to match the characteristics of each receiver group.

Selecting the PIM mode depends on the multicast applications that use various mechanisms to build multicast distribution trees. Based on the multicast scale factor and centralized source deployment design for one-to-many multicast communication in community college LAN infrastructures, Cisco recommends deploying PIM-SM because it is efficient and intelligent in building multicast distribution tree. All the recommended platforms in this design support PIM-SM mode on physical or logical (switched virtual interface [SVI] and EtherChannel) interfaces.

Designing PIM Rendezvous Point

The following sections discuss best practices in designing the PIM RP.

PIM-SM RP Placement Best Practices

It is assumed that each community college site has a wide range of local multicast sources in the data center for distributed community college IT-managed media and student research and development applications. In such a distributed multicast network design, Cisco recommends deploying PIM RP on

each site for wired or wireless multicast receivers and sources to join and register at the closest RP. The community college reference design recommends PIM-SM RP placement on a VSS-enabled and single resilient core system in the three-tier campus design, or on the collapsed core/distribution system in the two-tier campus design model.

PIM-SM RP Mode Best Practices

PIM-SM supports RP deployment in the following three modes in the network:

- *Static*—In this mode, RP must be statically identified and configured on each PIM router in the network. RP load balancing and redundancy can be achieved using anycast RP.
- *Auto-RP*—This mode is a dynamic method for discovering and announcing the RP in the network. Auto-RP implementation is beneficial when there are multiple RPs and groups that often change in the network. To prevent network reconfiguration during a change, the RP mapping agent router must be designated in the network to receive RP group announcements and to arbitrate conflicts, as part of the PIM version 1 specification.
- *BootStrap Router (BSR)*—This mode performs the same tasks as Auto-RP but in a different way, and is part of the PIM version 2 specification. Auto-RP and BSR cannot co-exist or interoperate in the same network.

In a small to mid-sized multicast network, static RP configuration is recommended over the other modes. Static RP implementation offers RP redundancy and load sharing, and an additional simple access control list (ACL) can be applied to deploy RP without compromising multicast network security. Cisco recommends designing the community college LAN multicast network using the static PIM-SM mode configuration.

PIM-SM RP Redundancy Best Practices

PIM-SM RP redundancy and load sharing becomes imperative in the community college LAN design, because each recommended core layer design model provides resiliency and simplicity. In the Cisco Catalyst 6500 VSS-enabled core layer, the dynamically discovered group-to-RP entries are fully synchronized to the standby switch. Combining NSF/SSO capabilities with IPv4 multicast reduces the network recovery time and retains the user and application performance at an optimal level. In the non-VSS-enabled network design, PIM-SM uses Anycast RP and Multicast Source Discovery Protocol (MSDP) for node failure protection. PIM-SM redundancy and load sharing is simplified with the Cisco VSS-enabled core. Because VSS is logically a single system and provides node protection, there is no need to implement Anycast RP and MSDP on a VSS-enabled PIM-SM RP.

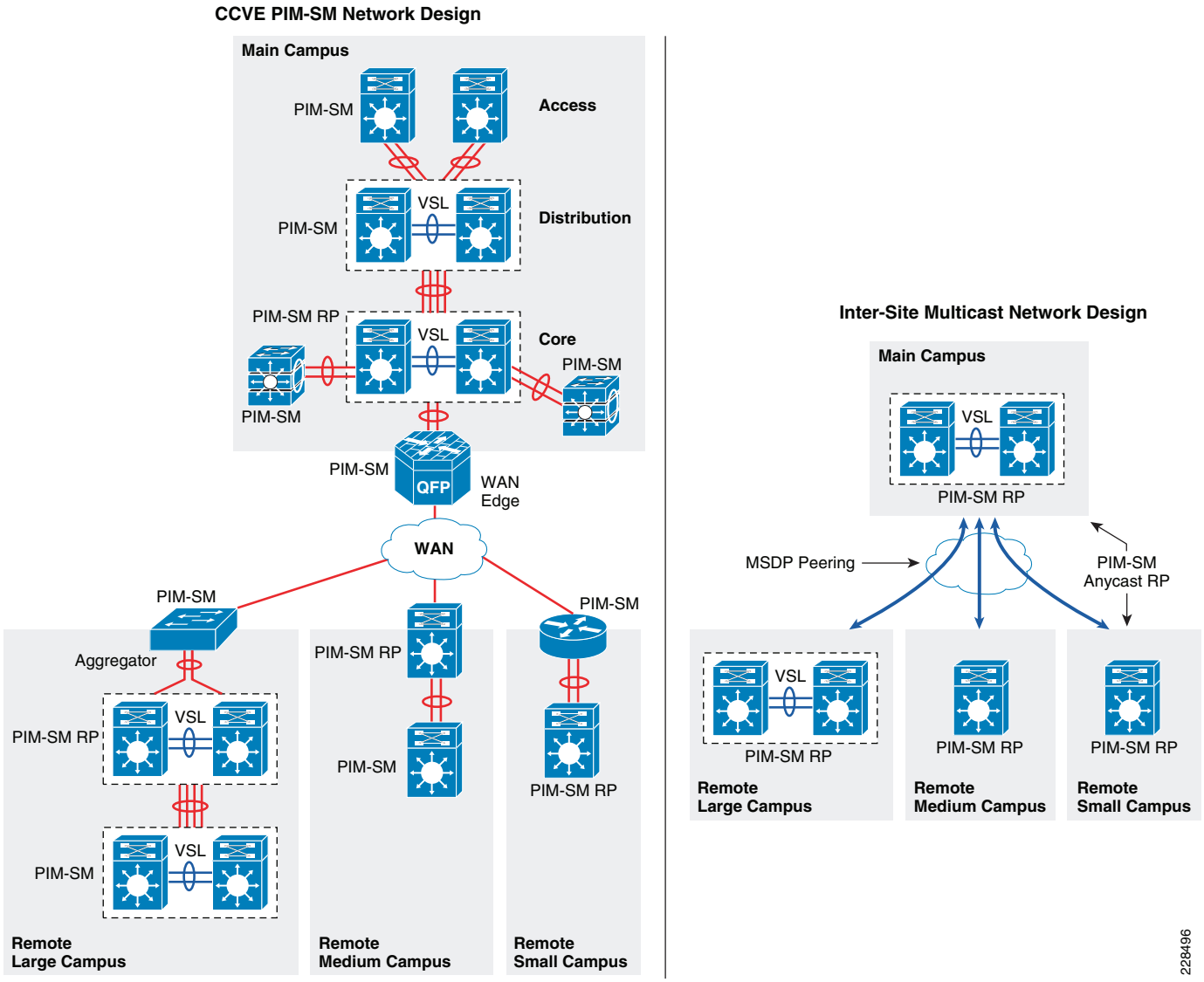
Inter-Site PIM RP Best Practices

MSDP allows PIM RPs to share information about the active sources. PIM-SM RPs discover local receivers through PIM join messages, while the multicast source can be in a local or remote network domain. MSDP allows each multicast domain to maintain an independent RP that does not rely on other multicast domains, but does enable RPs to forward traffic between domains. PIM-SM is used to forward the traffic between the multicast domains.

Anycast RP is a useful application of MSDP. Originally developed for interdomain multicast applications, MSDP used with Anycast RP is an intradomain feature that provides redundancy and load sharing capabilities. Large networks typically use Anycast RP for configuring a PIM-SM network to meet fault tolerance requirements within a single multicast domain.

The community college LAN multicast network must be designed with Anycast RP. PIM-SM RP at the main or the centralized core must establish an MSDP session with RP on each remote site to exchange distributed multicast source information and allow RPs to join SPT to active sources as needed. Figure 3-31 shows an example of a community college LAN multicast network design.

Figure 3-31 Community College LAN Multicast Network Design



Dynamic Group Membership Design

Multicast receiver registration is done via IGMP protocol signaling. IGMP is an integrated component of an IP multicast framework that allows the receiver hosts and transmitting sources to be dynamically added to and removed from the network. Without IGMP, the network is forced to flood rather than multicast the transmissions for each group. IGMP operates between a multicast receiver host in the access layer and the Layer 3 router at the distribution layer.

The multicast system role changes when the access layer is deployed in the multilayer and routed access models. Because multilayer access switches do not run PIM, it becomes complex to make forwarding decisions out of the receiver port. In such a situation, Layer 2 access switches flood the traffic on all ports. This multilayer limitation in access switches is solved by using the IGMP snooping feature, which is enabled by default and is recommended to not be disabled.

IGMP is still required when a Layer 3 access layer switch is deployed in the routed access network design. Because the Layer 3 boundary is pushed down to the access layer, IGMP communication is limited between a receiver host and the Layer 3 access switch. In addition to the unicast routing protocol, PIM-SM must be enabled at the Layer 3 access switch to communicate with RPs in the network.

Designing Multicast Security

When designing multicast security in the community college LAN design, two key concerns are preventing a rogue source and preventing a rogue PIM-RP.

Preventing Rogue Source

In a PIM-SM network, an unwanted traffic source can be controlled with the **pim accept-register** command. When the source traffic hits the first-hop router, the first-hop router (DR) creates the (S,G) state and sends a PIM source register message to the RP. If the source is not listed in the accept-register filter list (configured on the RP), the RP rejects the register and sends back an immediate Register-Stop message to the DR. The drawback with this method of source filtering is that with the **pim accept-register** command on the RP, the PIM-SM (S,G) state is still created on the first-hop router of the source. This can result in traffic reaching receivers local to the source and located between the source and the RP. Furthermore, because the **pim accept-register** command works on the control plane of the RP, this can be used to overload the RP with fake register messages and possibly cause a DoS condition.

Preventing Rogue PIM-RP

Like the multicast source, any router can be misconfigured or can maliciously advertise itself as a multicast RP in the network with the valid multicast group address. With a static RP configuration, each PIM-enabled router in the network can be configured to use static RP for the multicast source and override any other Auto-RP or BSR multicast router announcement from the network.

QoS for Application Performance Optimization

The function and guaranteed low latency bandwidth expectation of network users and endpoints has evolved significantly over the past few years. Application and device awareness has become a key tool in providing differentiated service treatment at the campus LAN edge. Media applications, and particularly video-oriented media applications, are evolving as the education community enters the digital era of delivering education, as well as the increased campus network and asset security requirements. Integrating video applications in the community college LAN network exponentially increases bandwidth utilization and fundamentally shifts traffic patterns. Business drivers behind this media application growth include remote learning, as well as leveraging the network as a platform to build an energy-efficient network to minimize cost and go “green”. High-definition media is transitioning from the desktop to conference rooms, and social networking phenomena are crossing over into educational settings. Besides internal and college research applications, media applications are fueling a new wave of IP convergence, requiring the ongoing development of converged network designs.

Converging media applications onto an IP network is much more complex than converging voice over IP (VoIP) alone. Media applications are generally bandwidth-intensive and bursty (as compared to VoIP), and many different types of media applications exist; in addition to IP telephony, applications can include live and on-demand streaming media applications, digital signage applications, high-definition room-based conferencing applications, as well as an infinite array of data-oriented applications. By

embracing media applications as the next cycle of convergence, community college IT departments can think holistically about their network design and its readiness to support the coming tidal wave of media applications, and develop a network-wide strategy to ensure high quality end-user experiences.

The community college LAN infrastructure must set the administrative policies to provide differentiated forwarding services to the network applications, users and endpoints to prevent contention. The characteristic of network services and applications must be well understood, so that policies can be defined that allow network resources to be used for internal applications, to provide best-effort services for external traffic, and to keep the network protected from threats.

The policy for providing network resources to an internal application is further complicated when interactive video and real-time VoIP applications are converged over the same network that is switching mid-to-low priority data traffic. Deploying QoS technologies in the campus allows different types of traffic to contend inequitably for network resources. Real-time applications such as voice, interactive, and physical security video can be given priority or preferential services over generic data applications, but not to the point that data applications are starving for bandwidth.

Community College LAN QoS Framework

Each group of managed and un-managed applications with unique traffic patterns and service level requirements requires a dedicated QoS class to provision and guarantee these service level requirements. The community college LAN network architect may need to determine the number of classes for various applications, as well as how should these individual classes should be implemented to deliver differentiated services consistently in main and remote college campus sites. Cisco recommends following relevant industry standards and guidelines whenever possible, to extend the effectiveness of your QoS policies beyond your direct administrative control.

With minor changes, the community college LAN QoS framework is developed based on RFC4594 that follows industry standard and guidelines to function consistently in heterogeneous network environment. These guidelines are to be viewed as industry best-practice recommendations. Community college and service providers are encouraged to adopt these marking and provisioning recommendations, with the aim of improving QoS consistency, compatibility, and interoperability. However, because these guidelines are not standards, modifications can be made to these recommendations as specific needs or constraints require. To this end, to meet specific business requirements, Cisco has made a minor modification to its adoption of RFC 4594, namely the switching of call-signaling and broadcast video markings (to CS3 and CS5, respectively).

RFC 4594 outlines twelve classes of media applications that have unique service level requirements, as shown in Figure 3-32.

Figure 3-32 Community College LAN Campus 12-Class QoS Policy Recommendation

Application Class	Media Application Examples	PHB	Admission Control	Queuing and Dropping
VoIP Telephony	Cisco IP Phone	EF	Required	Priority Queue (PQ)
Broadcast Video	Cisco IPVS, Enterprise TV	CS5	Required	(Optional) PQ
Real-Time Interactive	Cisco TelePresence	CS4	Required	(Optional) PQ
Multimedia Conferencing	Cisco CUPC, WebEx	AF4	Required	BW Queue + DSCP WRED
Multimedia Streaming	Cisco DMS, IP/TV	AF3	Recommended	BW Queue + DSCP WRED
Network Control	EIGRP, OSPF, HSRP, IKE	CS6		BW Queue
Call-Signaling	SCCP, SIP, H.323	CS3		BW Queue
Ops/Admin/Mgmt (OAM)	SNMP, SSH, Syslog	CS2		BW Queue
Transactional Data	ERP Apps, CRM Apps	AF2		BW Queue + DSCP WRED
Bulk Data	E-mail, FTP, Backup	AF1		BW Queue + DSCP WRED
Best Effort	Default Class	DF		Default Queue + RED
Scavenger	YouTube, Gaming, P2P	CS1		Min BW Queue

228497

The twelve classes are as follows:

- *VoIP telephony*—This service class is intended for VoIP telephony (bearer-only) traffic (VoIP signaling traffic is assigned to the call-signaling class). Traffic assigned to this class should be marked EF. This class is provisioned with expedited forwarding (EF) per-hop behavior (PHB). The EF PHB-defined in RFC 3246 is a strict-priority queuing service and, as such, admission to this class should be controlled (admission control is discussed in the following section). Examples of this type of traffic include G.711 and G.729a.
- *Broadcast video*—This service class is intended for broadcast TV, live events, video surveillance flows, and similar *inelastic* streaming video flows, which are highly drop sensitive and have no retransmission and/or flow control capabilities. Traffic in this class should be marked class selector 5 (CS5) and may be provisioned with an EF PHB; as such, admission to this class should be controlled. Examples of this traffic include live Cisco Digital Media System (DMS) streams to desktops or to Cisco Digital Media Players (DMPs), live Cisco Enterprise TV (ETV) streams, and Cisco IP Video Surveillance.
- *Real-time interactive*—This service class is intended for (inelastic) room-based, high-definition interactive video applications and is intended primarily for voice and video components of these applications. Whenever technically possible and administratively feasible, data sub-components of this class can be separated out and assigned to the transactional data traffic class. Traffic in this class should be marked CS4 and may be provisioned with an EF PHB; as such, admission to this class should be controlled. A sample application is Cisco TelePresence.
- *Multimedia conferencing*—This service class is intended for desktop software multimedia collaboration applications and is intended primarily for voice and video components of these applications. Whenever technically possible and administratively feasible, data sub-components of this class can be separated out and assigned to the transactional data traffic class. Traffic in this class should be marked assured forwarding (AF) Class 4 (AF41) and should be provisioned with a guaranteed bandwidth queue with Differentiated Services Code Point (DSCP)-based Weighted Random Early Detection (WRED) enabled. Admission to this class should be controlled;

additionally, traffic in this class may be subject to policing and re-marking. Sample applications include Cisco Unified Personal Communicator, Cisco Unified Video Advantage, and the Cisco Unified IP Phone 7985G.

- *Multimedia streaming*—This service class is intended for video-on-demand (VoD) streaming video flows, which, in general, are more elastic than broadcast/live streaming flows. Traffic in this class should be marked AF Class 3 (AF31) and should be provisioned with a guaranteed bandwidth queue with DSCP-based WRED enabled. Admission control is recommended on this traffic class (though not strictly required) and this class may be subject to policing and re-marking. Sample applications include Cisco Digital Media System VoD streams.
- *Network control*—This service class is intended for network control plane traffic, which is required for reliable operation of the enterprise network. Traffic in this class should be marked CS6 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, because network control traffic should not be dropped (if this class is experiencing drops, the bandwidth allocated to it should be re-provisioned). Sample traffic includes EIGRP, OSPF, Border Gateway Protocol (BGP), HSRP, Internet Key Exchange (IKE), and so on.
- *Call-signaling*—This service class is intended for signaling traffic that supports IP voice and video telephony. Traffic in this class should be marked CS3 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, because call-signaling traffic should not be dropped (if this class is experiencing drops, the bandwidth allocated to it should be re-provisioned). Sample traffic includes Skinny Call Control Protocol (SCCP), Session Initiation Protocol (SIP), H.323, and so on.
- *Operations/administration/management (OAM)*—This service class is intended for network operations, administration, and management traffic. This class is critical to the ongoing maintenance and support of the network. Traffic in this class should be marked CS2 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, because OAM traffic should not be dropped (if this class is experiencing drops, the bandwidth allocated to it should be re-provisioned). Sample traffic includes Secure Shell (SSH), Simple Network Management Protocol (SNMP), Syslog, and so on.
- *Transactional data (or low-latency data)*—This service class is intended for interactive, "foreground" data applications (foreground refers to applications from which users are expecting a response via the network to continue with their tasks; excessive latency directly impacts user productivity). Traffic in this class should be marked AF Class 2 (AF21) and should be provisioned with a dedicated bandwidth queue with DSCP-WRED enabled. This traffic class may be subject to policing and re-marking. Sample applications include data components of multimedia collaboration applications, Enterprise Resource Planning (ERP) applications, Customer Relationship Management (CRM) applications, database applications, and so on.
- *Bulk data (or high-throughput data)*—This service class is intended for non-interactive "background" data applications (background refers to applications from which users are not awaiting a response via the network to continue with their tasks; excessive latency in response times of background applications does not directly impact user productivity). Traffic in this class should be marked AF Class 1 (AF11) and should be provisioned with a dedicated bandwidth queue with DSCP-WRED enabled. This traffic class may be subject to policing and re-marking. Sample applications include E-mail, backup operations, FTP/SFTP transfers, video and content distribution, and so on.
- *Best effort (or default class)*—This service class is the default class. The vast majority of applications will continue to default to this best-effort service class; as such, this default class should be adequately provisioned. Traffic in this class is marked default forwarding (DF or DSCP 0) and should be provisioned with a dedicated queue. WRED is recommended to be enabled on this class.

- *Scavenger (or low-priority data)*—This service class is intended for non-business-related traffic flows, such as data or video applications that are entertainment and/or gaming-oriented. The approach of a less-than Best-Effort service class for non-business applications (as opposed to shutting these down entirely) has proven to be a popular, political compromise. These applications are permitted on enterprise networks, as long as resources are always available for business-critical voice, video, and data applications. However, as soon as the network experiences congestion, this class is the first to be penalized and aggressively dropped. Traffic in this class should be marked CS1 and should be provisioned with a minimal bandwidth queue that is the first to starve should network congestion occur. Sample traffic includes YouTube, Xbox Live/360 movies, iTunes, BitTorrent, and so on.

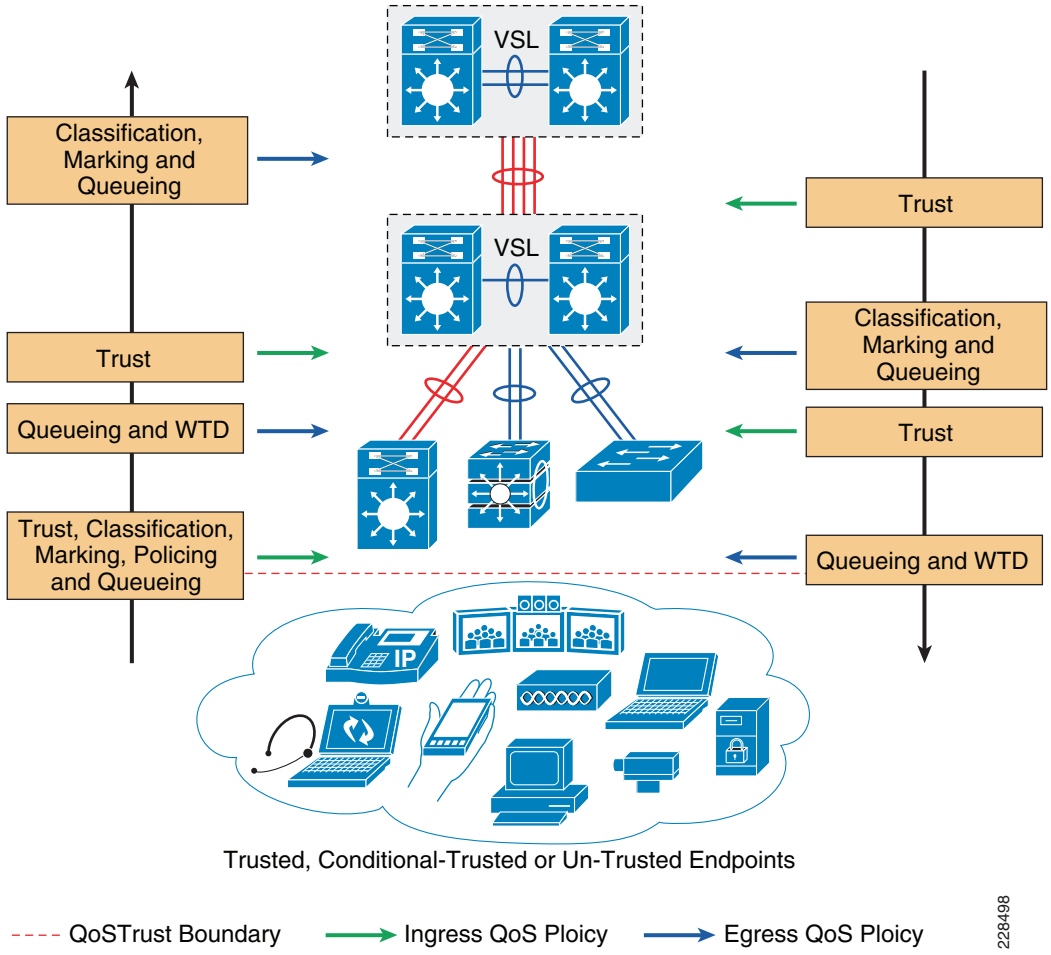
Designing Community College LAN QoS Trust Boundary and Policies

To build an end-to-end QoS framework that offers transparent and consistent QoS service without compromising performance, it is important to create an blueprint of the network, classifying a set of trusted applications, devices, and forwarding paths; and then define common QoS policy settings independent of how QoS is implemented within the system.

QoS settings applied at the LAN network edge sets the ingress rule based on deep packet classification and marks the traffic before it is forwarded inside the campus core. To retain the marking set by access layer switches, it is important that other LAN network devices in the college campus trust the marking and apply the same policy to retain the QoS settings and offer symmetric treatment. Bi-directional network communication between applications, endpoints, or other network devices requires the same treatment when traffic enters or leaves the network, and must be taken into account when designing the trust model between network endpoints and core and edge campus devices.

The trust or un-trust model simplifies the rules for defining bi-directional QoS policy settings. Figure 3-33 shows the QoS trust model setting that sets the QoS implementation guidelines in community college campus networks.

Figure 3-33 Campus QoS Trust and Policies



Community College LAN QoS Best Practices

With an overall application strategy in place, end-to-end QoS policies can be designed for each device and interface, as determined by their roles in the network infrastructure. However, because the Cisco QoS toolset provides many QoS design and deployment options, a few succinct design principles can help simplify strategic QoS deployments, as discussed in the following sections.

Hardware versus Software QoS

A fundamental QoS design principle is to always enable QoS policies in hardware rather than software whenever possible. Cisco IOS routers perform QoS in software, which places incremental loads on the CPU, depending on the complexity and functionality of the policy. Cisco Catalyst switches, on the other hand, perform QoS in dedicated hardware application-specific integrated circuits (ASICs) on Ethernet-based ports, and as such do not tax their main CPUs to administer QoS policies. This allows complex policies to be applied at line rates even up to Gigabit or 10-Gigabit speeds.

Classification and Marking Best Practices

When classifying and marking traffic, a recommended design principle is to classify and mark applications as close to their sources as technically and administratively feasible. This principle promotes end-to-end differentiated services and PHBs.

In general, it is not recommended to trust markings that can be set by users on their PCs or other similar devices, because users can easily abuse provisioned QoS policies if permitted to mark their own traffic. For example, if an EF PHB has been provisioned over the network, a PC user can easily configure all their traffic to be marked to EF, thus hijacking network priority queues to service non-realtime traffic. Such abuse can easily ruin the service quality of realtime applications throughout the college campus. On the other hand, if community college network administrator controls are in place that centrally administer PC QoS markings, it may be possible and advantageous to trust these.

Following this rule, it is recommended to use DSCP markings whenever possible, because these are end-to-end, more granular, and more extensible than Layer 2 markings. Layer 2 markings are lost when the media changes (such as a LAN-to-WAN/VPN edge). There is also less marking granularity at Layer 2. For example, 802.1P supports only three bits (values 0–7), as does Multiprotocol Label Switching Experimental (MPLS EXP). Therefore, only up to eight classes of traffic can be supported at Layer 2, and inter-class relative priority (such as RFC 2597 Assured Forwarding Drop Preference markdown) is not supported. Layer 3-based DSCP markings allow for up to 64 classes of traffic, which provides more flexibility and is adequate in large-scale deployments and for future requirements.

As the network border blurs between enterprise and education community network and service providers, the need for interoperability and complementary QoS markings is critical. Cisco recommends following the IETF standards-based DSCP PHB markings to ensure interoperability and future expansion. Because the community college voice, video, and data applications marking recommendations are standards-based, as previously discussed, community colleges can easily adopt these markings to interface with service provider classes of service.

Policing and Markdown Best Practices

There is little reason to forward unwanted traffic that gets policed and drop by a subsequent tier node, especially when unwanted traffic is the result of DoS or worm attacks in the college network. Excessive volume attack traffic can destabilize network systems, which can result in outages. Cisco recommends policing traffic flows as close to their sources as possible. This principle applies also to legitimate flows, because worm-generated traffic can masquerade under legitimate, well-known TCP/UDP ports and cause extreme amounts of traffic to be poured into the network infrastructure. Such excesses should be monitored at the source and marked down appropriately.

Whenever supported, markdown should be done according to standards-based rules, such as RFC 2597 (AF PHB). For example, excess traffic marked to AFx1 should be marked down to AFx2 (or AFx3 whenever dual-rate policing such as defined in RFC 2698 is supported). Following such markdowns, congestion management policies, such as DSCP-based WRED, should be configured to drop AFx3 more aggressively than AFx2, which in turn should be dropped more aggressively than AFx1.

Queuing and Dropping Best Practices

Critical media applications require uncompromised performance and service guarantees regardless of network conditions. Enabling outbound queueing in each network tier provides end-to-end service guarantees during potential network congestion. This common principle applies to campus-to-WAN/Internet edges, where speed mismatches are most pronounced; and campus interswitch links, where oversubscription ratios create the greater potential for network congestion.

Because each application class has unique service level requirements, each should be assigned optimally a dedicated queue. A wide range of platforms in varying roles exist in community college networks, so each must be bounded by a limited number of hardware or service provider queues. No fewer than four queues are required to support QoS policies for various types of applications, specifically as follows:

- Realtime queue (to support a RFC 3246 EF PHB service)
- Guaranteed-bandwidth queue (to support RFC 2597 AF PHB services)
- Default queue (to support a RFC 2474 DF service)
- Bandwidth-constrained queue (to support a RFC 3662 scavenger service)

Additional queuing recommendations for these classes are discussed next.

Strict-Priority Queuing Recommendations

The realtime or strict priority class corresponds to the RFC 3246 EF PHB. The amount of bandwidth assigned to the realtime queuing class is variable. However, if the majority of bandwidth is provisioned with strict priority queuing (which is effectively a FIFO queue), the overall effect is a dampening of QoS functionality, both for latency- and jitter-sensitive realtime applications (contending with each other within the FIFO priority queue), and also for non-realtime applications (because these may periodically receive significant bandwidth allocation fluctuations, depending on the instantaneous amount of traffic being serviced by the priority queue). Remember that the goal of convergence is to enable voice, video, and data applications to transparently co-exist on a single community college network infrastructure. When realtime applications dominate a link, non-realtime applications fluctuate significantly in their response times, destroying the transparency of the converged network.

For example, consider a 45 Mbps DS3 link configured to support two Cisco TelePresence CTS-3000 calls with an EF PHB service. Assuming that both systems are configured to support full high definition, each such call requires 15 Mbps of strict-priority queuing. Before the TelePresence calls are placed, non-realtime applications have access to 100 percent of the bandwidth on the link; to simplify the example, assume there are no other realtime applications on this link. However, after these TelePresence calls are established, all non-realtime applications are suddenly contending for less than 33 percent of the link. TCP windowing takes effect and many applications hang, timeout, or become stuck in a non-responsive state, which usually translates into users calling the IT help desk to complain about the network (which happens to be functioning properly, albeit in a poorly-configured manner).

Note As previously discussed, Cisco IOS software allows the abstraction (and thus configuration) of multiple strict priority LLQs. In such a multiple LLQ context, this design principle applies to the sum of all LLQs to be within one-third of link capacity.

It is vitally important to understand that this strict priority queuing rule is simply a best practice design recommendation and is not a mandate. There may be cases where specific business objectives cannot be met while holding to this recommendation. In such cases, the community college network administrator must provision according to their detailed requirements and constraints. However, it is important to recognize the tradeoffs involved with over-provisioning strict priority traffic and its negative performance impact, both on other realtime flows and also on non-realtime-application response times.

And finally, any traffic assigned to a strict-priority queue should be governed by an admission control mechanism.

Best Effort Queuing Recommendation

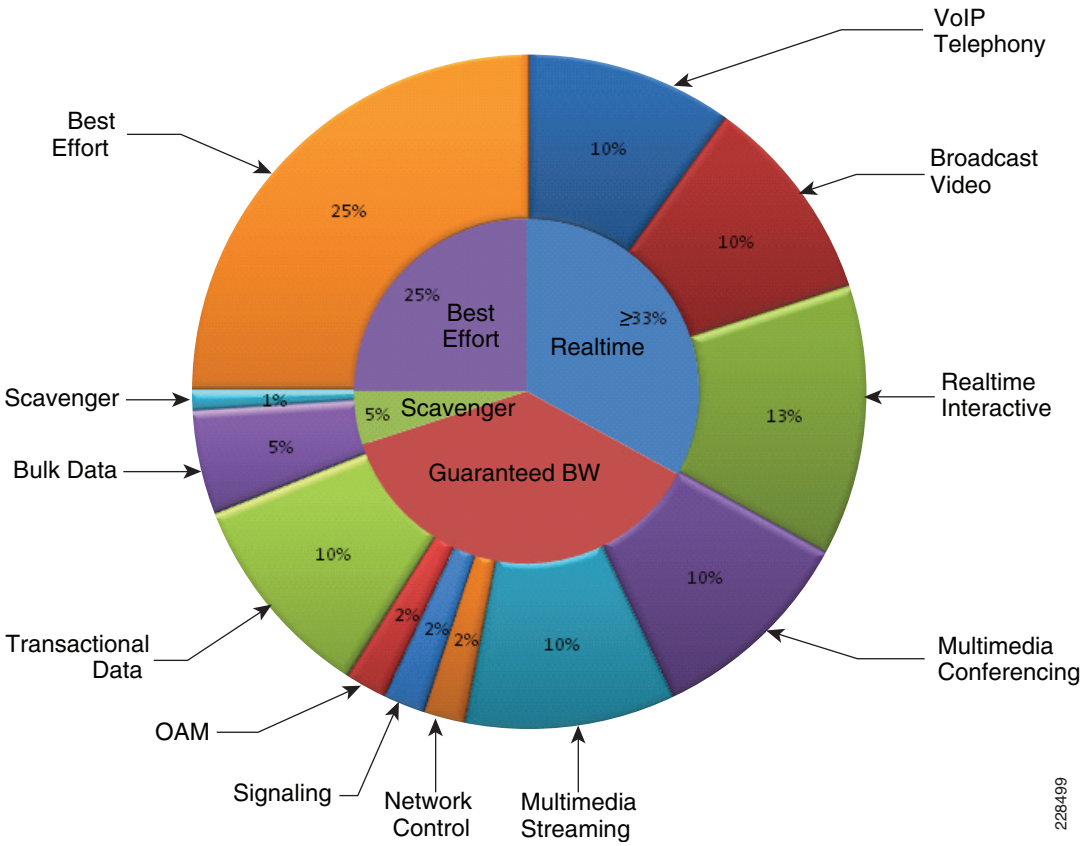
The best effort class is the default class for all traffic that has not been explicitly assigned to another application-class queue. Only if an application has been selected for preferential/deferential treatment is it removed from the default class. Because most community colleges may have several types of applications running in networks, adequate bandwidth must be provisioned for this class as a whole to handle the number and volume of applications that default to it. Therefore, Cisco recommends reserving at least 25 percent of link bandwidth for the default best effort class.

Scavenger Class Queuing Recommendations

Whenever the scavenger queuing class is enabled, it should be assigned a minimal amount of link bandwidth capacity, such as 1 percent, or whatever the minimal bandwidth allocation that the platform supports. On some platforms, queuing distinctions between bulk data and scavenger traffic flows cannot be made, either because queuing assignments are determined by class of service (CoS) values (and both of these application classes share the same CoS value of 1), or because only a limited amount of hardware queues exist, precluding the use of separate dedicated queues for each of these two classes. In such cases, the scavenger/bulk queue can be assigned a moderate amount of bandwidth, such as 5 percent.

These queuing rules are summarized in Figure 3-34, where the inner pie chart represents a hardware or service provider queuing model that is limited to four queues and the outer pie chart represents a corresponding, more granular queuing model that is not bound by such constraints.

Figure 3-34 Compatible 4-Class and 12-Class Queuing Models



High-Availability in LAN Network Design

Network reliability and availability is not a new demand, but is well planned during the early network design phase. To prevent a catastrophic network failure during an unplanned network outage event, it is important to identify network fault domains and define rapid recovery plans to minimize the application impact during minor and major network outage conditions.

Because every tier of the LAN network design can be classified as a fault domain, deploying redundant systems can be effective. However, this introduces a new set of challenges, such as higher cost and the added complexity of managing more systems. Network reliability and availability can be simplified using several Cisco high availability technologies that offer complete failure transparency to the end users and applications during planned or unplanned network outages.

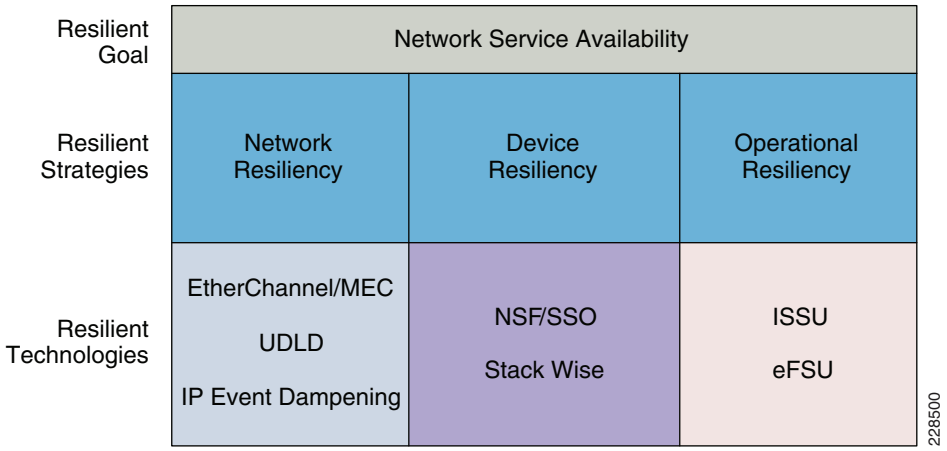
Cisco high availability technologies can be deployed based on critical versus non-critical platform roles in the network. Some of the high availability techniques can be achieved with the LAN network design inherent within the community college network design, without making major network changes. However, the critical network systems that are deployed in the main campus that provide global connectivity may require additional hardware and software components to provide non-stop communications. The following three major resiliency requirements encompass most of the common types of failure conditions; depending on the LAN design tier, the resiliency option appropriate to the role and network service type must be deployed:

- *Network resiliency*—Provides redundancy during physical link failures, such as fiber cut, bad transceivers, incorrect cablings, and so on.
- *Device resiliency*—Protects the network during abnormal node failure triggered by hardware or software, such as software crashes, a non-responsive supervisor, and so on.
- *Operational resiliency*—Enables resiliency capabilities to the next level, providing complete network availability even during planned network outage conditions, using In Service Software Upgrade (ISSU) features.

Community College LAN Design High-Availability Framework

This high availability framework is based on the three major resiliency strategies described in the previous section. Several high availability technologies must be deployed at each layer to provide higher network availability and rapid recovery during failure conditions, to prevent communication failure or degraded network-wide application performance. (See Figure 3-35.)

Figure 3-35 Community College LAN Design High-Availability Goals, Strategy, and Technologies



Network Resiliency Best Practices

The most common network fault occurrence in the LAN network is a link failure between two systems. Link failures can be caused by issues such as a fiber cut, miswiring, and so on. Redundant parallel physical links between two systems can increase availability, but also change how overall higher layer protocols construct the adjacency and loop-free forwarding topology to the parallel physical paths.

Deploying redundant parallel paths in the recommended community college LAN design by default develops a non-optimal topology that keeps the network under-utilized and requires protocol-based network recovery. In the same network design, the routed access model eliminates such limitations and enables the full load balancing capabilities to increase bandwidth capacity and minimize the application impact during a single path failure. To develop a consistent network resiliency service in the centralized main and remote college campus sites, the following basic principles apply:

- Deploying redundant parallel paths are the basic requirement to employ network resiliency at any tier. It is critical to simplify the control plane and forwarding plane operation by bundling all physical paths into a single logical bundled interface (EtherChannel). Implement a defense-in-depth approach to failure detection and recovery mechanisms. An example of this is configuring the UniDirectional Link Detection (UDLD) protocol, which uses a Layer 2 keep-alive to test that the switch-to-switch links are connected and operating correctly, and acts as a backup to the native Layer 1 unidirectional link detection capabilities provided by 802.3z and 802.3ae standards. UDLD is not an EtherChannel function; it operates independently over each individual physical port at Layer 2 and remains transparent to the rest of the port configuration. Therefore, UDLD can be deployed on ports implemented in Layer 2 or Layer 3 modes.
- Ensure that the design is self-stabilizing. Hardware or software errors may cause ports to flap, which creates false alarms and destabilizes the network topology. Implementing route summarization advertises a concise topology view to the network, which prevents core network instability. However, within the summarized boundary, the flood may not be protected. Deploy IP event dampening as an tool to prevent the control and forwarding plane impact caused by physical topology instability.

These principles are intended to be a complementary part of the overall structured modular design approach to the campus design, and serve primarily to reinforce good resilient design practices.

Device Resiliency Best Practices

Another major component of an overall campus high availability framework is providing device or node level protection that can be triggered during any type of abnormal internal hardware or software process within the system. Some of the common internal failures are a software-triggered crash, power outages, line card failures, and so on. LAN network devices can be considered as a single-point-of-failure and are considered to be major failure condition because the recovery type may require a network administrator to mitigate the failure and recover the system. The network recovery time can remain undeterministic, causing complete or partial network outage, depending on the network design.

Redundant hardware components for device resiliency vary between fixed configuration and modular Cisco Catalyst switches. To protect against common network faults or resets, all critical community college campus network devices must be deployed with a similar device resiliency configuration. This subsection provides basic redundant hardware deployment guidelines at the access layer and collapsed core switching platforms in the campus network.

Redundant Power System

Redundant power supplies for network systems protect against power outages, power supply failures, and so on. It is important not only to protect the internal network system but also the endpoints that rely on power delivery over the Ethernet network. Redundant power systems can be deployed in the two following configuration modes:

- *Modular switch*—Dual power supplies can be deployed in modular switching platforms such as the Cisco Catalyst 6500 and 4500-E Series platforms. By default, the power supply operates in redundant mode, offering the 1+1 redundant option. Overall power capacity planning must be done to dynamically allow for network growth. Lower power supplies can be combined to allocate power to all internal and external resources, but may not be able to offer power redundancy.
- *Fixed configuration switch*—The power supply in fixed configuration switches can be internal or use Cisco RPS 2300 external power supplies. A single Cisco RPS 2300 power supply uses a modular power supply and fan for flexibility, and can deliver power to multiple switches. Deploying an internal and external power supply solution protects critical access layer switches during power outages, and provides completes fault transparency and constant network availability.

Redundant Control Plane

Device or node resiliency in modular Cisco Catalyst 6500/4500 platforms and Cisco StackWise provides a 1+1 redundancy option with enterprise-class high availability and deterministic network recovery time. The following sub-sections provide high availability design details, as well as graceful network recovery techniques that do not impact the control plane and provide constant forwarding capabilities during failure events.

Stateful Switchover

The stateful switchover (SSO) capability in modular switching platforms such as the Cisco Catalyst 4500 and 6500 provides complete carrier-class high availability in the campus network. Cisco recommends distribution and core layer design model be the center point of the entire college communication network. Deploying redundant supervisors in the mission-critical distribution and core system provides non-stop communication throughout the network. To provide 99.999 percent service availability in the access layer, the Catalyst 4500 must be equipped with redundant supervisors to critical endpoints, such as Cisco TelePresence.

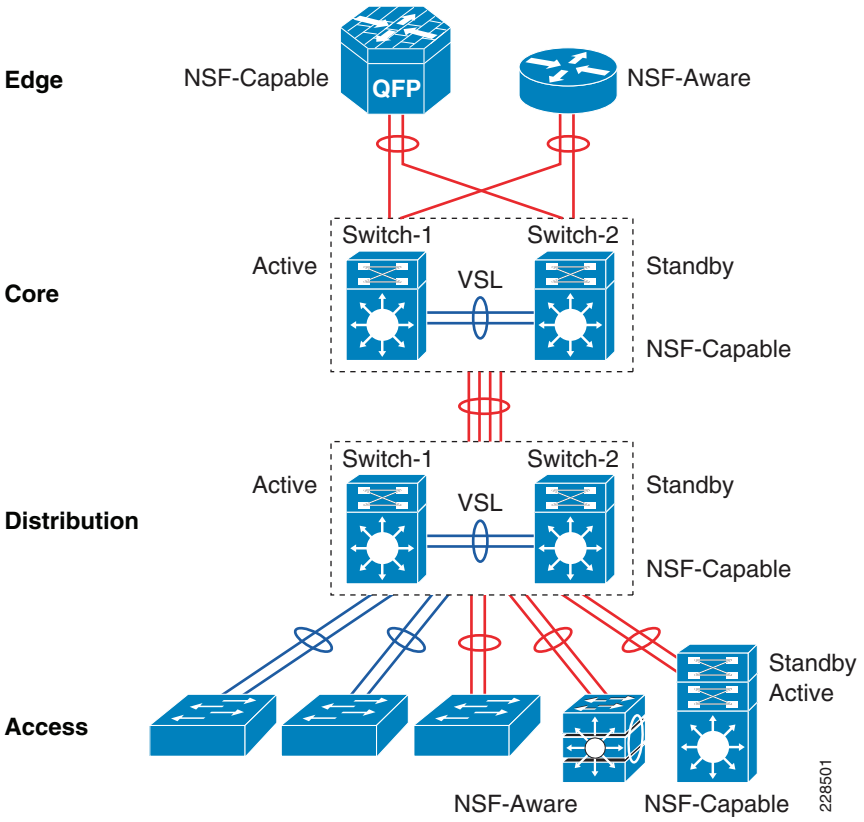
Cisco StackWise is an low-cost solution to provide device-level high availability. Cisco StackWise is designed with unique hardware and software capabilities that distribute, synchronize, and protect common forwarding information across all member switches in a stack ring. During master switch failure, the new master switch re-election remains transparent to the network devices and endpoints. Deploying Cisco StackWise according to the recommended guidelines protects against network interruption, and recovers the network in sub-seconds during master switch re-election.

Bundling SSO with NSF capability and the awareness function allows the network to operate without errors during a primary supervisor module failure. Users of realtime applications such as VoIP do not hang up the phone, and IP video surveillance cameras do not freeze.

Non-Stop Forwarding

Cisco VSS and the single highly resilient-based campus system provides uninterrupted network availability using non-stop forwarding (NSF) without impacting end-to-end application performance. The Cisco VSS and redundant supervisor system is an NSF-capable platform; thus, every network device that connects to VSS or the redundant supervisor system must be NSF-aware to provide optimal resiliency. By default, most Cisco Layer 3 network devices are NSF-aware systems that operate in NSF helper mode for graceful network recovery. (See Figure 3-36.)

Figure 3-36 Community College LAN Design NSF/SSO Capable and Aware Systems



Operational Resiliency Best Practices

Designing the network to recover from failure events is only one aspect of the overall campus non-stop design. Converged network environments are continuing to move toward requiring true 7x24x365 availability. The community college LAN network is part of the backbone of the college network and must be designed to enable standard operational processes, configuration changes, and software and hardware upgrades without disrupting network services.

The ability to make changes, upgrade software, and replace or upgrade hardware becomes challenging without a redundant system in the campus core. The ability to upgrade individual devices without taking them out of service is similarly based on having internal component redundancy (such as with power supplies and supervisors), complemented with the system software capabilities. The Cisco Catalyst 4500 and 6500 support realtime upgrade software in the campus.

Catalyst 4500—ISSU

Full-image ISSU on the Cisco Catalyst 4500 leverages dual supervisors to allow for a full, in-place Cisco IOS upgrade, such as moving from 12.2(50)SG to 12.2(53)SG for example. This leverages the NSF/SSO capabilities of the switch and provides for less than 200 msec of traffic loss during a full Cisco IOS upgrade.

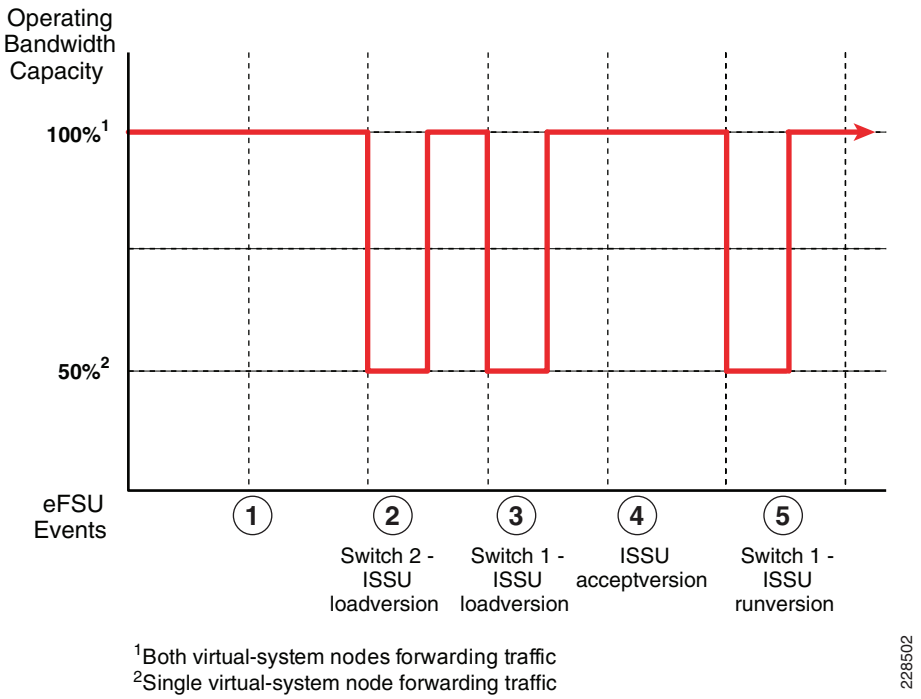
Having the ability to operate the campus as a non-stop system depends on the appropriate capabilities being designed-in from the start. Network and device level redundancy, along with the necessary software control mechanisms, guarantee controlled and fast recovery of all data flows following any network failure, while concurrently providing the ability to proactively manage the non-stop infrastructure.

Catalyst 6500 VSS—eFSU

A network upgrade requires planned network and system downtime. VSS offers unmatched network availability to the core. With the Enhanced Fast Software Upgrade (eFSU) feature, the VSS can continue to provide network services during the upgrade. With the eFSU feature, the VSS network upgrade remains transparent and hitless to the applications and end users (see Figure 3-37). Because eFSU works in conjunction with NSF/SSO technology, the network devices can gracefully restore control and forwarding information during the upgrade process, while the bandwidth capacity operates at 50 percent and the data plane can converge within sub-seconds.

For a hitless software update, the ISSU process requires three sequential upgrade events for error-free software install on both virtual switch systems. Each upgrade event causes traffic to be re-routed to a redundant MEC path, causing sub-second traffic loss that does not impact realtime network applications, such as VoIP.

Figure 3-37 Real-time Network Upgrade Events and Availability



Summary

Designing the LAN network aspects for the community college network design establishes the foundation for all other aspects within the service fabric (WAN, security, mobility, and UC) as well as laying the foundation to provide safety and security, operational efficiencies, virtual learning environments, and secure classrooms.

This chapter reviews the two LAN design models recommended by Cisco, as well as where to apply these models within the various locations of a community college network. Each of the layers is discussed and design guidance is provided on where to place and how to deploy these layers. Finally, key network foundation services such as routing, switching, QoS, multicast, and high availability best practices are given for the entire community college design.

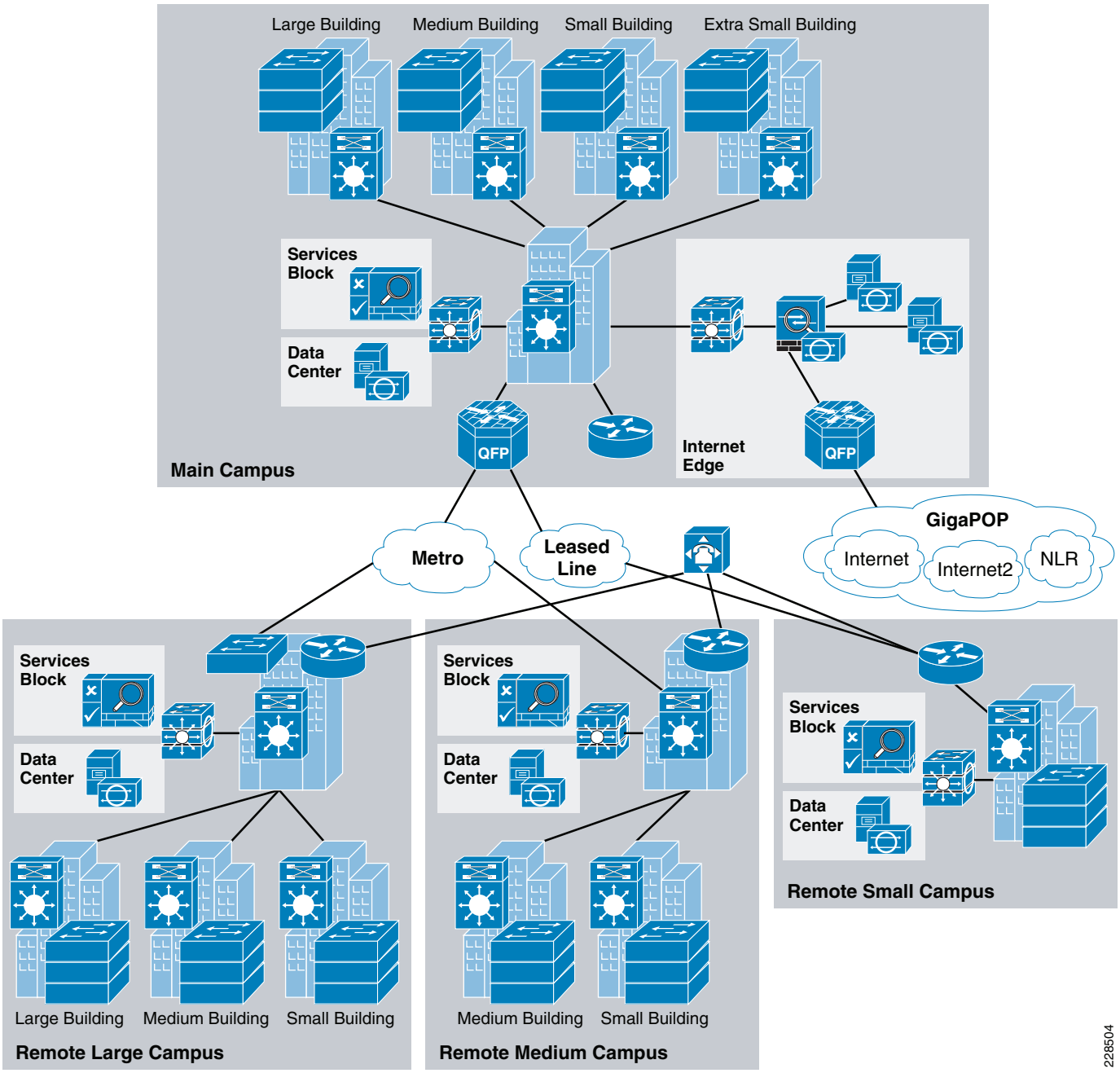
CHAPTER 4

Community College WAN Design Considerations

WAN Design

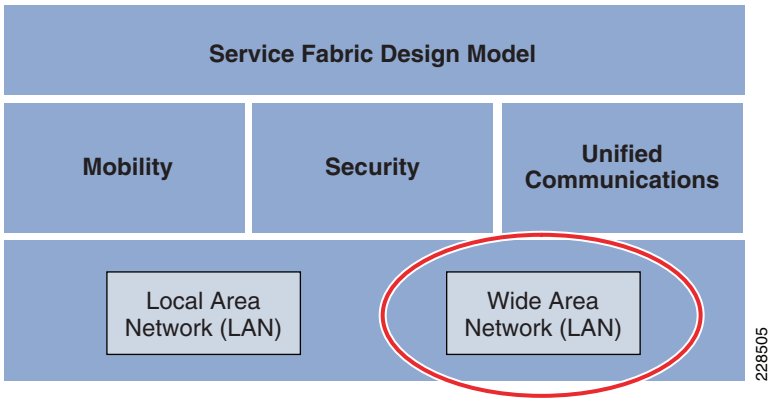
The Cisco Community College reference design is a multi-campus design where a campus consists of multiple buildings and services. The campuses are interconnected through various WAN transports as shown in Figure 4-1.

Figure 4-1 Community College WAN Design Diagram



Within the Community College reference design, the service fabric network provides the foundation on which all the solutions and services are built upon to solve the business challenges facing community colleges. These challenges include virtual learning, secure connected classrooms, and safety and security. This service fabric consists of four distinct components as shown in Figure 4-2.

Figure 4-2 The Service Fabric Design Model



This chapter discusses the WAN design component of the community college service fabric design. This section discusses how the WAN design is planned for community colleges, the assumptions made, the platforms chosen, and the justification for choosing a platform. The WAN design is highly critical to provide network access for remote campus locations to the main campus site, as well as connectivity between community colleges, and general Internet access for the entire college. The WAN design should not be viewed merely for providing access, but mainly to see how the business requirements can be met. In today's collaborative learning environment, it is important for communication to exist between students and teachers. This communication could be with voice, video, or data applications. Moreover, the video applications, may possess, flavors ranging from desktop video to real-time video. To provide this collaborative environment, highly resilient and, highly performing WAN designs are required.

The main components of Community College WAN design are as follows:

- WAN transport
- WAN devices
- Network Foundation services—Routing, QoS, and multicast

WAN Transport

This section discusses the different WAN transports present in the community college.

Private WAN Service

One of the main requirements for community colleges is the ability to collaborate with other colleges within North America and globally. To achieve the inter connectivity between the colleges, the network should be connected to certain providers, such as Lambda rail, Internet2. The community colleges need to connect to Gigapops—regional networks, which provide access to these private WAN networks. The following sections provide a brief description on these two network types:

Internet2 is a not-for-profit advanced networking consortium comprising more than 200 U.S. universities in cooperation with 70 leading corporations, 45 government agencies, laboratories, and other institutions of higher learning as well over 50 international partner organizations. Internet2 provides its members both leading-edge network capabilities and unique partnership opportunities that together facilitate the development, deployment and use of revolutionary Internet technologies. The Internet2 network's physical implementation is comprised of an advanced IP network, virtual circuit network and core optical network. It provides the necessary scalability for member institutions to

efficiently provision resources to address bandwidth-intensive requirements of their campuses such as, collaborative applications, distributed research experiments, grid-based data analysis and social networking. For more information on the Internet2 network, refer to the following URL:

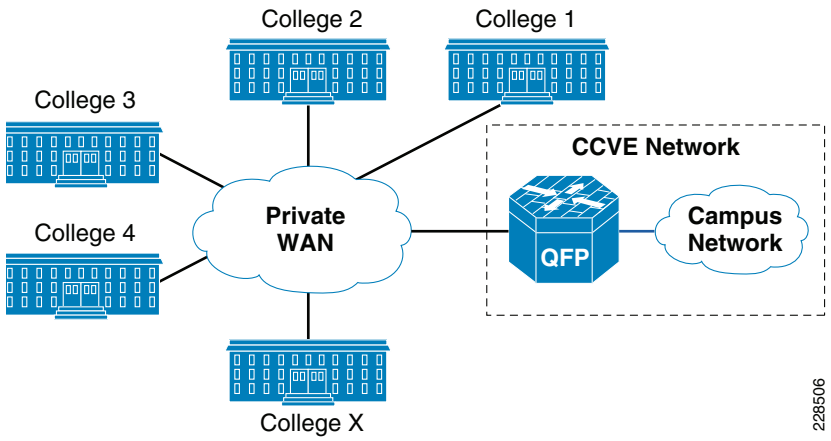
http://www.internet2.edu/network/

National LambdaRail (NLR) is a high-speed, fiber-optic network infrastructure linking over 30 cities in 21 states. It is owned by the U.S. research and education community and is dedicated to serving the needs of researchers and research groups. NLR's high-performance network backbone offers unrestricted usage and bandwidth, a choice of cutting-edge network services and applications, and customized service for individual researchers and projects. NLR services include high-capacity 10Gb Ethernet LAN-PHY or OC-192 lambdas, point-to-point or multipoint Ethernet-based transport, routed IP-based services, and TelePresence video-conference services. For more information on the NLR network and its services, refer to the following URL:

http://www.nlr.net/

This design assumes that community colleges are connected to one of these networks using either Layer 2 or Layer 3 networks for WAN connectivity, using WAN speeds of 100Mbs. The physical connection is assumed to be one connection to the service provider, but there will be two logical connections—one for accessing private networks, and the second one for Internet access. Figure 4-3 depicts how community college would connect to different colleges, universities, and research networks using either NLR or Internet2 service.

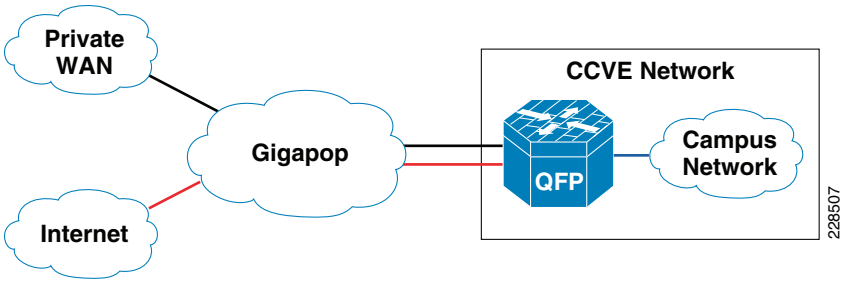
Figure 4-3 Community College Connection to Other Colleges Using Private WAN



Internet Service

The physical connection for reaching the Internet and the private WAN network is same; however, both circuits are logically separated using different sub-interfaces. Therefore, it is similar to a situation where a customer is connected to different service providers. See Figure 4-4.

Figure 4-4 Community College Internet Service



Metro Service

Metro Ethernet is one of the fastest growing WAN transport technologies in the telecommunications industry. The advantages of using this WAN transport are as follows:

- Scalability and reachability
  - The services offered would scale from 1Mbps to 10Gbps, and beyond in granular increments, which makes this transport highly scalable.
  - Service providers worldwide are migrating their networks to provide metro services; thereby, it is available at large number of places.
- Performance, QoS, and suitability for convergence
  - Inherently Ethernet networks require less processing to operate and manage and operate at higher bandwidth than other technologies.
  - The granular options in bandwidth, ability to provide different SLA based on voice, video, and data applications that provide QoS service to customers.
  - Low latency and delay variation make it the best solution for video, voice, and data.
- Cost savings
  - Metro Ethernet brings the cost model of Ethernet to the WAN.
- Expediting and enabling new applications
  - Accelerates implementations with reduced resources for overburdened IT departments.
  - Enables new applications requiring high bandwidth, and low latency that were previously not possible or prohibited by high cost.

There are two popular methods of service for Metro Ethernet:

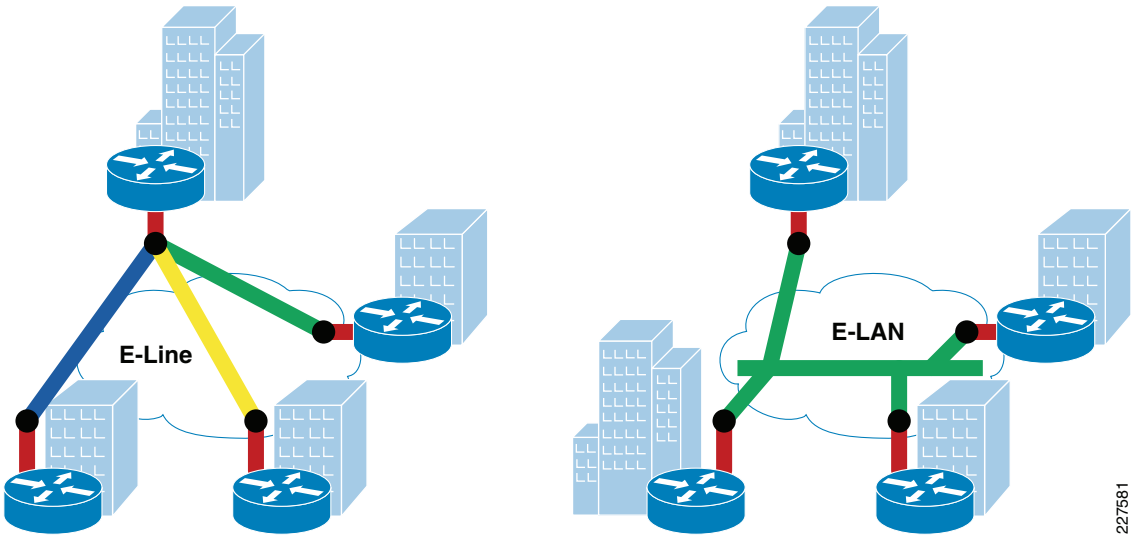
1. E-line, which is also known as Ethernet Virtual Private Line (EVPL) provides a point-to-point service.
2. E-LAN which provides multipoint or any-to-any connectivity.

EVPL, like Frame Relay, provides for multiplexing multiple point-to-point connections over a single physical link. In the case of Frame Relay, the access link is a serial interface to a Frame Relay switch with individual data-link connection identifiers (DLCIs), identifying the multiple virtual circuits or connections. In the case of EVPL, the physical link is Ethernet, typically FastEthernet or Gigabit Ethernet, and the multiple circuits are identified as VLANs by way of an 802.1q trunk.

E-LAN, also known as Virtual Private LAN Services (VPLS), provides any-to-any connectivity within the Metro area, which allows flexibility. It passes 802.q trunks across the SP network known as Q-in-Q.

Figure 4-5 shows the difference between these services.

Figure 4-5 Different Services Available

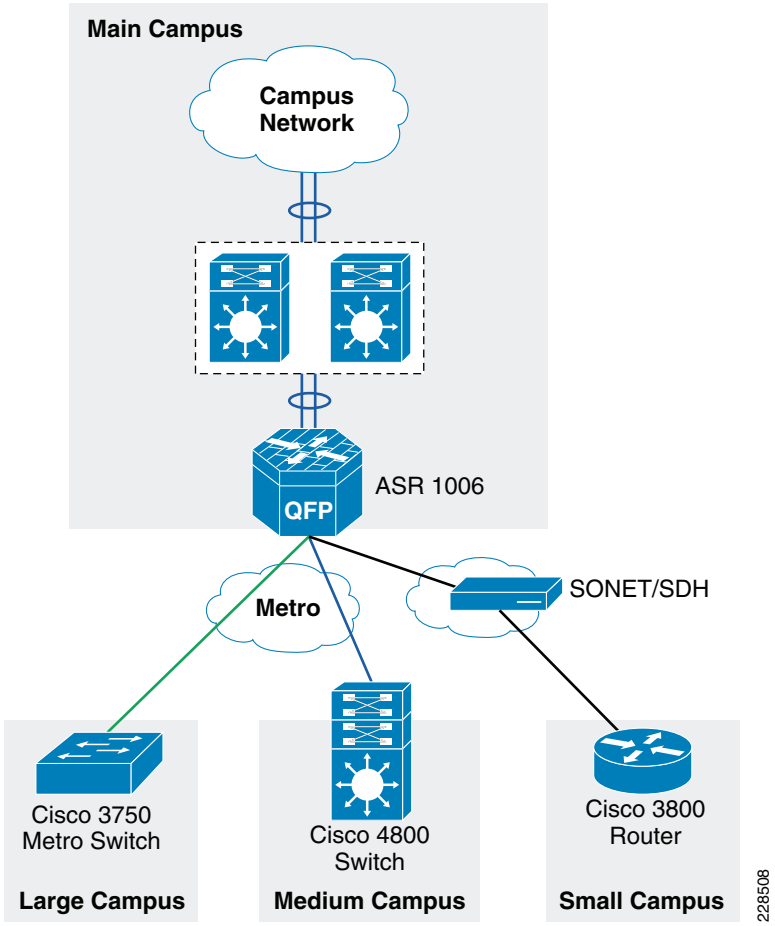


This section discusses how the Metro service is designed in the Community College reference design. The Metro service is used to provide connectivity between the remote campuses to the main campus site. The key reasons for recommending Metro service for community college are as follows:

- *Centralized administration and management*—E-line service provides point-to-point connectivity, where as, E-LAN provides point-to-multipoint connectivity. Having a point-to-point connectivity mandates that all the remote campus sites need to traverse the main campus site to reach the other, making the centralized administration applicable.
- *Performance*—Since all the application services are centrally located at main campus site, the WAN bandwidth required for remote campus sites to main campus site should be at least 100 Mbps. The Metro transport can provide 100Mbps, and more if needed in the future.

Therefore, in this design, it is recommended that the remote large and remote medium campus locations use E-line service to connect to the main campus site. Figure 4-6 shows how the remote campus locations are connected to main campus site using Metro service.

Figure 4-6 The Metro Transport Deployment in Community College WAN Design



Leased-Line Service

The WAN bandwidth requirement for a small remote site is assumed to be 20Mbps. Cisco recommends that the remote small campus site connect to the main campus site using a private leased-line service. The leased-line service is more readily available for these type of locations and the bandwidth is sufficient for the remote small campus application requirements.

WAN Aggregation Platform Selection in the Community College Reference Design

In addition to selecting the WAN service for connectivity between college campus locations and access to the Internet, choosing the appropriate WAN aggregation router is essential. For each location in the Community College reference design, various WAN aggregation platforms are selected based on the requirements.

Main Campus WAN Aggregation Platform Selection

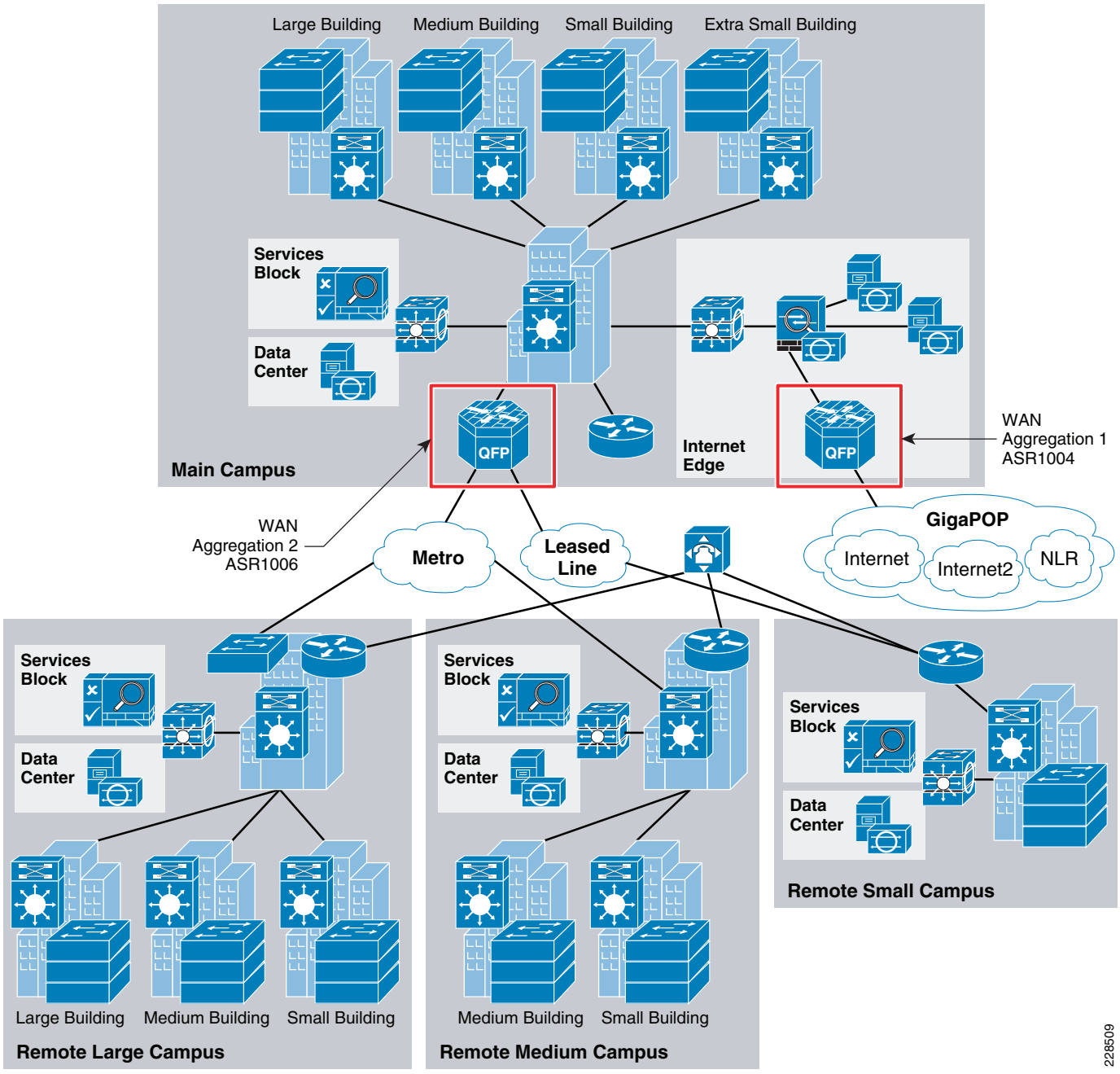
A WAN aggregation router aggregates all the incoming WAN circuits from various locations in the network as well as the Internet and also provides the proper QoS required for application delivery. Cisco recommends the Cisco ASR family of routers as the WAN aggregation platform for the main campus location.

The Cisco ASR 1000 Series Router family consists of three different models:

- The Cisco ASR 1002 Router is a 3-SPA, 2-rack-unit (RU) chassis with one Embedded Services Processor (ESP) slot that comes with an integrated Router Processor (RP), integrated Cisco ASR 1000 Series Shared Port Adapter Interface Processor (SIP), and integrated four Gigabit Ethernet ports.
- The Cisco ASR 1004 Router is an 8-SPA, 4-RU chassis with one ESP slot, one RP slot, and two SIP slots.
- The Cisco ASR 1006 Router is a 12-SPA, 6-RU, hardware redundant chassis with two ESP slots, two RP slots and three SIP slots.

In community college WAN design, there are two places where the WAN aggregation occurs in the main campus location. The first place is where the main campus location connects to outside world using private WAN and Internet networks. The second place is where all the remote campus locations connect to the main campus sites. Figure 4-7 shows the two different WAN aggregation devices.

Figure 4-7 The WAN Aggregation Points in Community College



WAN Aggregation 1

Cisco ASR 1004 Series router is recommended as WAN aggregation platform for private WAN/Internet connectivity. This choice was made considering the cost and required features—performance, QoS, routing, and resiliency, which are essential requirements for WAN aggregation router. Moreover, this platform contains built-in resiliency capabilities such as ISSU and IOS-based redundancy.

WAN Aggregation 2

The second WAN aggregation device provides connectivity to the large and medium remote community college campuses. To perform this aggregation, the Cisco ASR 1006 router with redundant route processors and redundant ESP's has been recommended for the following reasons:

- *Performance*—Up to 20 Gbps throughput
- *Port density*—Up to 12 shared port adapters (SPAs), the highest port density solution of the three Cisco ASR 1000 routers
- *Resiliency*—Cisco ASR 1006 router supports hardware redundancy and in-service software upgrades (ISSU). This chassis would support dual route processors, and dual ESP modules to support the hardware redundancy. Moreover, this router would also support EtherChannel load balancing feature.

Remote Large Campus WAN Aggregation Platform Selection

The WAN connectivity between the large remote campus sites to the main campus site is fairly simpler because of the lack of requirements of advanced encryption technologies. Therefore, the main idea is to reduce the cost and try to consolidate the WAN functionality into the distribution device at the large campus site. However, at the large campus site, as per the campus LAN design document VSS has been chosen as distribution switch, and it does not support WAN functionality. Therefore, a dedicated WAN aggregation device needed to perform that functionality, and the choice can be an ASR, 7200, or 3750ME switches. Out of these choices, considering the cost/performance criteria, the Cisco 3750ME switch was selected to perform the WAN aggregation. The Cisco 3750 Metro switch has the following features/capabilities to adequately meet the requirements:

- Hierarchical QoS
- Routing support: OSPF, EIGRP, BGP
- Multicast support: PIM
- Redundant power supply

Remote Medium Campus WAN Aggregation Platform Selection

As discussed in Chapter 3, "Community College LAN Design Considerations," the remote medium campus collapses the WAN edge and core-layer LAN functionality into a single switch to provide cost effectiveness to meet the budget needs for this size location. The remote medium campus location is connected to the main campus location through Metro service. At the remote medium campus location, the WAN and LAN aggregation platform is the Cisco Catalyst 4507 switch. This switch has necessary features to perform as WAN router. However, if there is the need for advanced WAN features such as MPLS, the Cisco Catalyst 3750 ME or Cisco ISR Series router or upgrading to the Cisco Catalyst 6500 series could be explored as an option. For this design, the Cisco Catalyst 4500 Series switches has been chosen to perform the dual functionality as WAN router, in addition to its role as core-layer LAN switch.

Remote Small Campus WAN Aggregation Platform Selection

The remote small campus is connected to main campus using a private leased-line service. The WAN speed between the remote small campus and the main campus location is assumed to be around 20Mbps, and this service is provided by a traditional leased line. Since it is a leased-line circuit, WAN devices such as Cisco 3750 Metro or 4507 switch can not be used. Therefore, an integrated services router is needed to meet the requirement. For this reason, the Cisco 3845 Series router is chosen as WAN platform for remote small campus. The main advantages of using the Cisco 3845 Series router are as follows:

- Enhanced Network Module Slot
- Support for over 90 existing and new modules
- Voice Features: Analog and digital voice call support and optional voice mail support
- Support for majority of existing AIMs, NMs, WICs, VWICs, and VICs
- Integrated GE ports with copper and fiber support

Network Foundation Services

The key network foundation services are as follows:

- Routing
- QoS
- Resiliency
- Multicast

Routing Design

This section discusses how routing is designed in Community College reference WAN design. As indicated in the WAN transport design, the Community College reference design has multiple transports—NLR or I2 networks, Internet, Metro Service, and leased-line services. The NLR or I2 networks would provide access to reach other community colleges, universities, and research networks globally. Internet service would help the Community College to reach Internet. Metro/leased-line service would help to connect remote campus locations to the main campus. To provide connectivity using these transport services we have designed two distinct routing domains – external and internal. The external routing domain is where the Community College would connect with external autonomous system, and the internal routing domain is where the entire routing domain is within single autonomous system. The following section would discuss about the external routing domain design, and the internal routing domain design.

External Routing Domain

As indicated above, the external routing domain would connect with different service providers, NLR or I2, and the Internet service. This is applicable only to the WAN aggregation router 1, which interfaces with both NLR or I2, and the Internet service, because it the only router which interfaces with the external domain.

The main design considerations for routing for the Internet/private WAN edge router are as follows:

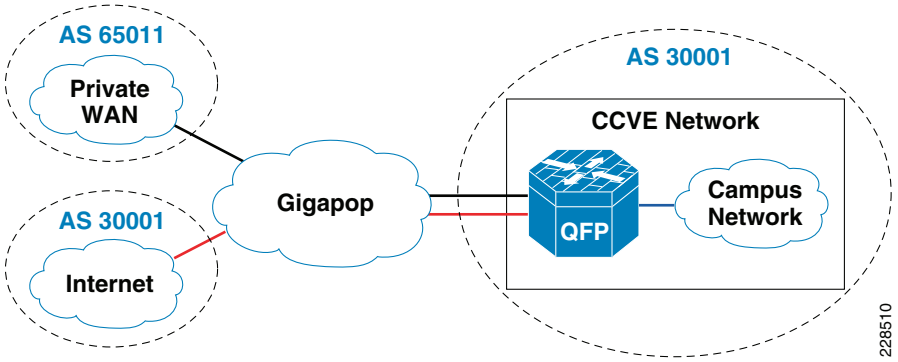
- Scale up to large number of routes
- Support for multi-homing—connection to different service providers
- Ability to implement complex polices—Have separate policies for incoming and outgoing traffic

To meet the above requirements, BGP has been chosen as the routing protocol because of the following reasons:

- *Scalability*—BGP is far superior when routing table entries is quite large.

- *Complex policies*—IGP protocol is better in environments where the neighbors are trusted, whereas when dealing with different service providers' complex policies are needed to deal with incoming entries, and outgoing entries. BGP supports having different policies for incoming and outgoing prefixes. Figure 4-8 shows the BGP design.

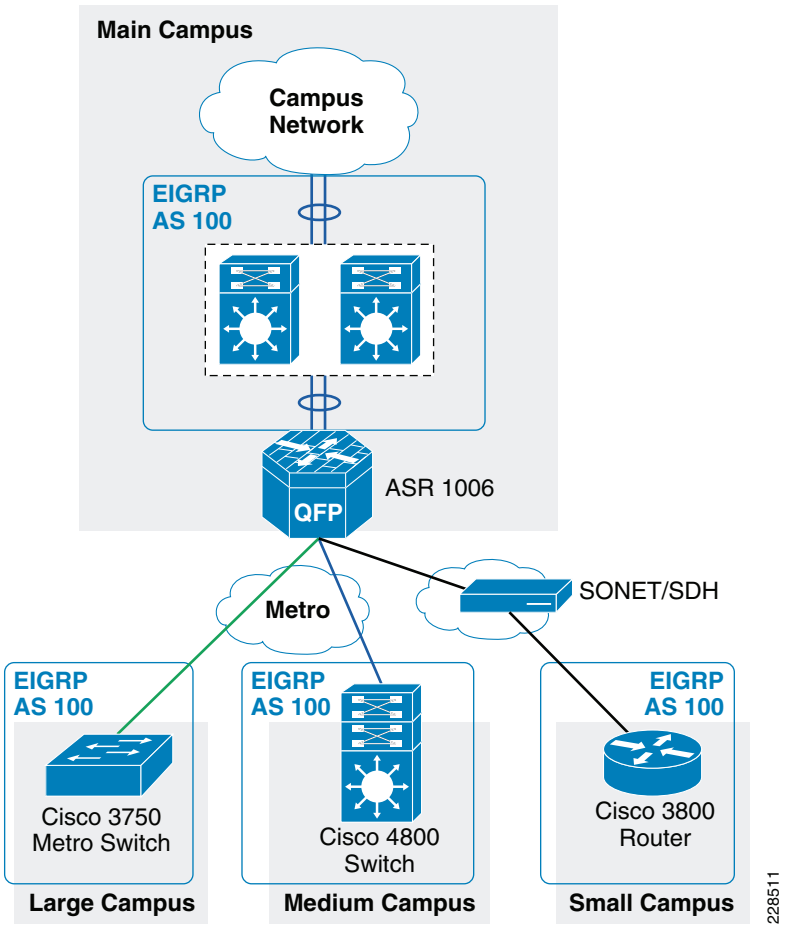
Figure 4-8 BGP Design in Community College



Internal Routing Domain

EIGRP is chosen as the routing protocol for designing the internal routing domain, which is basically connecting all the devices in the campus network. EIGRP is a balanced hybrid routing protocol that builds neighbor adjacency and flat routing topology on per autonomous-system (AS)-basis. It is important to design EIGRP routing domain in college infrastructure with all the design principles defined earlier in this section. CCVE SRA network infrastructure must be deployed in recommended EIGRP protocol design to secure, simplify, and optimize the network performance. Figure 4-9 depicts the design of EIGRP for internal network.

Figure 4-9 EIGRP Design Diagram



To obtain more information about EIGRP design, refer to the "Community College Network Foundation Services Design" section on page 3-25.

QoS

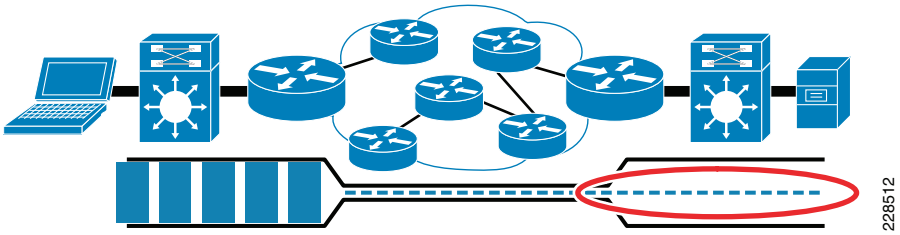
QoS is a part of foundation services, which is very critical to the application performance. Today's networks are rapidly converging into IP network. The traditional applications, which used the networks, were voice, video, and data. However, broadcast video, real-time video, video surveillance, and many other applications have all converged into IP networks. Moreover, each of these applications require different performance characteristics on the network. For example, data applications may need only high throughput, but are tolerant to delay and loss. Similarly, voice applications need constant low bandwidth and low delay performance. To cater to these performance characteristics, Cisco IOS has several rich QoS tools such as classification and marking, queuing, WRED, policing, shaping, and many other tools to effect the traffic characteristics. Before discussing the QoS design, the following subsection provides a brief introduction on these characteristics.

Traffic Characteristics

The main traffic characteristics are bandwidth, delay, loss, and jitter.

- *Bandwidth*—Lack of proper bandwidth can cause applications from performing poorly. This problem would be exacerbated if there were more centralized applications. The bandwidth constraint occurs because of the difference between the bandwidth available at LAN and the WAN. As shown in Figure 4-10, the bandwidth of the WAN transport dictates the amount of traffic received at each remote site. Applications are constrained by the amount of WAN bandwidth.

Figure 4-10 Bandwidth Constraint Due to Difference in Speeds



- *Jitter*—Occurs when there are bandwidth mismatches between the sender, and receiver which could result in poor performance of delay sensitive applications like voice, and video.
- *Loss*—occurs when the queues become full, and there is not enough bandwidth to send the packets.
- *Delay*—Is an important characteristic, which plays a large role in determining the performance of the applications. For a properly designed voice network the one-way delay must be less then 150 msec.

QoS Design for WAN Devices

For any application regardless of whether it is video, voice, or data the traffic characteristics just mentioned need to be fully understood before making any decisions on WAN transport or the platforms needed to deploy these services. Cisco QoS tools help to optimize these characteristics so that voice, video, and data applications performance is optimized. The voice and video applications are highly delay-and drop-sensitive, but the difference lies in the bandwidth requirement. The voice applications have a constant and low bandwidth requirement, but the video applications have variable bandwidth requirements. Therefore, it is important to have a good QoS policy to accommodate these applications.

Regardless of the WAN transport chosen, QoS design is the most significant factor in determining the success of network deployment. There are number of benefits in deploying a consistent, coherent QoS scheme across all network layers. It helps not only in optimizing the network performance, it helps to mitigate network attacks, and also manage the control plane traffic. Therefore, when the platforms are selected at each network layer, QoS must always be considered in the design choice.

In the WAN links the congestion can occur when there are speed mismatches. This may occur because there is significant difference between LAN speeds and WAN speeds. To prevent that from occurring, the following two major tools can be used:

- Low-Latency Queuing (LLQ), which is used for highest-priority traffic (voice/ video).
- Class-based Weighted-Fair Queuing (CBWFQ), which can be used for guaranteeing bandwidth to data applications.

The general guidelines for deploying the WAN edge device considerations are as follows:

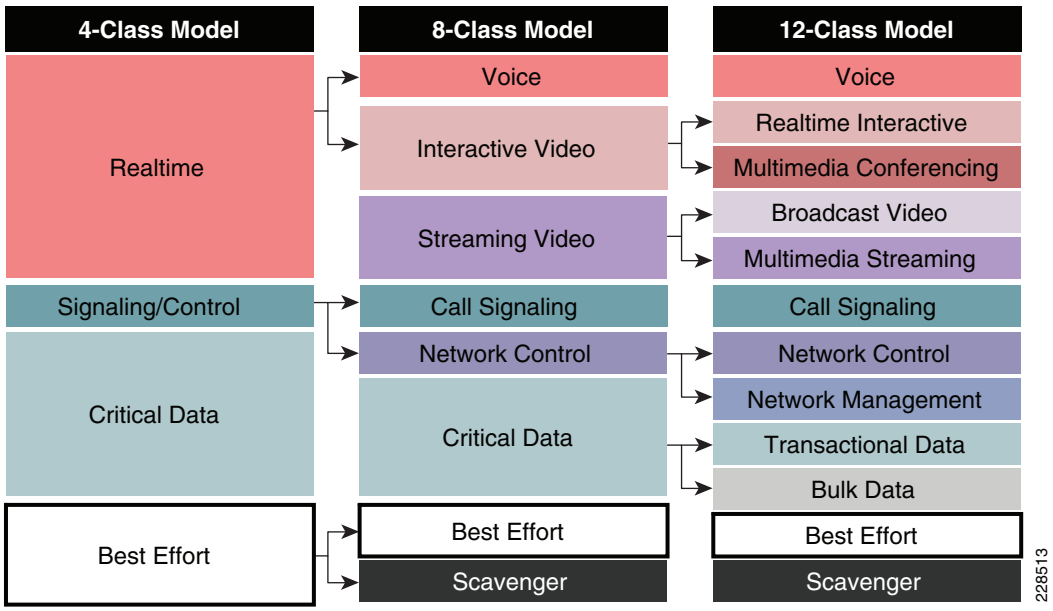
- For WAN speeds between 1Mpbs to 100Mbps, use hierarchical policies for sub-line-rate Ethernet connections to provide shaping and CBWFQ/LLQ.
- For WAN speeds between 100Mbps to 10Gbps, use ASR1000 with QFP or hardware queuing via Cisco Catalyst 3750-Metro and 6500/7600 WAN modules.

When designing the QoS for WAN architecture, there are two main considerations to start with:

- Whether the service provider will provide four classes of traffic.
- The service provider will only provide one class of traffic.

This document assumes that the service provider will support at least 4 classes of traffic such as REAL_TIME, GOLD, SILVER, and DEFAULT. The community college campus LAN supports 12 classes of traffic, which will be mapped to 4 classes of traffic on the WAN side. Figure 4-11 illustrates the recommended markings for different application traffic.

Figure 4-11 Mapping of 12-Class Model to 4-classes



Once the QoS policy is designed the next pertinent question is the appropriate allocation of bandwidth for the 4 classes of traffic. Table 4-1 describes the different classes, and the percentage, and actual bandwidth allocated for each class of traffic.

Table 4-1 Classes of Traffic

Class of Traffic	4-class SP Model	Bandwidth Allocated	Actual Bandwidth
Voice, Broadcast Video, Real Time Interactive	SP- Real-Time	30%	30 Mbps
Network Control Signaling Transactional Data	SP-Critical 1	20%	20 Mbps
Multi-media Conferencing Multimedia streaming OAM	SP-Critical 2	20%	20 Mbps
Bulk data Scavenger Best Effort	SP-Best Effort	30%	30 Mbps

Redundancy

Redundancy must be factored into the WAN design for a number of reasons. Since the WAN may span across several service provider networks, it is likely that network will be subjected to different kinds of failures occurring all the time. One of the following failures can occur over a period of time: route flaps, brownouts, fibers being cut, and device failures. The probability of these occurring over a short period of time is low, but the occurrence is highly likely over a long period of time. To meet these challenges, different kind of redundancy should be planned. The following are the some of the ways to support redundancy:

- NSF/SSO—For networks to obtain 99.9999% of availability, technologies such as NSF/SSO are needed. The NSF would route packets until route convergence is complete, where as SSO allows standby RP to take immediate control and maintain connectivity protocols.
- Service Software Upgrade (ISSU) allows software to be updated or modified while packet forwarding continues with minimal interruption.
- Ether channel load balancing—Enabling this feature provides link resiliency and load balancing of traffic. This feature is enabled on the WAN aggregation 2 device. Figure 4-12 shows where this feature is enabled.

Figure 4-12 Link Resiliency

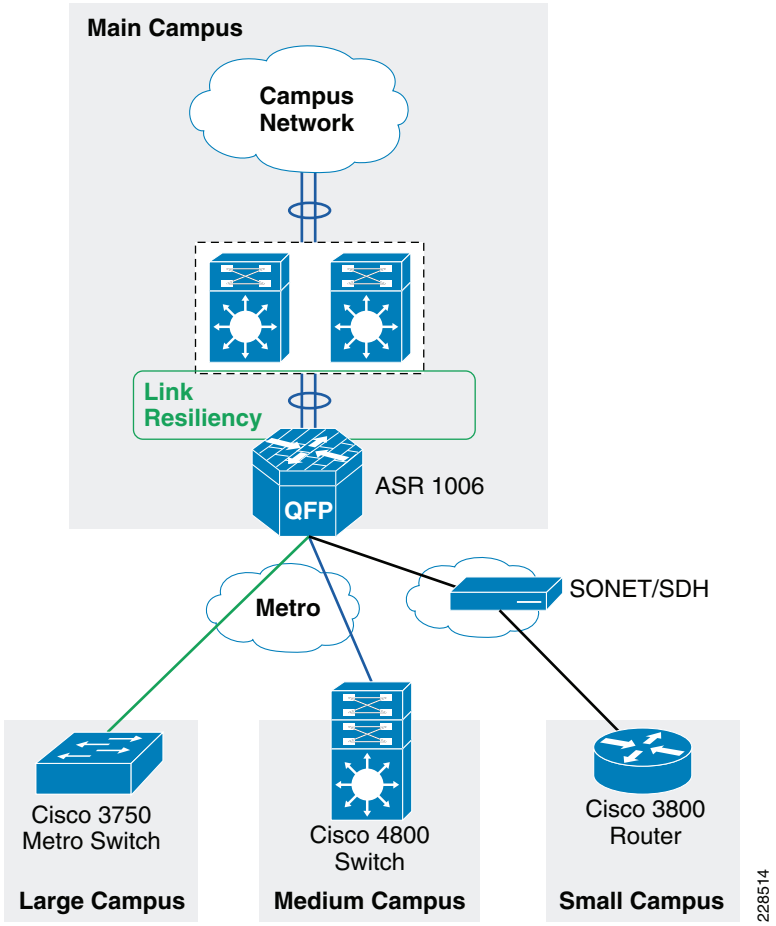


Table 4-2 shows the various WAN devices that are designed for resiliency.

Table 4-2 WAN Devices

Device	WAN transport	Resiliency feature
WAN aggregation 1	Private WAN/Internet	ISSU, IOS based redundancy
WAN aggregation 2	Metro	Redundant ESP, RP'

This section discusses how to incorporate the resiliency principle in Cisco Community College reference design for the WAN design. To enable resiliency adds cost and complexity to the design. Therefore, resiliency has been added at certain places where it is absolutely critical to the network architecture rather than designing redundancy at every place of the network.

In the Cisco Community College reference design the redundancy is planned at both WAN aggregation router1, and WAN aggregation router 2 in the main campus location. As explained in the WAN aggregation platform selection for the main campus location discussion ASR routers have been selected at both WAN aggregation locations places. However, we have different models, at both WAN aggregation places. When the ASR router interfaces with the private WAN, Internet networks the ASR 1004 with IOS-based redundancy has been chosen. Similarly, for the ASR router that interfaces with Metro connections, the ASR 1006 with dual RP, and dual ESP to provide for hardware-based redundancy has been chosen. Both of these models support In Service Software Upgrade (ISSU) capabilities to allow a user to upgrade Cisco IOS XE Software while the system remains in service. To obtain more information on ASR resiliency capabilities, see the ASR page at following URL: http://www.cisco.com/go/asr1000

Multicast

The main design considerations for multicast are as follows:

- The number of groups supported by the WAN edge device. This is scalability factor of the WAN edge device. The platform chosen must support the number of required groups.
- The placement of the RP—There are couple of options available with RP placement, which include Anycast with Static, Anycast with Auto-RP, or Anycast with BSR.
- Multicast protocols—PIM-Sparse mode, IGMP
- QoS policy must be configured for multicast traffic, so that this traffic does not affect the unicast traffic.

In the Community College reference design, we are assuming that multicast traffic would be present only within the campus, and not between the community colleges. Therefore, to obtain more information about multicast design for campus, refer to "Community College Network Foundation Services Design" section on page 3-25.

Summary

Designing the WAN network aspects for the Cisco Community College reference design interconnects the various LAN locations as well as lays the foundation to provide safety and security, operational efficiencies, virtual learning environments, and secure classrooms.

This chapter reviewed the WAN design models recommended by Cisco and where to apply these models within the various locations within a community college network. Key WAN design principles such as WAN aggregation platform selection, QoS, multicast and redundancy best practices were discussed for the entire community college design. Designing the WAN network of a community college using these

recommendations and best practices will establish a network that is resilient in case of failure, scalable for future grown, simplified to deploy and manage and cost efficient to meet the budget needs of a community college.

CHAPTER 5

Community College Mobility Design Considerations

Mobility Design

The Cisco Community College reference design is intended to assist community colleges in the design and deployment of advanced network-based solutions within twenty-first century learning environments.

The reference design addresses the business challenges currently facing community colleges. At the heart of the reference design is the network service fabric, which is a collection of products, features, and technologies that provide a robust routing and switching foundation upon which all solutions and services are built. Operating on top of the network service fabric are all the services used within the community college network to solve business problems, which include the following:

- Safety and security
- Virtual learning
- Secure connected classrooms
- Operational efficiencies

Community college students are dynamic, mobile, and technology-savvy. When on campus, they move about while equipped with an array of mobility-enabled devices including PDAs, phones, and laptops. In contrast to the typical enterprise business environment, community colleges consist of a large student population that typically experiences a complete turnover every few years. Typical community college students tend to use new applications and the network for many aspects of their lives, demanding connectivity wherever they are. This connected generation is untethered from wired access connectivity and assumes the presence of a high-performance, reliable wireless LAN (WLAN) in all major campus areas.

The mobility design implemented by a community college must meet the needs of this mobile generation while also addressing the requirements of faculty, staff, administrators, and visitors. The challenge for community colleges is to create a robust, end-to-end, mobility-enabled network that supports their requirements at a cost that is within their often constrained budgets. Community colleges should be equipped with a mobility solution that supports the following:

- Secure communications between local and remote campus sites to support students, faculty, staff, administrators, and visitors, using the new generation of mobility-enabled devices and applications in the current marketplace
- A scalable design model that can easily accommodate the addition of new campus buildings as well as existing building modifications
- Built-in support for bandwidth-intensive, high-speed multimedia applications

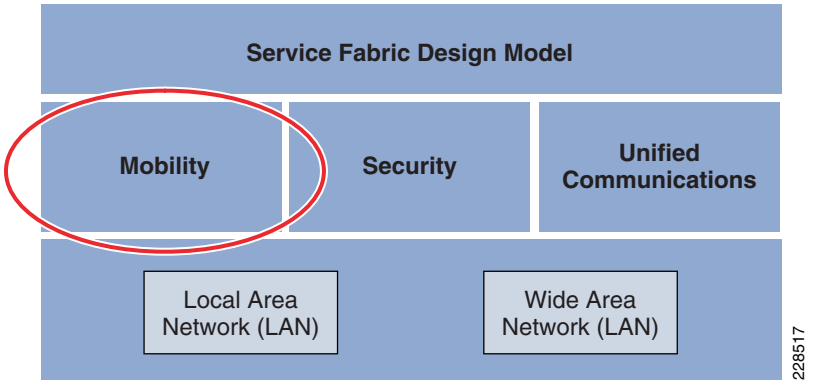
- Simplified management tools to facilitate maintenance of the system-wide mobility solution
- The use of new tools and applications for mobile learning, collaboration, and campus operations
- Effective communication with public safety first responders in the event of an emergency

In addition, each community college must remain competitive, differentiating itself from its peer institutions so as to attract and retain the best students and faculty. Students want to attend quality community colleges that provide technology services relevant to the way they live, work, and learn. They want to take full advantage of community college capabilities to facilitate their success while they are students, as well as when they are pursuing post-graduation placement. A community college with a pervasive, high-speed wireless network not only demonstrates technological leadership and innovation, but enables the deployment of innovative applications that improve learning, the streamlining of operations, collaboration enhancements, and productivity improvements.

This mobile campus lifestyle helps to drive the need for careful wireless capacity and coverage planning. Keep in mind that the traditional scenario of a mass of students filing into a large lecture hall within a monolithic campus building is no longer the only learning environment seen within higher educational institutions. High performance, secure wireless technologies can enable “virtual classrooms” even in non-traditional settings, such as leased space in shopping malls, retail plazas, and even from homes and offices. School administrators need secure access to tools, records, and resources, as well as access to mobile voice capabilities throughout the campus. In addition, the expectation for secure, reliable, high-performance guest access by contractors, vendors, and other guests of the community college establishment has become a standard and expected component of doing business.

To meet these and other student, faculty, and guest needs, community colleges must evolve into mobility-enabled campuses and twenty-first century learning centers. The primary objectives of this document are the design considerations surrounding the requirements and expectations that must be considered when integrating mobility into the Cisco Community College reference design, as well as the tradeoffs required to facilitate the four service requirements stated previously. These design considerations form a critical part of the overall service fabric design model, shown in Figure 5-1.

Figure 5-1 Service Fabric Design Model

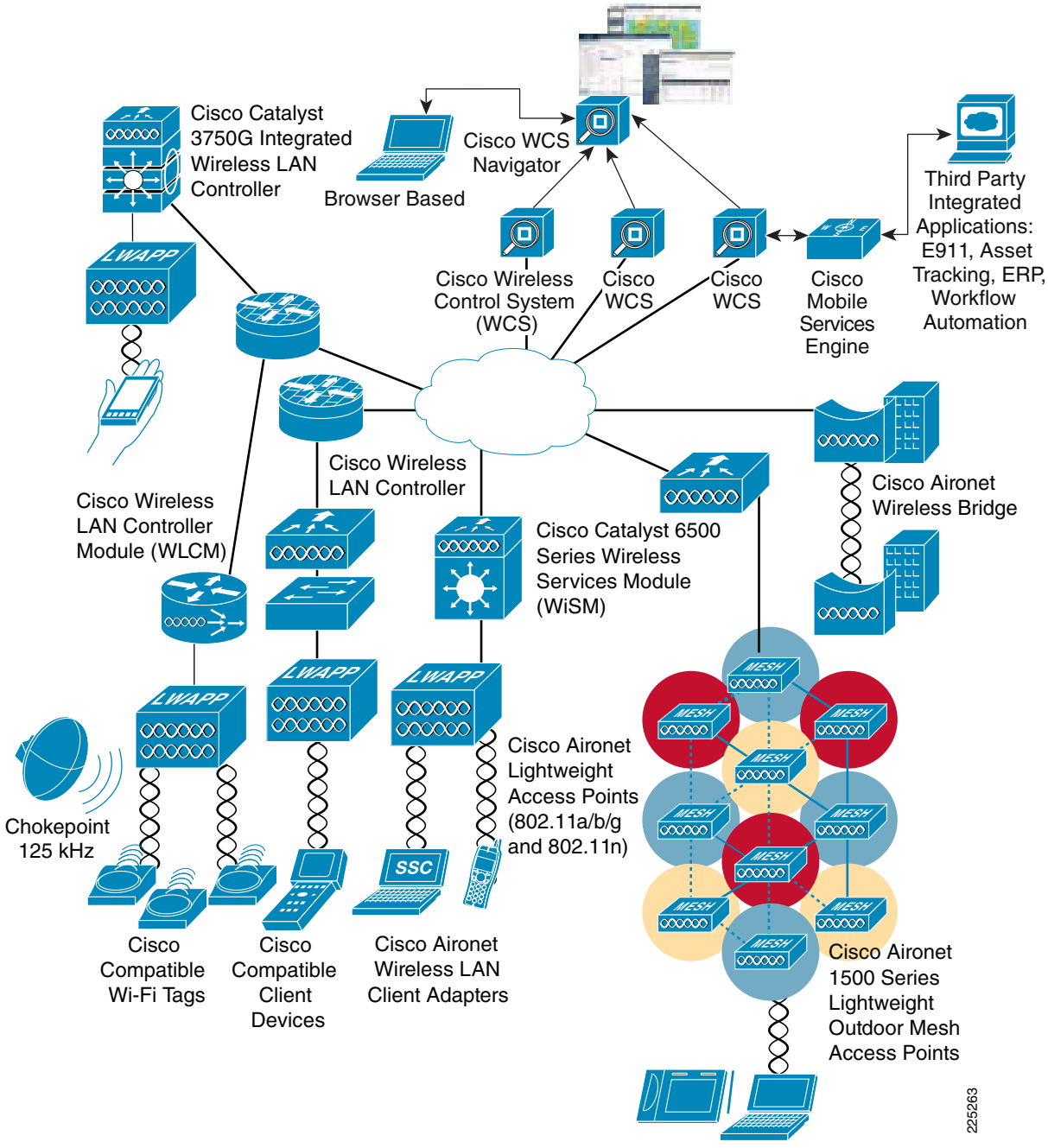


Given the mobility of students, staff, and visitors, wireless LANs have emerged as one of the most effective and high performance means for these mobile users to access the campus network. The Cisco Unified Wireless Network (Cisco UWN) is a unified solution that addresses the wireless network security, deployment, management, and control aspects of deploying a wireless network. It combines the best elements of wireless and wired networking to deliver secure, scalable wireless networks with a low total cost of ownership.

Figure 5-2 shows a high-level topology of the Cisco Unified Network, which includes access points that use the Control and Provisioning of Lightweight Access Points (CAPWAP) protocol; the Cisco Wireless Control System (WCS); and the Cisco Wireless LAN Controller (WLC). In addition to the traditional

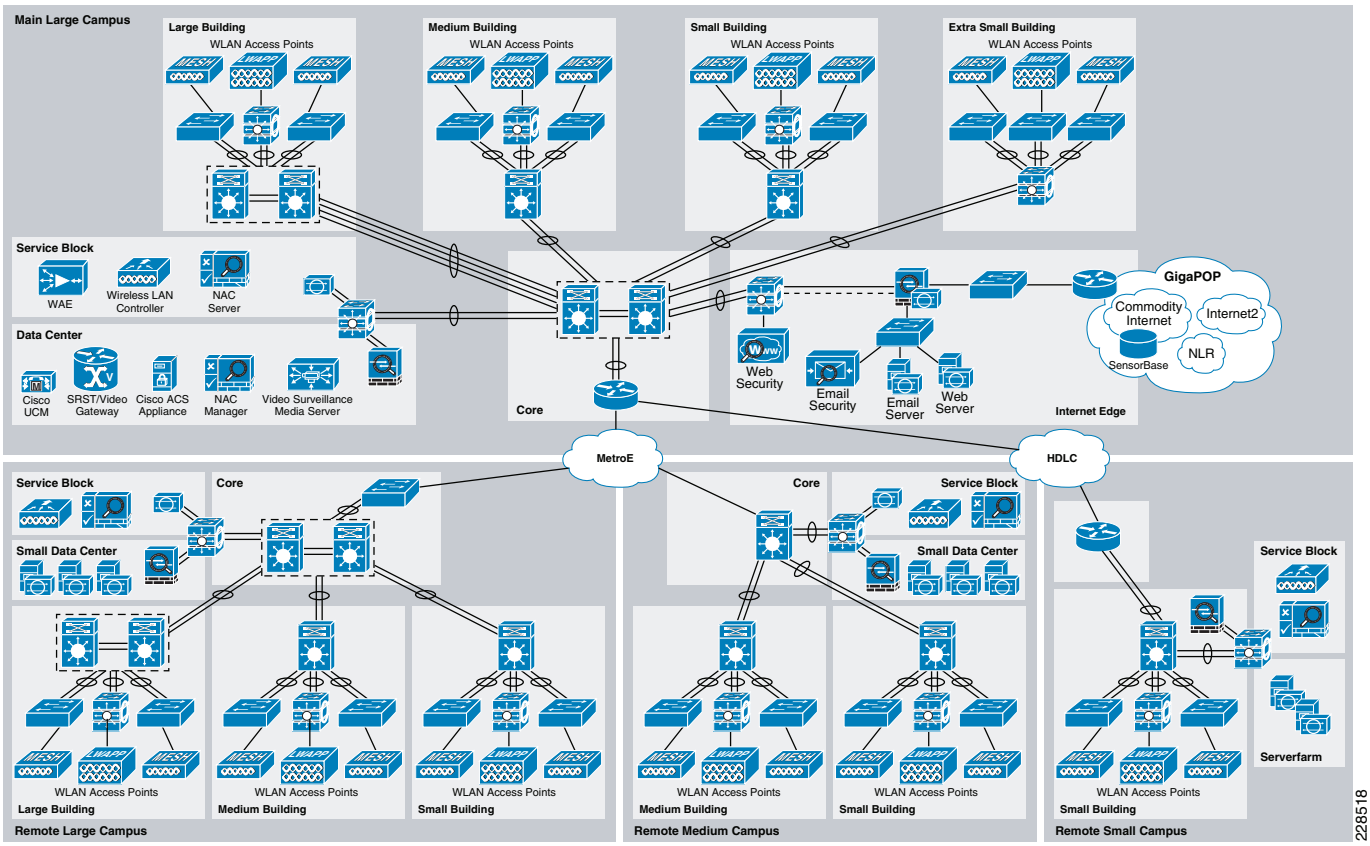
standalone WLAN controller, alternate hardware platforms include the Cisco ISR router Wireless LAN Controller Module (WLCM) or the Cisco Catalyst 6500 Wireless Services Module (WiSM). The Cisco Access Control Server (ACS) and its Authentication, Authorization, and Accounting (AAA) features complete the solution by providing Remote Authentication Dial-In User Service (RADIUS) services in support of user authentication and authorization.

Figure 5-2 Cisco Unified Wireless Network Overview



The Cisco Community College reference design accommodates a main campus and one or more remote smaller campuses interconnected over a metro Ethernet or managed WAN service. Each of these campuses may contain one or more buildings of varying sizes, as shown in Figure 5-3.

Figure 5-3 Community College Reference Design Overview



Operating on top of this network are all the services used within the community college environment such as safety and security systems, voice communications, video surveillance equipment, and so on. The core of these services are deployed and managed at the main campus building, allowing each remote campus to reduce the need for separate services to be operated and maintained by community college IT personnel. These centralized systems and applications are served by a data center in the main campus.

As Figure 5-3 shows, the Cisco Community College reference design uses a centralized approach in which key resources are centrally deployed at either the campus or college level. The key feature of this integration is the use of one or more WLAN controllers at each campus, with the overall WLAN management function (the Cisco WCS) located at the main campus. This approach simplifies the deployment and operation of the network, helping to ensure smooth performance, enhance security, enhance network maintainability, maximize network availability, and reduce overall operating costs.

The Cisco Community College reference design takes into account that cost and limited network administrative resources are common limiting factors for most community colleges. The topologies and platforms are carefully selected to increase productivity while minimizing the overall cost and complexity of operation. In certain instances, tradeoffs are necessary to reach these goals, and this document points out such areas.

The Cisco mobility approach within the Cisco Community College reference design focuses on the following key areas:

- *Accessibility*

  - Enabling students, staff, and guests to be accessible and productive on the network, regardless of whether they are in a traditional classroom setting, collaborating in a study hall, having lunch with colleagues within campus eating areas, or simply enjoying a breath of fresh air outside a campus building
  - Enabling easy, secure guest access to college guests such as alumni, prospective students, contractors, vendors and other visitors.

- *Usability*

  In addition to extremely high WLAN transmission speeds made possible by the current generation of IEEE 802.11n technology, latency-sensitive applications (such as IP telephony and video conferencing) are supported over the WLAN using appropriately applied quality-of-service (QoS) classification. This gives preferential treatment to real-time traffic, helping to ensure that video and audio information arrives on time.

- *Security*
  - Segmenting authorized users and blocking unauthorized users
  - Extending the services of the network safely to authorized parties
  - Enforcing security policy compliance on all devices seeking to access network computing resources. Faculty and other staff enjoy rapid and reliable authentication through IEEE 802.1x and Extensible Authentication Protocol (EAP), with all information sent and received on the WLAN being encrypted.

Note For information on how security design is addressed within the Cisco Community College reference design, see Chapter 6, "Community College Security Design Considerations."

- *Manageability*

  A relatively small team of college network administrators must be able to easily deploy, operate, and manage hundreds of access points that may reside within a multi-campus community college. A single, easy-to-understand WLAN management framework provides small, medium, and large community colleges with the same level of WLAN management scalability, reliability, and ease of deployment demanded by traditional enterprise business customers.

- *Reliability*
  - Providing adequate capability to recover from a single-layer fault of a WLAN access component or controller wired link
  - Ensuring that WLAN accessibility is maintained for students, faculty, staffs and visitors in the event of common failures

Accessibility

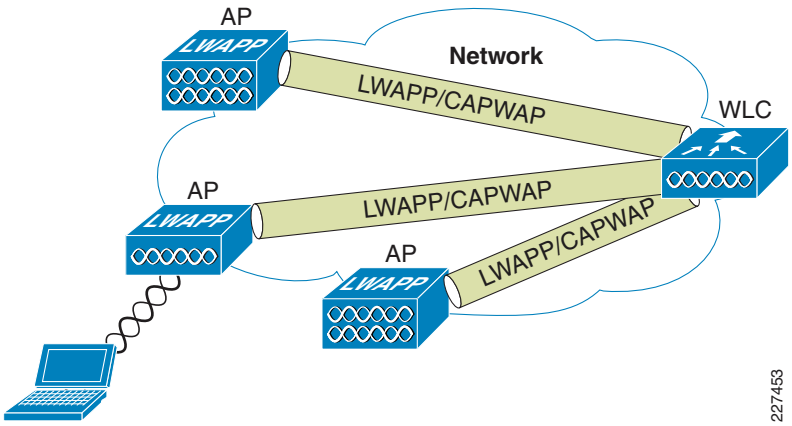
This section provides a brief introduction to the fundamental protocol used for communication between access points and WLAN controllers, followed by a discussion of mobility design considerations pertaining to those aspects of the Cisco Community College reference design relevant to accessibility, such as the following:

- WLAN controller location
- WLAN controller connectivity
- Access points

The basic mobility components involved with providing WLAN access in the Cisco Community College reference design consists of WLAN controllers and access points that communicate with each other using the IETF standard CAPWAP protocol. In this arrangement, access points provide the radio connection to wireless clients, and WLAN controllers manage the access points and provide connectivity to the wired network.

Figure 5-4 shows the use of CAPWAP by access points to communicate with and tunnel traffic to a WLAN controller.

Figure 5-4 CAPWAP Access Point to WLC Communication



CAPWAP enables the controller to manage a collection of wireless access points, and has the following three primary functions in the mobility design:

- Control and management of the access point
- Tunneling of WLAN client traffic to the WLAN controller
- Collection of 802.11 data for overall WLAN system management

CAPWAP is also intended to provide WLAN controllers with a standardized mechanism with which to manage radio-frequency ID (RFID) readers and similar devices, as well as enable controllers to interoperate with third-party access points in the future.

In controller software Release 5.2 or later, Cisco lightweight access points use CAPWAP to communicate between the controller and other lightweight access points on the network. Controller software releases before Release 5.2 use the Lightweight Access Point Protocol (LWAPP) for these communications. Note that most CAPWAP-enabled access points are also compatible with the preceding LWAPP protocol. An exception is that the Cisco Aironet 1140 Series Access Point supports only CAPWAP.

The mobility approach in the Cisco Community College reference design is based on the feature set available in Cisco Wireless LAN Controller software Release 6.0, which uses CAPWAP.

For detailed CAPWAP protocol information, see the following URL: http://www.ietf.org/rfc/rfc5415.txt.

WLAN Controller Location

WLAN campus deployments are typically categorized into two main categories, *distributed* and *centralized*:

- *Distributed controller*—In this model, WLAN controllers are located throughout the campus network, typically on a per-building basis, and are responsible for managing the access points resident in a given building. This technique is commonly used to connect controllers to the campus network using distribution routers located within each building. In the distributed deployment model, the CAPWAP tunnels formed between access points and WLAN controllers are typically fully contained within the confines of the building.
- *Centralized controller*—In this model, WLAN controllers are placed at a centralized location in the network. Because centralized WLAN controllers are typically not located in the same building as the access points they manage, the CAPWAP tunnels formed between them must traverse the campus backbone network.

The Cisco Community College reference design is based on the centralization of WLAN controllers, on a per-campus basis, and follows established best practices, such as those contained in Chapter 2 of the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_ent_mob_design.html.

Figure 5-3 shows the planned deployment of WLAN controllers within distinct per-campus service blocks, each associated with the main, large remote, medium remote, and small remote campus sites respectively. Service blocks tend to be deployed at locations in the network where high availability routing, switching, and power is present. In addition, these areas tend to be locally or remotely managed by network staff possessing higher skill sets.

Some of the advantages underlying the decision to centralize the deployment of WLAN controllers on a per-campus basis include the following:

- *Reduced acquisition and maintenance costs*—By servicing the needs of all campus users from a central point, the number of WLAN controller hardware platforms deployed can be reduced compared to that required for a distributed, per-building design. Similarly, incremental software licensing costs associated with WLAN controllers are reduced as well. These economies of scale typically increase with the size of the campus WLAN.
- *Reduced administrative requirements*—By minimizing the total number of WLAN controllers deployed, the controller management burden imposed on community college campus network administrators is minimized.
- *Cost-effective capacity management*—The use of a centralized WLAN controller model allows the designer the ability to centrally service access points located in multiple building locations and efficiently manage controller capacity.
- *Simplified network management and high availability*—Centralized WLAN controller designs simplify overall network management of controllers, as well as facilitate cost-effective controller high availability approaches. This can protect the campus from a loss of WLAN access in the rare event of a controller failure, without the expense of 1:1 controller duplication.
- *Reduced component interaction points*—Centralizing WLAN controllers minimizes the number of integration points that must be managed when interfacing the controller with other devices. When integrating the WLAN controller with the Network Admission Control (NAC) appliance on any given campus, for example, only one integration point must be administered.
- *Increased performance and reliability*—Centralized WLAN controller deployments usually lead to highly efficient inter-controller mobility. For large campuses, there is also an incremental economy of scale that occurs as the network grows larger. By centralizing WLAN controllers on a per-campus

basis, CAPWAP tunneling between access points and WLAN controllers is not normally required to traverse WAN links (except during controller failover), thereby conserving WAN bandwidth and improving performance overall.

Note For additional information on inter-controller mobility and roaming, see the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch2_Arch.html#wp1028197.

The choice of WLAN controller for the Cisco Community College reference design is the Cisco 5508 Wireless Controller, as shown in Figure 5-5.

Figure 5-5 Cisco 5508 Wireless Controller

The Cisco 5508 Wireless Controller is a highly scalable and flexible platform that enables system-wide services for mission-critical wireless in medium to large-sized enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the Cisco 5508 Wireless Controller offers the ability to simultaneously manage from 12 to a maximum of 250 access points per controller. Base access point controller licensing provides the flexibility to purchase only the number of access point licenses required, with the ability to add additional access point licenses in the future when community college campus growth occurs. In campuses requiring more than 250 total access points, or load sharing/high availability is required, multiple controllers can be deployed as necessary.

More information on the Cisco 5508 Wireless Controller can be found at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/data_sheet_c78-521631.html.

WLAN Controller Connectivity

This section discusses WLAN controller connectivity, including the following:

- Controller connectivity to the wired network
- Controller connectivity to the wireless devices
- Defining WLANs and Service Set Identifiers (SSIDs)
- WLAN controller mobility groups
- WLAN controller access point groups
- WLAN controller RF groups

Controller Connectivity to the Wired Network

WLAN controllers possess physical entities known as *ports* that connect the controller to its neighboring switch (the Cisco 5508 Wireless Controller supports up to eight Gigabit Ethernet Small Form-Factor Pluggable [SFP] ports). Each physical port on the controller supports, by default, an 802.1Q VLAN trunk, with fixed trunking characteristics.

Note For more information concerning the various types of ports present on Cisco WLAN controllers, see the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* at the following URL: http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/Controller60CG.html.

Interfaces are logical entities found on the controller. An interface may have multiple parameters associated with it, including an IP address, default gateway, primary physical port, optional secondary physical port, VLAN identifier, and Dynamic Host Configuration Protocol (DHCP) server. Each interface is mapped to at least one primary port, and multiple interfaces can be mapped to a single controller port.

Note For more information concerning the various types of interfaces present on Cisco WLAN controllers, see the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* at the following URL: http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/Controller60CG.html.

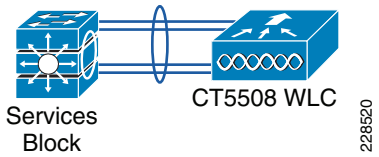
A special type of controller interface is known as the *AP manager interface*. A controller has one or more AP manager interfaces, which are used for all Layer 3 communications between the controller and its joined access points. The IP address of the AP manager interface is used as the tunnel source for CAPWAP packets from the controller to the access point, and as the destination for CAPWAP packets from the access point to the controller. The AP manager interface communicates through a distribution system port by listening across the Layer 3 network for CAPWAP "join" messages generated by access points seeking to communicate with and "join" the controller.

Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances traffic transparently to the user. LAG bundles all the enabled distribution ports on the WLAN controller into a single EtherChannel interface.

Currently published best practices specify either multiple AP manager interfaces (with individual Ethernet links to one or more switches) or link aggregation (with all links destined for the same switch or switch stack) as the recommended methods of interconnecting WLAN controllers with wired network infrastructure. For more information, see the following URL: http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/c60mint.html#wp1277659.

In the Cisco Community College reference design, the Cisco 5508 Wireless Controllers are interconnected with the modular switches or switch stacks found in the services block using link aggregation and EtherChannel exclusively, as shown in Figure 5-6.

Figure 5-6 WLAN Controller Link Aggregation to Services Block



In this way, one or more centralized WLAN controllers are connected via the services block to the campus core. This design can make use of up to eight Gigabit Ethernet connections from the Cisco 5508 Wireless Controller to the services block. These Gigabit Ethernet connections should be distributed among different modular line cards or switch stack members as much as possible, so as to ensure that the failure of a single line card or switch stack failure does not result in total failure of the WLAN controller connection to the campus network. The switch features required to implement this connectivity between the WLAN controller and the services block are the same switch features that would otherwise be used for EtherChannel connectivity between switches in general.

Further discussion of the advantages of using controller link aggregation, as well as the considerations concerning its implementation in the Cisco Community College reference design can be found in Controller Link Aggregation, page 5-36.

The key advantage of using link aggregation in this fashion instead of multiple AP manager interfaces is design performance, reliability, and simplicity:

- With the Ethernet bundle comprising up to eight Gigabit Ethernet links, link aggregation provides very high traffic bandwidth between the controller and the campus network.
- With link aggregation, if any of the controller ports fail, traffic is automatically migrated to one of the other controller ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data. Terminating on different modules within a single Catalyst modular switch, or different switch stack members (as shown in Figure 5-6), provides redundancy and ensures that connectivity between the services block switch and the controller is maintained in the rare event of a failure.
- Link aggregation also offers simplicity in controller configuration; for example, configuring primary and secondary ports for each interface is not required.

Controller Connectivity to Wireless Devices

This section deals with the design considerations that involve provisioning wireless access for the various user groups that reside within the community college campus system, such as the faculty, administrators, students, and guests. These considerations include the WLAN controllers deployed in the campus services blocks, as well as the access points that are located in the campus buildings.

Defining WLANs and SSIDs

In most community colleges, various campus user groups likely require access to the WLAN for a variety of purposes. Although peaks in usage may occur at different times, it is safe to assume that a large portion of these groups will likely want access to the WLAN at the same time. Thus, in designing for mobility within the Cisco Community College reference design, the physical campus wireless infrastructure needs to support logical segmentation in such a fashion that a reasonable proportion of all users can be serviced simultaneously and with an appropriate degree of security and performance.

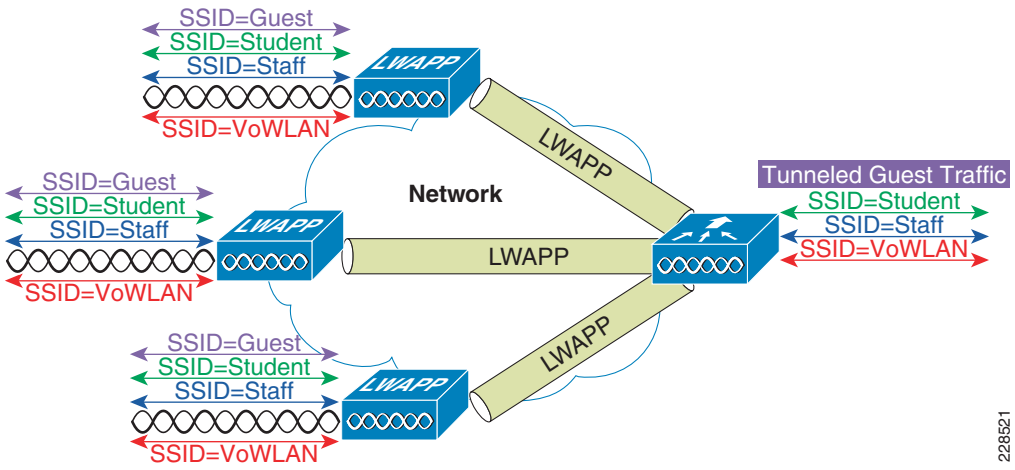
One of the basic building blocks used in the WLAN controller to address this need is the ability to provision logical WLANs, each of which are mapped to different wired network interfaces by the WLAN controller. These WLANs are configured and assigned a unique SSID, which is a sequence of characters that uniquely names a WLAN. For this reason, an SSID is also sometimes referred to simply as a *network name*.

Note Each set of wireless devices communicating directly with each other is called a basic service set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). An SSID is simply the 1–32 byte alphanumeric name given to each ESS.

To promote ease of administration, the value chosen for the SSID should bear some direct relationship to the intended purpose of the WLAN.

Figure 5-7 provides a high-level illustration of the four logical WLANs that provide mobility within the Cisco Community College reference design, and how they are mapped to WLAN controller network interfaces or tunneled to another controller. For ease of administration and the support of students, faculty, and guests that frequent multiple campuses, the names chosen for the WLAN SSIDs should be consistent within each campus in the community college system. For example, student wireless access should be available anywhere there is WLAN RF coverage within this particular community college system using the SSID entitled *student*.

Figure 5-7 WLAN SSIDs



In the Community College reference design, the set of WLAN SSIDs provide access to the following WLANs:

- A *secured staff* WLAN network with dynamically generated per-user, per-session encryption keys.

  This WLAN would be used by college faculty, staff, and administration using managed client devices, such as laptops, PDAs, and so on. The secured staff WLAN is designed to provide secure access and good performance for devices controlled by the community college network administration staff. Unlike the student and guest access WLANs, devices that are used on the secured staff WLAN are usually procured and deployed by (or with the knowledge and cooperation of) the community college network administration staff on behalf of faculty and other university staff users. Faculty and staff users are typically prohibited from bringing their own personal PDAs, laptops, or voice over WLAN (VoWLAN) phones to use on the secured staff WLAN. This allows,

for example, a baseline level of authentication and encryption to be deployed for the secured staff WLAN without concern for whether or not the devices using the secured staff WLAN can support this level of authentication and encryption.

The characteristics of this WLAN include the following:

- Wi-Fi Protected Access 2 (WPA2) encryption with 802.1x/EAP authentication, and Cisco Centralized Key Management (Cisco CKM, also referred to as CCKM) for enhanced roaming.

  Most modern WLAN client devices being produced today support this level of authentication and encryption. The addition of Cisco CKM in this case provides for faster roaming by enabling Cisco CKM-equipped clients to securely roam from one access point to another without the need to re-authenticate after the roam completes.

- Broadcast SSID enabled. Enabling this helps to avoid potential connectivity difficulties with some clients. There is no real disadvantage to enabling broadcast SSID.

- QoS profile setting of *silver* (best effort delivery).

Note For more details on WLAN QoS, see the references contained at the end of Quality-of-Service, page 5-27.

- Wi-Fi Multimedia (WMM) policy of allowed. This allows devices and applications that can support 802.1e enhanced QoS prioritization to do so. Enabling the use of WMM in this way is also in compliance with the 802.11n.

- Mandatory IP address assignment via DHCP. Eliminating the configuration of static IP addresses helps to mitigate the risk of IP address duplication.

- Radio policy set to allow clients to use either 2.4 GHz or 5 GHz to access this WLAN. This allows clients that can take advantage of benefits of 5 GHz operation (such as increased capacity and reduced interference) to do so.

Note The 802.11b and 802.11g physical layers (PHYs) are applied in the unlicensed 2.4 GHz industrial, scientific, and medical (ISM) frequency band, whereas the 802.11a PHY is applied in the unlicensed 5 GHz ISM band. “Dual-band” 802.11a/bg clients are capable of operating in either 2.4 or 5 GHz frequency bands because they are capable of using any of the three PHYs. Selection between PHYs is typically achieved via software configuration.

Clients using the very high speed 802.11n PHY may be designed to operate in a single band, or they may be 802.11n “dual-band” clients. Unlike the 802.11b, 802.11g, and 802.11a PHYs, simply stating that a client is 802.11n does not precisely indicate what frequency bands the client is capable of operating within.

For more information about the 802.11n PHY and its application to the 2.4 and 5 GHz frequency bands, see the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_80211n_design_and_deployment_guidelines.html.

- A *secured VoWLAN* network that is optimized for VoWLAN usage by college faculty, staff, and administration using managed client devices.

  As was the case with the secured staff WLAN, this WLAN is designed to provide secure access and good performance when used with VoWLAN devices (such as the Cisco Unified Wireless IP Phone 7925G) that are usually procured, deployed, and managed by (or with the knowledge and

cooperation of) the community college network administration staff. Such procurement is usually conducted on behalf of faculty and other university staff users. To assure proper security and promote effective device management, faculty and staff users are typically prohibited from bringing their own personal VoWLAN phones and using them on this WLAN. This allows, for example, a baseline level of authentication and encryption to be deployed for this WLAN with the knowledge that the devices using this WLAN can support that level of security. The key differences between this WLAN and the secured staff WLAN include the following:

- The security policy on this WLAN is WPA with Cisco CKM, which is recommended as a best practice for the Cisco 7921G and 7925G VoWLAN phones.
- WLAN controller QoS profile setting of *platinum*, which assigns the highest prioritization to voice traffic.
- WMM policy is *required* (this precludes the use of clients that do not support WMM).
- Load-based Call Admission Control (CAC) should be specified for this WLAN. This prevents VoWLAN calls from being added to an access point that is unable to accept them without compromising call quality.
- The radio policy should be set to allow clients to access only this WLAN using 5 GHz. This helps to ensure that all secured voice devices take full advantage of the robust call capacity and reduced co-channel interference characteristics associated with 5 GHz.

For further information on best practices for voice applications, see the *Voice over Wireless LAN 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html.

- A *student WLAN* that uses web authentication for wireless access to the network using unmanaged and privately owned clients such as laptops, PDAs, iPod Touch, iPhones, and so on.

  This method of access is normally simple enough for all WLAN users and all platforms, regardless of manufacturer or model. A key challenge in managing wireless access for any large population of users possessing the freedom to choose their wireless clients is how to provide ubiquitous access while still providing an acceptable level of security. Because the ratio of students to network administrative staff is so heavily skewed in favor of the number of students, any student access WLAN solution should require virtually “zero touch” from campus community college network staff, while allowing the vast majority of devices on the marketplace to successfully connect to the network. Characteristics of the student WLAN include the following:

  - 802.1x /EAP authentication is not used. For simplicity of configuration across all devices, encryption is not configured on the student WLAN. Transport-level or application-layer encryption may be used if deemed applicable.
  - To provide access control and an audit trail, the student access WLAN authenticates the user via a web portal (“web authentication”) where all network access, apart from DHCP and Domain Name Service (DNS), is blocked until the user enters a correct username and password into an authentication web page.
  - The student WLAN client device user is re-directed to the web authentication web page whenever the client attempts to open any web page before successful web authentication. This authentication web page can be provided either by an internal WLAN controller web server or the NAC appliance in the Cisco Community College reference design. Usernames and passwords for authentication can reside on a RADIUS AAA server (such as Cisco ACS).
  - Broadcast SSID is enabled.
  - QoS profile setting of *silver* (best effort delivery).
  - WMM policy is set to *allowed*.

  - Radio policy should be set such that client access is allowed using either 2.4 GHz or 5 GHz.

- A *guest access* WLAN that uses web authentication for guest users of the campus network.

  Traffic to and from this guest access WLAN is tunneled to the DMZ transparently, with no visibility by, or interaction with, other traffic in the enterprise. The Cisco Community College reference design uses the Cisco Unified Wireless Network to provide a flexible, easy-to-implement method for deploying wireless guest access by using Ethernet in IP (RFC3378) within the Cisco Community College reference design. Ethernet in IP is used to create a tunnel across a Layer 3 topology between two WLAN controller endpoints (known as the *foreign* and *anchor* controllers). The foreign controller is the controller resident in the respective campus services block described earlier, whereas the anchor controller is resident within the network DMZ. The benefit of this approach is that no additional protocols or segmentation techniques must be implemented to isolate guest traffic travelling within the tunnel from all other enterprise traffic.

  See Guest Access, page 5-28 for further information regarding considerations surrounding the products and techniques used to provide guest access when designing for mobility in the Cisco Community College reference design.

  For technical information on Guest Access best practices in wireless networks, see the Guest Access section in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch10GuAc.html.

  Similar to the requirements stated earlier for the student access WLAN, the guest access WLAN must also be designed to accommodate campus guests (such as alumni, vendors, contractors, prospective students, parents, and so on) as well as the wide variety of WLAN guest clients they may bring onto the campus. Although their numbers will likely be much less compared to that of students, the WLAN clients brought onto campus by guest users are typically not managed or directly supported by community college campus network administrative staff. Because of the lack of control over the type of device used, mandating the use of 802.1x authentication and WPA or WPA2 encryption is usually not practical for guest access.

  Characteristics of the guest access WLAN include the following:

  - The guest access WLAN uses web authentication in a fashion similar to what was described in the student access WLAN, in order to provide access control and an audit trail.
  - The guest access WLAN user is re-directed to a web authentication web page whenever the user attempts to open any web page before successful authentication via the web portal. This authentication web page is provided by an internal WLAN controller web server in the Cisco Community College reference design. However, there is an option of using a non-controller-based web authentication server, such as the Cisco NAC Appliance. Usernames and passwords for authentication can reside on a RADIUS AAA server (Cisco ACS).
  - Broadcast SSID is enabled.
  - The guest access WLAN uses a QoS profile setting of *bronze* (less than best effort).
  - WMM policy is set to *allowed.*
  - Radio policy should be set such that client access is allowed to use either 2.4 GHz or 5 GHz.

  Additional information about the definition of controller WLANs and SSIDs can be found in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html.

WLAN Controller Mobility Groups

A *mobility group* is a group of WLAN controllers that behave as a single virtual WLAN controller, sharing essential end client, access point, and RF information. A given WLAN controller is able to make decisions based on data received from other members of the mobility group, rather than relying solely on the information learned from its own directly connected access points and clients. The WLAN controllers in a mobility group form a mesh of authenticated tunnels between themselves, affording any member controller the ability to efficiently communicate with any other member controller within the group.

Mobility groups are used to help facilitate seamless client roaming between access points that are joined to different WLAN controllers. The primary purpose of a mobility group is to create a virtual WLAN domain (across multiple WLAN controllers) to provide a comprehensive view of a wireless coverage area. Typically, two WLAN controllers should be placed in the same mobility group when an inter-controller roam is possible between access points. If the possibility of a roaming event does not exist, it may not make sense to put the WLAN controllers in the same mobility group.

For example, consider the scenario illustrated in Figure 5-8. Here we see a large and a medium building located on the same campus, in relatively close proximity to one another, with a small building located on a remote campus some distance away. Assume for the purposes of this example that the access points of each building are joined to a different WLAN controller, with the controllers servicing the large and medium building located within the main campus service block, and the WLAN controller servicing the smaller building located on the remote campus. The circular and oval patterns surrounding each building are intended to represent a very simplistic view of hypothetical outdoor RF coverage.

Figure 5-8 Campus Roaming

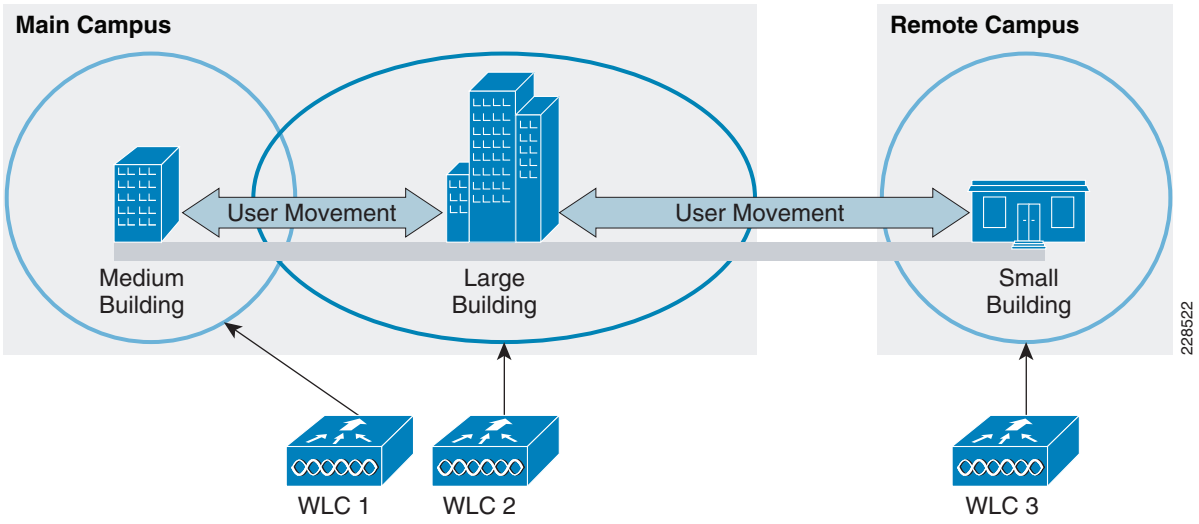


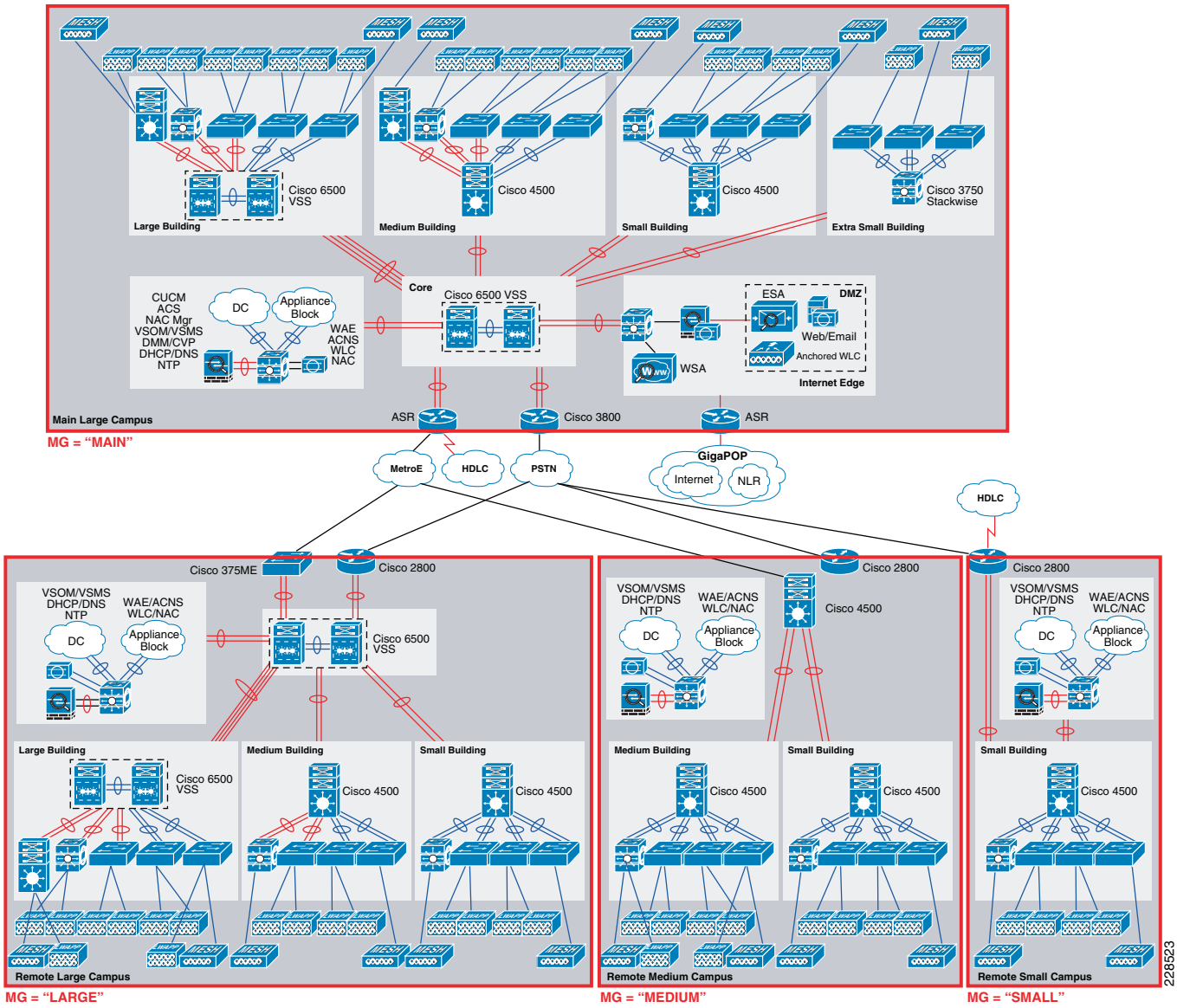
Figure 5-8 shows that there is overlapping coverage between the large and medium buildings, but not between the small building and any other building. This is because users must leave the main campus and traverse through a part of the town to get to the smaller remote campus, and vice versa. Because roaming is clearly possible between the medium and large building, but not between the small building and any other building, only the WLAN controllers servicing the medium and large building are required to be in the same mobility group. The WLAN controller servicing the small building may be configured to be a member of the same mobility group, but it is not mandatory in this case.

In applying the concept of mobility groups to the Cisco Community College reference design, consider the following:

- Within a community college or community college system comprised of one or more campuses, it is assumed that intra-campus roaming is possible between all buildings resident on the same campus. This may not actually be the case in all campuses, as some may have buildings co-located on the same campus where areas of non-coverage exist between them. However, assuming that intra-campus roaming is possible between all buildings allows us to make a design assumption that is generally applicable to both situations. Thus, in our Community College reference design, all WLAN controllers serving access points deployed on the same campus are placed within the same mobility group.
- It is also assumed that in the vast majority of cases, remote campuses are sufficiently distant from the main campus (as well as from one another) to render inter-campus roaming impractical. Allowing for the rare exception that two campuses may be adjacent or otherwise overlap one another, for the most part it is assumed that roaming between buildings located on different campuses is very unlikely.

Figure 5-9 provides a high-level illustration of how mobility group assignment can be handled in the Community College reference design. Note that *MG* refers to the mobility group name assigned for the campus.

Figure 5-9 Community College Mobility Groups



The following are some of the key design considerations concerning mobility groups:

- The controllers present at each campus are defined as members of a mobility group unique to that campus. Each controller in the same mobility group is defined as a peer in the mobility list of all controllers for that mobility group.
- If inter-campus roaming between two campuses is possible, the controllers at both campuses should be assigned into the same mobility group and defined as peers in the mobility list of all controllers for that mobility group.
- Because of high-speed WAN/MAN connectivity between campuses, access point failover to a remote backup controller resident at the main campus becomes feasible. To support this, access points can be configured to failover to a WLAN controller outside of their mobility group. This is discussed further in Controller Redundancy, page 5-39 and AP Controller Failover, page 5-41.

- A single mobility group can contain a maximum of 72 WLAN controllers. The number of access points supported in a mobility group is bound by the number of controllers and the access point capacity of each controller. Thus, for the Cisco 5508 Wireless Controller, a mobility group can have up to 72 times 250, or 18,000 access points.

The advantage of this approach to mobility group use is clarity and simplicity in deployment and administration. This is a key point when keeping in mind that the typical community college has a limited network administrative staff that is usually resource-constrained and very busy. By dividing the community college system into mobility groups as indicated in Figure 5-9, design simplicity is maintained. Given the large capacity of the Cisco 5508 Wireless Controller, the limitation on the maximum number of controllers per mobility group is not a significant tradeoff.

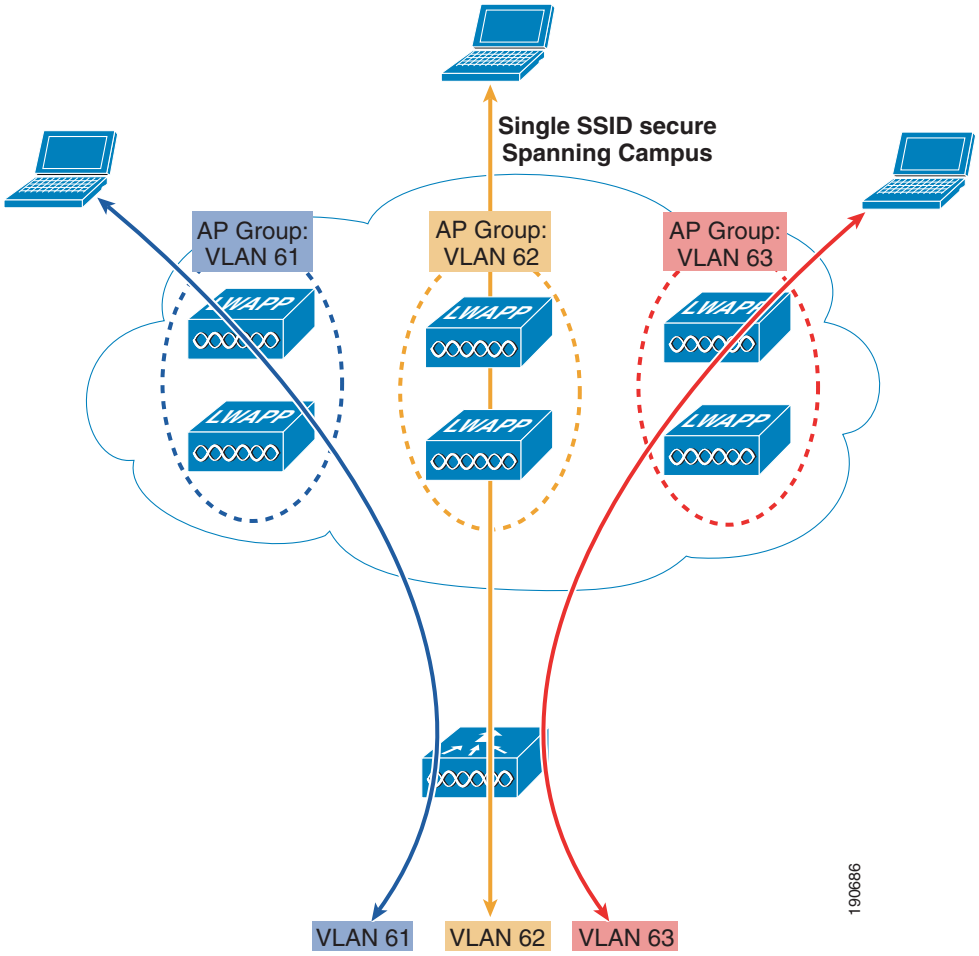
Additional information about WLAN controller mobility groups, including best practice information, can be found in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch2_Arch.html#wp1028143.

WLAN Controller Access Point Groups

Typically, each WLAN defined on the controller is mapped to a single dynamic interface (as shown earlier for the secure staff, VoWLAN, and student access WLANs). Consider the case however, where the Cisco 5508 Wireless Controller is deployed and licensed for 250 access points. Assume also that there are 10 users associated to each access point, using the same WLAN and SSID. This would result in 2500 users sharing the single VLAN to which the WLAN is mapped. A potential issue with this approach is that, depending on the particular overall network design, the use of subnets large enough to support 2500 users may not be possible.

To address this issue, the WLAN can be divided into multiple segments using the AP grouping capability of the WLAN controller. AP grouping allows a single WLAN to be supported across multiple dynamic VLAN interfaces on the controller. This is done by assigning a group of access points to an access point group at the WLAN controller, and then mapping the group to a specific dynamic interface. In this way, access points can be grouped logically, such as by building or set of buildings. Figure 5-10 shows the use of AP grouping based on site-specific VLANs.

Figure 5-10 Access Point (AP) Groups



As shown in Figure 5-10, three dynamic interfaces are configured, each mapping to a site-specific VLAN: VLANs 61, 62, and 63. Each site-specific VLAN is mapped to a group of access points that uses the same WLAN/SSID (AP groups one, two, and three). Thus, a faculty member associating to the WLAN using an access point that is part of AP group one is assigned an IP address from the VLAN 61 IP subnet. Likewise, a faculty member associating to the WLAN using an access point that is part of AP group two is assigned an IP address from the VLAN 62 IP subnet, and so on. Roaming between the site-specific VLANs is then handled internally by the WLAN controller as a Layer 3 roaming event. As such, the WLAN client maintains its original IP address.

Cisco 5508 Wireless Controllers can contain up to 192 access point group definitions, with up to 16 WLANs defined in each group. Each access point advertises only the enabled WLANs that belong to its access point group. Access points do not advertise disabled WLANs that are contained within its access point group, or WLANs belonging to another access point group.

In implementations of the Cisco Community College reference design where addressing limitations are present, the use of access point grouping to allow a single WLAN to be supported across multiple dynamic VLAN interfaces on the controller can be extremely beneficial.

WLAN Controller RF Groups

The strategy behind how *RF groups*, otherwise known as *RF domains*, are deployed within the Cisco Community College reference design represents another important deployment consideration that can affect overall accessibility. An RF group is a cluster of WLAN controllers that collectively coordinate and calculate their dynamic radio resource management (RRM) settings. Grouping WLAN controllers into RF groups in this way allows the dynamic RRM algorithms used by the Cisco Unified Wireless Network to scale beyond a single WLAN controller. In this way, the benefits of Cisco RRM for a given RF group can be extended between floors, buildings, and even across campuses.

Note Complete information regarding Cisco Radio Resource Management can be found in the *Cisco Radio Resource Management under Unified Wireless Networks* at the following URL: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml.

If there is any possibility that an access point joined to one WLAN controller may receive RF transmissions from an access point joined to a different WLAN controller, the implementation of system-wide RRM is recommended, to include both controllers and their access points. In this way, RRM can be used to optimize configuration settings to avoid 802.11 interference and contention as much as possible. In this case, both WLAN controllers should be configured with the same RF group name.

In general, Cisco prefers simplicity in the configuration of RF groups within the mobility design. Thus, all WLAN controllers in the Community College reference design are configured with the same RF group name. Although it is true that geographically disparate WLAN controllers have very little chance of experiencing RF interaction, and thus need not be contained in the same RF domain, for most community college deployments there is no disadvantage to doing so. An exception to this would be in extremely large deployments, as the maximum number of controllers that can be defined in a single mobility group is twenty. A clear advantage to this approach is simplicity of configuration and better support of N+1 controller redundancy (see Controller Redundancy, page 5-39 for further details).

A more detailed discussion as well as best practice recommendations regarding the use of RF groups can be found in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch2_Arch.html#wp1028184.

Access Points

In the Cisco Community College reference design, it is anticipated that each campus building requiring WLAN access will be outfitted with dual-band 802.11n access points providing RF coverage in both the 2.4 and 5 GHz bands. It is generally assumed that campus users will require WLAN access in most building interior areas, plus a 50–75 yard outdoor perimeter area surrounding each building. Of course, it is important to consider that most buildings will almost certainly contain some areas not intended for human entry or occupancy at any time. Similarly, some buildings may possess areas within the aforementioned outdoor perimeter that simply may not be accessible to campus users at any time. During your initial mobility design, these vacant areas may not be identified, so the precise subset of interior and exterior areas requiring WLAN access will likely be better determined during the site survey planning process that is an integral part of any wireless network deployment.

Note For more information on site survey planning, see the *Cisco 802.11n Design and Deployment Guidelines* at the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_80211n_design_and_deployment_guidelines.html.

In most community colleges, the vast majority of interior building WLAN access can be provided by the Cisco Aironet 1140 Series 802.11n access point (see Figure 5-11), which delivers pervasive wireless connectivity while blending in seamlessly with the aesthetics of most modern campus learning environments.

Figure 5-11 Cisco Aironet 1140 Series 802.11n Access Point (AIR-LAP1142N)

To deliver the right mix of style and performance, the Cisco Aironet 1140 Series 802.11n access point contains six integrated omni-directional antenna elements that incorporate the use of three hidden discrete elements for each frequency band. Ideal for indoor environments such as classrooms, corridors, libraries, faculty offices, and so on, the Cisco Aironet 1140 Series 802.11n access point has a visually pleasing metal housing covered by a white plastic shell that blends with the most elegant learning environments. The Aironet 1140 series 802.11n access point provides the ability to be powered directly from 802.3af power-over-Ethernet (PoE) while sustaining full-performance 802.11n connections on both of its radios simultaneously. In the Cisco Community College reference design, the model of the Cisco 1140 Series 802.11n access point recommended for most interior campus building locations is the AIR-LAP1142N.

Note Complete information (including country-specific ordering information) regarding the Cisco Aironet 1140 series 802.11n Access Point can be found at the following URL: http://www.cisco.com/en/US/products/ps10092/index.html.

Although the Cisco Aironet 1140 Series 802.11n access point is capable of servicing the bulk of all community college interior wireless access needs, there are some tradeoffs to consider in specialized situations. For example, in situations where the results of pre-site survey planning indicate that the use of external antennas are required to best meet specific RF coverage requirements, an access point providing external antenna connectors will be necessary. This can be a situation where a focused directional antenna pattern is required, or simply one where aesthetic requirements demand that the access point be completely hidden, with only a small antenna footprint exposed to public view. In other cases, perhaps one or more access points will need to be deployed in laboratory environments where the anticipated operating temperature extremes are not within common norms. Here, extended operating temperature tolerances beyond that of the Cisco Aironet 1140 Series 802.11n access point may be required.

To assist in addressing these and other rare but still significant deployment challenges that may be encountered on the community college campus, the Cisco Aironet 1250 Series 802.11n access point is recommended (see Figure 5-12).

Figure 5-12 Cisco Aironet 1250 Series 802.11n Access Point (AIR-LAP1252AG)

Designed with a next-generation ruggedized modular form factor, the Cisco Aironet 1250 Series 802.11n access point is intended for no-compromise performance in combination with the inherent expandability and customizability required to address challenging deployment situations. With robust modularized construction and six RP-TNC antenna jacks that allow antennas to be positioned independently of the access point itself, the Cisco Aironet 1250 Series 802.11n access point can be used to address situations requiring focused directional coverage patterns, extended operating temperature capabilities or minimal-footprint installations where it is highly preferable that the access point chassis is totally hidden from view. In the Cisco Community College reference design, the AIR-LAP1252AG model of the Cisco 1250 Series of access points is recommended for those and other types of demanding deployments.

Note To help discourage theft and vandalism, both the Cisco 1140 as well as 1250 Series 802.11n access points are manufactured with a security slot machined into the access point casing. You can secure either model access point by installing a standard security cable (such as the Kensington Notebook MicroSaver, model number 64068) into the access point security cable slot.

Complete information regarding the Cisco Aironet 1250 series 802.11n access point can be found at the following URL: http://www.cisco.com/en/US/products/ps8382/index.html. Additional information concerning the antenna options available for the Cisco Aironet 1250 Series 802.11n access point can be found at the following URL:
http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/at_a_glance_c45-513837.pdf

Note that Cisco Aironet 1140 Series 802.11n access points can power both 802.11n radios, at full transmit power running two spatial streams with encryption, while drawing only 15.4 watts of power from an 802.3af PoE Catalyst switch. A tradeoff associated with the use of Cisco Aironet 1250 Series 802.11n access points is that the AP-1250 Series requires slightly more power to reach its peak levels of performance, approximately 18.5 to 20 watts of power from a switch capable of providing enhanced-PoE (ePoE). Keep in mind, however, that if the full performance capability of the Cisco Aironet 1250 series access point is not necessary in your particular deployment, or you wish to support only a single RF band (i.e., either 2.4 GHz or 5 GHz) the Cisco Aironet 1250 Series 802.11n access point can also operate with 15.4 watts from a 802.3af PoE Catalyst switch.

To provide the Cisco Aironet 1250 Series 802.11n access point with 20 watts of input power, Cisco recommends the following power options:

- An ePoE Cisco Catalyst switch or switch blade module (such as the 3560-E, 3750-E, 4500E and 6500E Series.
- The use of a mid-span ePoE injectors (Cisco part number AIR-PWRINJ4). This option allows the Cisco Aironet 1250 series 802.11n access point to deliver full 802.11n performance while connected to any Cisco Catalyst switch. Power is injected directly onto the wire by the AIR-PWRINJ4 mid-span injector without reliance on the power output level of the switch itself.

Although its deployment flexibility is unparalleled within the marketplace, in most community college installation cases, the Cisco Aironet 1250 series 802.11n access point is typically only deployed only in those locations where they are necessary to address challenging situations. Other tradeoffs include a higher total cost per access point because of the added cost of external antennas, a larger footprint, and a heavier mounting weight as compared to the Cisco Aironet 1140 series 802.11n access point.

Note For the Cisco Aironet 1250 Series 802.11n access point, Cisco recommends performing your site survey using the same levels of PoE input power as you expect to use in your final deployment. For example, if you plan to deploy Cisco Aironet 1250 Series 802.11n access points with 15.4 watts of PoE, it is recommended for consistency and accuracy that perform your site survey using the same PoE input power levels.

The following design considerations regarding dual-band access points should be kept in mind when designing networks for dense user environments (for example, interior classrooms and lecture halls within community college campus buildings):

- *Use the 5 GHz band whenever possible*

  In general, this applies for both 802.11n as well as pre-802.11n wireless clients. The characteristics of 5 GHz operation make it advantageous for most users, and especially 802.11n users, for the following reasons:

  - Despite the maturity of 802.11 wireless LAN technology, the installed base of 5 GHz 802.11a clients generally is not nearly as widespread as 2.4 GHz 802.11b and 802.11g clients. A smaller installed base of users translates into less contention with existing clients and better operation at higher throughput rates.
  - The number of non-802.11 interferers (such as cordless phones and wireless personal networks) operating in the 5 GHz band is still just a fraction of the number found within the 2.4 GHz band.
  - The amount of available bandwidth found in the 5 GHz band is much greater than that of the 2.4 GHz band. In the United States, there are twenty-one 5 GHz non-overlapping channels that can be deployed. This translates into the ability to deploy with density and capacity in mind, and allow background resources such as Cisco RRM to handle channel and power output requirements accordingly.

- *Design and survey for capacity, not just maximum coverage*

  It is a natural tendency to try to squeeze the most coverage from each access point deployed, thereby servicing as much of the campus as possible with the lowest total access point investment. When designing networks for high-speed applications, attempting to design for maximum coverage at maximum transmitter output power can be counter-productive, as the maximum coverage footprint is typically attained using lower data rates and degraded signal-to-noise ratios. In addition, such false economies often sacrifice the ability to effectively make use of advanced tools such as Cisco RRM to address anomalies such as “coverage holes” and other deficiencies. Instead, the successful designer should design for capacity and generally aim to have access points installed closer together at lower power output settings. This approach allows for access point transmitter power to be dynamically managed via Cisco RRM. It also allows the practical use of higher data rates, provides RRM with the necessary transmission power “headroom” to allow for the ability to compensate for environmental changes, and facilitates the use of advanced capabilities such as location-based context-aware services.

- *Mount access points or antennas on the ceiling when possible*

Cisco Aironet AP-1140 Series 802.11n access points should be mounted on ceilings only. Ceiling mounting is recommended in general for the types of indoor environments found within community colleges, especially for voice applications. In the majority of carpeted indoor environments, ceiling-mounted antennas typically have better signal paths to handheld phones, taking into consideration signal loss because of attenuation of the human head and other obstacles.

Ceiling mounting locations are usually readily available, and more importantly, they place the radiating portion of the antenna in open space, which usually allows for the most efficient signal propagation and reception. Cisco Aironet 1250 Series 802.11n access points can be mounted as deemed necessary during pre-site survey planning or during the actual site survey process. However, ceiling mounting of Cisco Aironet 1250 Series access point antennas is highly recommended, especially for omni-directional style antennas.

- *Avoid mounting on surfaces that are highly reflective to RF*

  Cisco recommends that all antennas be placed one to two wavelengths from surfaces that are highly reflective to RF, such as metal. The separation of one or more wavelengths between the antenna and reflective surfaces allows the access point radio a better opportunity to receive a transmission, and reduces the creation of nulls when the radio transmits. Based on this recommendation, a good general rule of thumb then is to ensure that all access point antennas are mounted at least five to six inches away from any large metal reflective surfaces. Note that although recent technological advances have helped greatly in mitigating problems with reflections, nulls, and multipath, a sensible antenna placement strategy still is very important to ensure a superior deployment.

- *Disable legacy and low speed data rates*

  Globally disable any unnecessary low speed 802.11a/b/g data rates. Clients operating at low data rates (for example, 1, 2, and 5.5 Mbps) consume more airtime when compared to clients transmitting the same data payloads at higher data rates such as 36 Mbps and 54 Mbps. Overall system performance in any given access point cell drops significantly when a large percentage of low data rate frames tend to consume available airtime. By designing for capacity and disabling lower data rates, aggregate system capacity can be increased.

  Unless you are aware of specific reasons why one of the data rates described below are required in your deployment (such as the presence of clients that can transmit or receive *only* at these rates), the following actions are recommended:

  – For 2.4 GHz, disable the 1, 2, 5.5, 6, and 9 Mbps rates.

  – For 5 GHz, disable at a minimum the 6 and 9 Mbps rates.

  A common question concerning 2.4 GHz is why not disable 802.11b entirely? In other words, why not disable the 1, 2, 5.5, and 11 Mbps 2.4 GHz rates altogether? Although this certainly may offer advantages relating to better performance for 802.11g users, this approach may not be entirely practical, especially on guest access WLANs where a visitor might attempt to gain access using a device with embedded legacy radio technology that may not support 802.11g. Because of this, depending on the mix of clients in the environment, it may be wiser to simply disable only the three 802.11b data rates below 11 Mbps. Only if you completely confident that the situation just described is entirely not applicable in your environment should you consider completely disabling all 802.11b data rates.

Additional best practice guidelines for access point and antenna deployments can be found in the following reference documents:

- *Enterprise Mobility 4.1 Design Guide*— http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

- *Voice Over Wireless LAN 4.1 Design Guide*— http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

To provide outdoor WLAN access around the immediate perimeter area of each campus building, the Cisco Aironet 1520 Series Lightweight Outdoor Access Point is recommended (see Figure 5-13).

Figure 5-13 Cisco Aironet 1520 Series Lightweight Outdoor Access Point

As part of the Cisco Community College reference design, the Cisco Aironet 1520 Series Lightweight Outdoor Access Point provides an outdoor extension to the campus wireless network, with central management provided through WLAN controllers and the Cisco Wireless Control System. A very rugged enclosure allows for deployment outdoors without the need to purchase additional housings or third-party National Electrical Manufacturers Association (NEMA) enclosures to provide protection from extreme weather. The robust, weatherized housing of the Cisco Aironet 1520 Series Lightweight Outdoor Access Point can be painted to adapt to local codes and aesthetics.

Although the Cisco Aironet 1520 Series Lightweight Outdoor Access Point is part of the outdoor mesh series of Cisco access point products, a full outdoor mesh campus infrastructure is beyond the scope of the Cisco Community College reference design at this time. Rather, in this design Cisco Aironet 1520 Series Lightweight Outdoor Access Points are deployed only as root access points (RAPs), located outdoors on each building in such a manner that a satisfactory outdoor perimeter area is established. The precise location of these outdoor access points, as well as antenna choices, depends on the characteristics associated with the required coverage area and other particulars, and should be determined during pre-site survey planning.

For readers who wish to augment the recommendations made in this design guide and deploy a full campus outdoor mesh configuration, see the *Cisco Aironet 1520, 1130, 1240 Series Wireless Mesh Access Points, Design and Deployment Guide, Release 6.0* at the following URL: http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP_60.html.

In choosing among the various models of Cisco Aironet 1520 Lightweight Outdoor Access Points, readers may also wish to consider whether local campus, municipal, state or other public safety agencies are currently using or otherwise plan to deploy compatible 4.9 GHz public safety equipment (see note below) in emergency response vehicles. If this is the case, it may be wise to plan ahead in conjunction with campus and local public safety agencies to accommodate the use of this licensed band for connectivity from properly equipped first responders and emergency vehicles to your campus WLAN. In the event of a campus emergency, the ability to connect to and monitor in-building events, or access key safety and security applications, can significantly enhance the ability of law enforcement and other agencies to locate and combat threats.

Note In 2003, the U.S. Federal Communications Commission (FCC) allocated 50 MHz of spectrum in the 4.9 GHz band to public safety services. Public safety agencies can use this 4.9 GHz band to implement wireless networks with advanced services for the transmission of mission-critical information. Because

of the limited number of transmitters and the requirement for licensing, interference on the 4.9 GHz band tends to be below that of other bands, such as 2.4 GHz and 5 GHz. Communications using the 4.9 GHz public safety band must be related to the protection of life, health, or property. Examples include WLANs for incident scene management, mobile data, video surveillance, VoWLAN, fixed point-to-point, and so on.

Even if 4.9 GHz access is not available on campus, public safety agencies may still be able to access the campus WLAN using standard 2.4 GHz or 5 GHz unlicensed bands. This depends on whether the emergency response vehicles of the agencies in question are equipped to do so, as well as the configuration of their equipment. Keep in mind that when public safety users access campus WLANs using unlicensed 2.4 GHz and 5 GHz frequencies during crisis events, they must also contend for access with other unlicensed users of these frequencies, as well as deal with any interference from other sources located within those bands.

With this in mind, the particular model of outdoor access point recommended for outdoor perimeter building coverage, depending on the inclusion of 4.9 GHz as follows:

- The Cisco Aironet 1524PS (Public Safety) Lightweight Outdoor Access Point includes 4.9 GHz capability and provides flexible and secure outdoor WLAN coverage for both public safety and mobility services. The Cisco Aironet 1524PS Public Safety Lightweight Outdoor Access Point is a multiple-radio access point that complies with the IEEE 802.11a and 802.11b/g standards, as well as 4.9 GHz public safety licensed operation parameters. This access point can support independent data exchanges across all three radios simultaneously. The main tradeoff with the Cisco Aironet 1524PS Public Safety Lightweight Outdoor Access Point is the added purchase and deployment cost. However, in environments where public safety agencies are already equipped with compatible 4.9 GHz clients, the added benefits and advantages afforded by the 1524PS are often considered worthwhile. The model of Cisco Aironet 1524PS Public Safety Lightweight Outdoor Access Point recommended in the Cisco Community College reference design is the AIR-LAP1524PS.
- The Cisco Aironet 1522 Outdoor Lightweight Access Point is a dual-radio, dual-band product that is compliant with IEEE 802.11a (5-GHz) and 802.11b/g standards (2.4-GHz). Designed for demanding environments, the Cisco Aironet 1522 provides high performance device access through improved radio sensitivity and range performance. The tradeoffs of deploying this model are the lack of 4.9 GHz licensed public safety support in environments where 4.9 GHz is in use among public safety agencies. The model of Cisco Aironet 1522 Lightweight Outdoor Access Point recommended in the Cisco Community College reference design for deployments without 4.9GHz is the AIR-LAP1522AG.

Cisco offers a wide array of antenna options for the entire range of Cisco Aironet 1520 Series Lightweight Outdoor Access Points. Information on these antenna options can be found in the *Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide* at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet0900aecd8066a157.html.

All models of the Cisco Aironet 1520 Series Lightweight Outdoor Access Point can be powered from a multitude of sources, include PoE, direct DC, or direct AC. The entire range of power input options is described in the *Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide*.

Note Although the Cisco Aironet 1520 Series Lightweight Outdoor Access Point can be conveniently powered via PoE, a power injector (Cisco AIR-PWRINJ1500-2) specific to this product line must be used. Do not use any other power injector or Ethernet switch PoE capability (including enhanced PoE switches) in an attempt to directly provide PoE to Cisco Aironet 1520 Series Lightweight Outdoor Access Points. The Cisco Aironet 1520 Series Lightweight Outdoor Access Point is approved for use only with the Cisco AIR-PWRINJ1500-2 power injector. Keep in mind that although the Cisco Aironet 1520 Series

Lightweight Outdoor Access Point is intended to be installed exposed to outdoor weather elements, the AIR-PWRINJ1500-2 power injector is approved for indoor installation only.

Usability

This section discusses the mobility design considerations pertaining to those aspects of the Cisco Community College reference design that are relevant to overall usability, such as the following:

- Quality-of-service (QoS)
- Guest access
- Traffic and performance

Quality-of-Service

The WLAN controller should be configured to set the 802.1p marking of frames received and forwarded onto the wired VLAN to reflect the QoS policy used on this WLAN. Therefore, if the WLAN controller is connected to a switch that is configured to trust the class-of-service (CoS) and maintain a translation table between CoS and Differentiated Services Code Point (DSCP), the translation between wireless QoS policy and wired network QoS policy occurs automatically.

In the Cisco Community College reference design, WLAN traffic is prioritized based on the QoS profiles (platinum, silver, bronze, and so on) applied to each WLAN. However, this does not change the IP QoS classification (DSCP) of the client traffic carried, which means that client traffic leaving WLAN controllers may need to be reclassified based on network policy.

This may be achieved via one of following approaches:

- Applying policy at each of the switch virtual interfaces (SVIs) connecting the WLAN controller to the wired network
- Learning the QoS policy that has already been applied by the wireless networking components, because this should already be in alignment with the overall network policy

In the Cisco Community College reference design, the plan is to use the latter approach, because it provides both the advantage of initial configuration simplicity as well as ongoing ease of maintenance. This technique requires only that the QoS profiles be maintained on the WLAN controllers themselves, without the need to configure explicit policies on adjacent switches. Switches need to be configured to trust only the QoS of frames forwarded to them by the WLAN controller.

To implement this approach, the WLAN controller should be configured to set the 802.1p marking of packets forwarded onto wired VLANs to reflect the QoS policy used on the specific WLAN from which they were received. Therefore, if the WLAN controller is connected to a switch that is configured to trust CoS and maintain a translation table between CoS and DSCP, the translation between wireless and wired network QoS policy occurs automatically.

For example, assume a packet received originates from a WLAN to which a platinum QoS profile has been assigned. This translates to a DSCP value of EF; therefore, the WLAN controller assigns a CoS value of 5 in the header of the frame that carries this data to the wired switch. Similarly, if the same packet originates from a WLAN assigned a QoS profile of silver, the translated CoS value is 0.

For more information on WLAN QoS, see the following URLs:

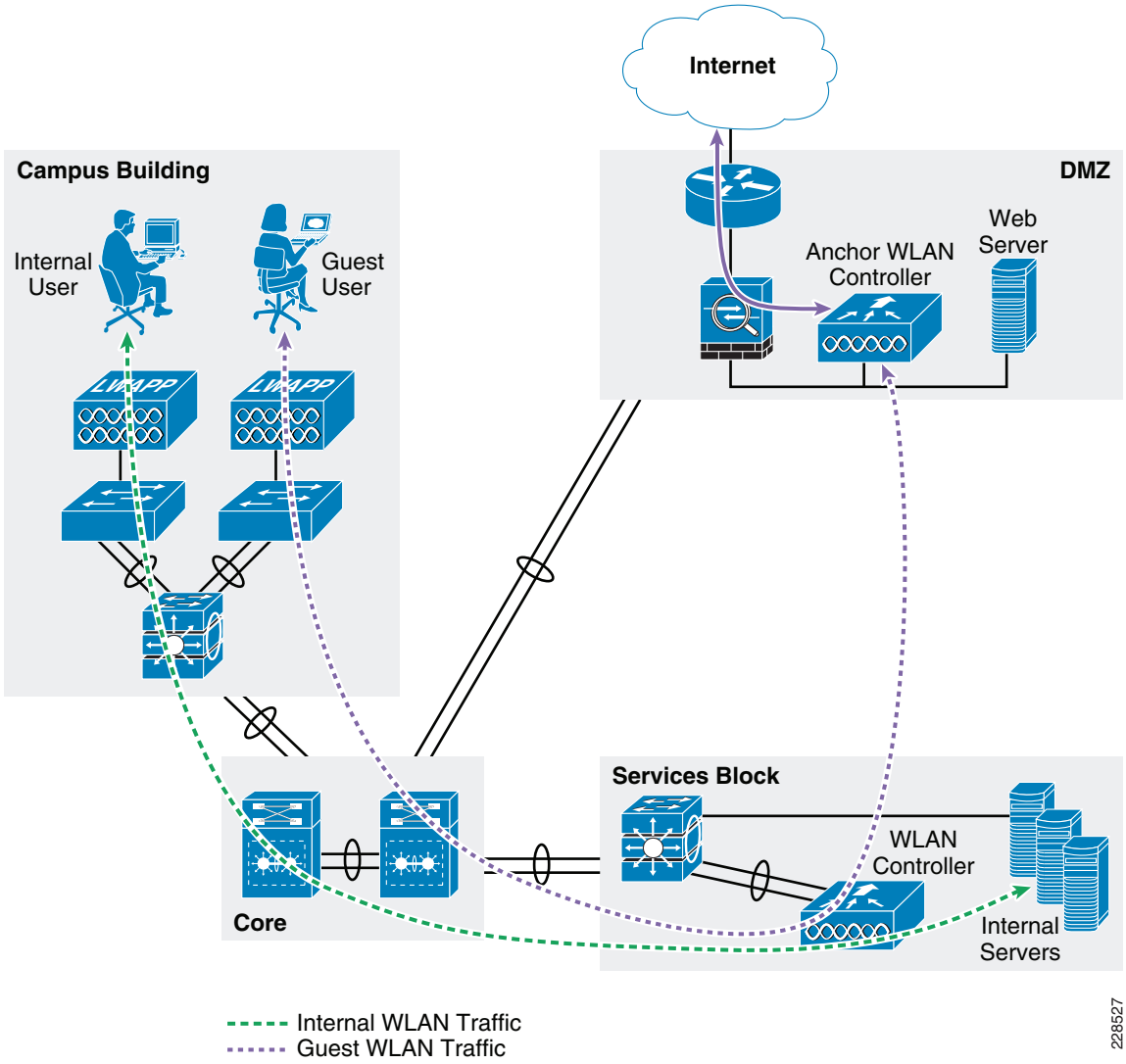
- *Voice over Wireless LAN 4.1 Design Guide 4.1*—http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html.

- *Enterprise Mobility 4.1 Design Guide*—http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch5_QoS.html

Guest Access

The Cisco Community College reference design uses the Cisco Unified Wireless LAN Guest Access option to offer a flexible, easy-to-implement method for deploying wireless guest access via Ethernet over IP (EoIP), as described in RFC3378. EoIP tunneling is used between two WLAN controller endpoints in the centralized network design. The benefit of this approach is that there are no additional protocols or segmentation techniques necessary to achieve guest traffic isolation in relation to other internal traffic. Figure 5-14 shows a high-level view of guest access using this technique with a centralized WLAN controller design.

Figure 5-14 Guest Access Solution High-Level Overview



As shown in Figure 5-14, a WLAN controller with a specific purpose is located in the main campus DMZ, where it is referred to as an *anchor controller*. The anchor controller is responsible for terminating EoIP tunnels originating from centralized campus WLAN controllers, and interfacing the traffic from these controllers to a firewall or border router. As described in earlier sections of this document, the centralized campus WLAN controllers are responsible for termination, management, and standard operation of the various WLANs provisioned throughout the enterprise, including one or more guest WLANs. Instead of being switched locally to a corresponding VLAN on the campus controller, guest WLANs are instead transported via the EoIP tunnel to the anchor controller in the DMZ.

When an access point receives information from a WLAN client via the guest access WLAN/SSID, these frames are encapsulated using CAPWAP from the access point to the campus WLAN controller. When received at the WLAN controller, they are encapsulated in EoIP from there to the anchor controller. After reaching the anchor controller, these frames are de-encapsulated and passed to a firewall or border router via the guest VLAN. The use of EoIP and an anchor WLAN controller in the DMZ allows guest user traffic to be transported and forwarded to the Internet transparently, with no visibility by, or interaction with, other traffic in the enterprise.

Because the anchor controller is responsible for termination of guest WLAN traffic and is positioned within the Internet DMZ, firewall rules must be established to limit communication between the anchor controller and only those controllers authorized to establish EoIP tunnels to them. Such rules might including filtering on source or destination controller addresses, UDP port 16666 for inter-WLAN controller communication, and IP protocol ID 97 (Ethernet over IP) for client traffic. Other rules that might be needed include the following:

- TCP 161 and 162 for SNMP
- UDP 69 for TFTP
- TCP 80 or 443 for HTTP, or HTTPS for GUI access
- TCP 23 or 22 for Telnet, or SSH for command-line interface (CLI) access

The following are other important considerations to keep in mind regarding the use of this guest access solution:

- For the best possible performance, Cisco strongly recommends that the anchor controller be dedicated to supporting EoIP guest access tunneling only. In other words, do not use the anchor controller for any other purpose but EoIP guest access tunneling. In particular, in addition to its guest access role, the anchor controller should not be used to control and manage other access points in the enterprise.
- When deploying a Cisco 5508 Wireless Controller as an anchor controller, keep in mind that because the anchor controller is not going to be used to manage access points, it can be licensed to support only a minimal number of access points. For example, a Cisco CT5508-12 (12 access point-licensed capacity) can function quite well as an anchor controller in the Cisco Community College reference design, even in networks where hundreds or thousands of access points may be joined to other campus Cisco 5508 Wireless Controllers.
- Multicast traffic is not supported over guest tunnels, even if multicast is enabled on wireless controllers.
- The mobility group name of the anchor controller should differ from that configured for campus controllers. This is done to keep the anchor controllers logically separate from the mobility groups associated with the general campus wireless deployment.
- The mobility group name for every campus WLAN controller that establishes EoIP tunnels with the anchor controller must be configured as a mobility group member in the anchor controller configuration.

Finally, although the focus for the Cisco Community College reference design is on the pure controller-based guest access solution, note that other, equally functional solutions are available that combine what is discussed in this section with the use of an access control platform external to the WLAN controller. For example, the guest access solution topology described in this section can be integrated with the Cisco NAC Appliance. This might be the case, for example, if the community college has already deployed the Cisco NAC Appliance within their Internet DMZ to support wired guest access services. As shown in Figure 5-15, the wireless guest access topology remains the same, except that in this scenario, the guest VLAN interface on the anchor controller connects to an inside interface on the NAC Appliance, instead of to a firewall or border router.

Figure 5-15 Cisco UWN Guest Access with Anchor WLC and NAC Appliance

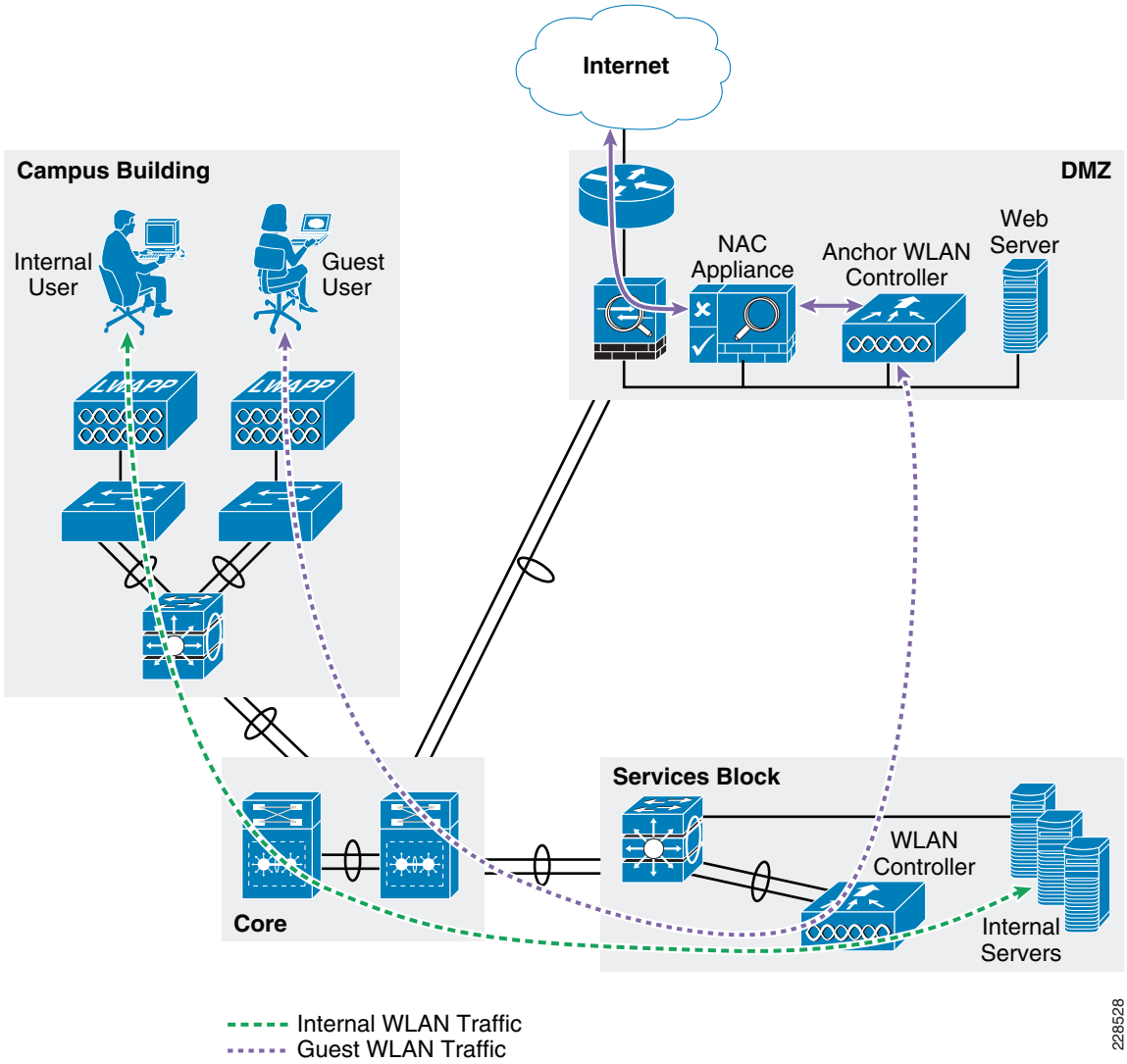
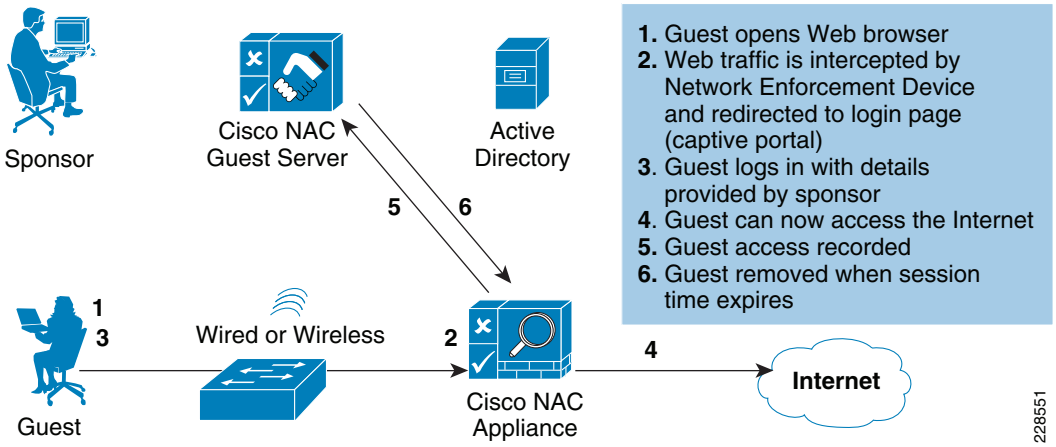


Figure 5-15 shows that the NAC Appliance is responsible for redirection, web authentication, and subsequent access to the Internet. The campus and anchor controllers are used only to tunnel guest WLAN traffic across the enterprise into the DMZ, where the NAC appliance is used to actually control guest access. The tradeoff here is the added cost of the external access control solution, versus the benefits it affords in relation to your particular deployment.

Note Additional information concerning the design and deployment of the Cisco Unified Wireless Network guest access solution can be found in the *Enterprise Mobility 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch10GuAc.html#wp999659.

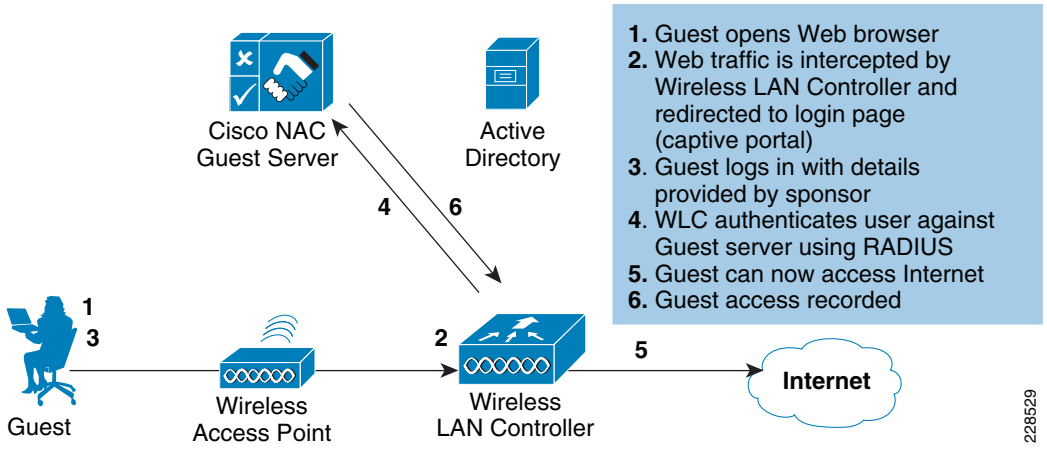
The Cisco NAC Guest Access Server is another member of the Cisco Network Admission Control solution family that can further enhance the utility of your design by assisting network administrators in the provisioning of guest access user accounts. The NAC Guest Access Server facilitates the creation of guest accounts for temporary network access by permitting provisioning by authorized personnel in a simple and secure manner. In addition, the whole process is recorded in a single place and stored for later reporting, including details of the network access activity. Cisco NAC Guest Server integrates with Cisco NAC Appliance through an application programming interface (API), allowing for guest accounts to be controlled via the Guest Server user interface, including creation, editing, suspension, and deletion of accounts. The Cisco NAC Guest Server then controls these accounts on the Cisco NAC Appliance through the API (shown in Figure 5-16). In addition, the Guest Server receives accounting information from the NAC Appliance to enable full reporting.

Figure 5-16 NAC Guest Server with NAC Appliance and WLAN Controller



Cisco NAC Guest Server can also integrate directly with Cisco WLAN controllers through the RADIUS protocol, allowing for guest accounts to be controlled via the Guest Server user interface, including the creation, editing, and deletion of guest accounts. In this case, the WLAN controller makes use of the NAC Guest Server to authenticate guest users (shown in Figure 5-17). In addition, the Guest Server receives accounting information from the WLAN controller to enable full reporting.

Figure 5-17 NAC Guest Server with WLAN Controller Alone



Note For more information on the Cisco NAC Guest Server, see the following URL: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd806e98c9.html.

Traffic and Performance

When designing mobility solutions incorporating the tunneling of CAPWAP traffic across campus infrastructure, questions often arise concerning the impact of such tunneling on network performance. In examining the impact of CAPWAP traffic in relation to overall network traffic volume, the following three points should be considered:

- *CAPWAP control traffic volume*—CAPWAP control traffic volume can vary considerably depending on the current activity state of the network. For example, this type of traffic volume usually reaches a zenith during a software upgrade or WLAN controller reboot. In most campuses, however, this degree of sporadic loading is considered negligible, and is of no consequence when considering the merits of a centralized deployment model over other options.
- *Tunneling overhead*—A Layer 3 CAPWAP tunnel adds a relatively negligible amount of overhead to a typical IP packet traversing to and from a WLAN client.

Note A previous examination of the Light Weight Access Point Protocol (LWAPP), the predecessor to CAPWAP and similar in many ways, indicates that this overhead is approximately 44 bytes. With that said, traffic studies have concluded that the average load LWAPP control traffic places on the network is approximately 0.35 Kb/sec. Given that average packets sizes found on large scale network deployments are approximately 300 bytes, this represents an overhead of approximately 15 percent.

Once again, this is generally viewed as resulting in little to no consequence, especially in light of the considerable merits associated with a centralized deployment versus other options.

- *Traffic engineering*—WLAN traffic tunneled to a centralized controller is typically routed from the location of the WLAN controller to its final destination in the network. In the case of the Cisco Community College reference design, established best practices are followed concerning the placement of WLAN controllers within each per-campus centralized services block. With that said, the longer tunnels and traffic flows associated with a centralized deployment model can be mitigated

by positioning the WLAN controllers in that part of the network where a large portion of the client traffic is already destined. In the Cisco Community College reference design, client-to-host/server traffic is typically destined for a local campus or main campus data center. This being the case, the overhead associated with any inefficiencies introduced because of centralized placement is not seen as adding significant delay or overhead.

Manageability

As mentioned earlier, each WLAN controller in the Cisco Community College reference design provides both a CLI as well as a graphical web user interface, which are primarily used for controller configuration and management. These user interfaces provide ready access to the network administrator. However, for a full-featured, centralized complete lifecycle mobility management solution that enables community college network administrators to successfully plan, configure, deploy, monitor, troubleshoot, and report on indoor and outdoor wireless networks, the use of the Cisco Wireless Control System (WCS) is highly recommended (see Figure 5-18).

Figure 5-18 Cisco Wireless Control System

The Cisco Wireless Control System allows very effective management of wireless networks supporting high-performance applications and mission-critical solutions. Effective management of these networks helps to simplify college network operation and improve the productivity of administrators, staff, and faculty. The comprehensive Cisco WCS platform scales to meet the needs of small, midsize, and large-scale WLANs across local and remote campuses. Cisco WCS gives college network administrators immediate access to the tools they need when they need them, wherever they may be located within the community college.

Operational costs are significantly reduced through a simplified and intuitive GUI, with built-in tools delivering improved efficiency and helping to reduce training costs, even as the campus network grows incrementally larger. Cisco WCS lowers operational costs by addressing the whole range of mobility management requirements (radio frequency, access points, controllers, mobility services, and so on) using a single unified management platform deployed in a centralized location, and with minimal impact on staffing requirements.

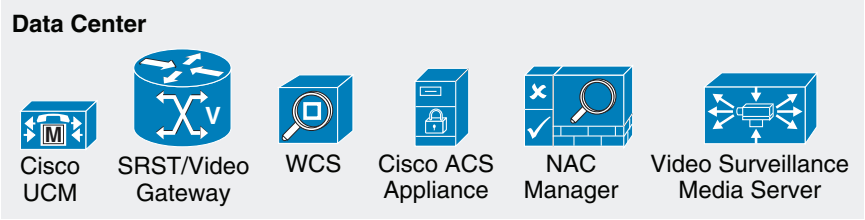
Cisco WCS can scale to manage hundreds of Cisco WLAN controllers, which in turn can manage thousands of Cisco Aironet access points. For installations where network management capabilities are considered mission-critical, WCS also supports a software-based high availability option that provides

failover from a primary (active) WCS server to a secondary (standby). Adding mobility services such as context-aware software and adaptive wireless intrusion prevention systems (wIPS) is simplified through Cisco WCS integration with the Cisco Mobility Services Engine (MSE).

Note A detailed description of each management feature and benefit available in the Cisco Wireless Control System is beyond the scope of this chapter, but the information can be found at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html.

In the Cisco Community College reference design, a centralized WCS management server located in the data center block within the main campus is used. The data center block was initially shown in Figure 5-3. Figure 5-19 provides greater detail and magnification.

Figure 5-19 WCS Within the Data Center Block



The current upper limit for scaling WCS on a high-end server is up to 3000 Cisco Aironet CAPWAP-based access points, and up to 750 Cisco WLAN controllers. As such, most implementations of the Cisco Community College reference design are well served by a mobility design using a WCS management server located on the main campus.

Note For further information on WCS hardware platforms and requirements, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0wst.html#wp1061082.

The planning, configuration, deployment, monitoring, reporting, auditing, and troubleshooting made available by WCS are accessible to any authorized community college network administrator via standard secured web browser access.

Generally speaking, it is anticipated that access to WCS will be restricted to network administrators and their staff located at the main and remote campuses, as well as faculty administrators and staff. However, these groups will not all have equivalent resource and functionality access. It is anticipated that resource access will be limited further, based on administrative level and assigned campus or campuses. With few exceptions, it is not anticipated that most students will be required nor authorized to use the majority of services offered by WCS.

In this design, the ability to query and manage campus mobility resources is regulated using the virtual domain feature of WCS, in conjunction with the appropriate assignment of WCS user rights. Thus, although key members of the main campus central network administration staff may possess the authority to manage any and all mobility resources located on any campus throughout the college system, remote campus administrators may be limited by the following:

- *Campus resource management visibility policy*—This is performed by assigning the network mobility infrastructure components associated with each campus to a WCS virtual domain, and assigning the virtual domains to appropriate network administrators. Key members of the central administrative staff are assigned to the WCS root domain, granting them overall authority to view

and configure all mobility infrastructure resources, on any campus, via their WCS management consoles. However, personnel responsible for local campus network administration are restricted to the discrete mobility infrastructure components associated with the virtual domain representing their local campus. These infrastructure components include WLAN controllers, access points, configuration templates, WCS events, reports, alarms, WLAN clients, and so on.

- *Campus resource management access policy*—Although the visibility of a resource is determined by WCS virtual domain assignment, the subset of acceptable actions that are allowed against any visible resources are further regulated by the assignment of appropriate WCS user and group rights, which allow policies to be applied that further limit what actions each may be allowed against any visible resources.

Via the WCS GUI interface, virtual domains (as well as WCS user rights) can be assigned at the WCS server or using an external security manager such as Cisco Secure ACS.

Note Further information regarding how WCS virtual domains may be used to limit individual campus network administrator access to segments of the mobility network outside of their scope of responsibility, while still providing for overall "root" administrator control of the entire wireless network, may be found at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/brochure_c02-474335.html.

Guest access credentials can be created and managed centrally using the Cisco WCS. A network administrator can create a limited privilege account within WCS that permits "lobby ambassador" access for the purpose of creating guest credentials. With such an account, the only function a lobby ambassador is permitted is to create and assign guest user credentials to controllers that have web-policy configured WLANs. In the rare event that a centralized WCS management system is not available because of a server failure, a network administrator can establish a local administrator account on the anchor WLAN controller, with lobby ambassador privileges, as a backup means of managing the guest access solution.

The use of a centralized WCS management server in the Cisco Community College reference design provides key advantages such as reduced initial deployment cost and ease of maintaining server resources in a centralized location, coupled with good performance across modern high-speed LANs and WANs. Of course, as with any design choice, certain tradeoffs exist, such as the following:

- *WCS server failure*

  In the Cisco Community College reference design, the centralized mobility network management services provided by WCS are not regarded as being mission-critical for the majority of community college deployments. Thus, in the rare event of a WCS server failure, and given the cost constraints of most community college environments, it is assumed that direct WLAN controller management workarounds (such as that described earlier for guest access management) are an acceptable cost compromise. Any downtime realized because of a WCS server failure, although undoubtedly very inconvenient, would in most cases not be viewed as entirely catastrophic. This being the case, the Cisco Community College reference design does not at this time provide for the added cost of a secondary WCS management server in an N+1 software-based high-availability arrangement. However, deployments where WCS management services are critical to the mission of the community college should instead consider modifying the design to include the services of a secondary WCS management platform configured for N+1 software-based high-availability.

Note For more information on WCS high availability configurations, see the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0admin.html#wp1132580.

- *Unrecoverable WAN failure*

  A catastrophic, unrecoverable WAN failure can interrupt management traffic between WCS and the WLAN controllers that are located on remote campuses. One way to protect against this is to distribute the WCS management server function out further into the network, and centralize WCS management on a per-campus basis. However, this increases the cost of WCS deployment significantly, requiring one WCS management server per campus, and preferably a Cisco WCS Navigator management aggregation platform located at the main campus site. Because it is believed that the centralized mobility network management services provided by WCS are not regarded as mission-critical to the majority of community colleges, these decentralized management options are not included in the Cisco Community College reference design at this time. Instead, it is assumed that in this type of a rare occurrence, the aforementioned ability to minimally manage WLAN controllers directly will suffice, should any network management intervention be required in such circumstances.

Note For more information on WCS Navigator, see the following URL: http://www.cisco.com/en/US/products/ps7305/index.html.

Reliability

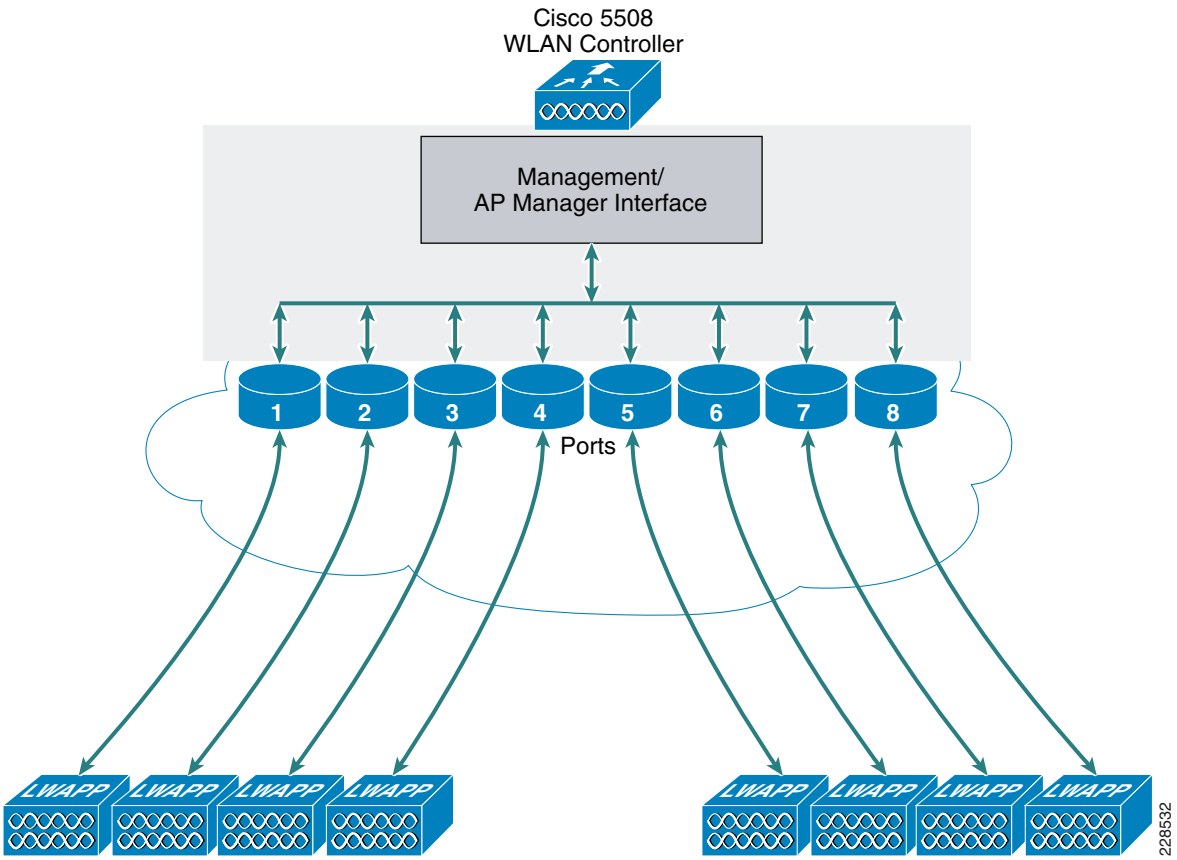
This section discusses the mobility design considerations pertaining to those aspects of the Cisco Community College reference design relevant to overall reliability, and includes the following:

- Controller link aggregation
- Controller redundancy
- AP controller failover

Controller Link Aggregation

An important capability used to enhance the reliability of WLAN controller interconnection to the wired network is *link aggregation* (*LAG*). As mentioned earlier, LAG is a partial implementation of the 802.3ad port aggregation standard. It bundles all the controller distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to make use of all controller wired ports. When LAG is enabled, the system dynamically manages port redundancy and load balances access points across each port, without interaction from the network administrator. With the Cisco 5508 Wireless Controller and the release 6.0 software used in the Cisco Community College reference design, all eight ports can be bundled together into a single Gigabit EtherChannel interface. LAG is effective in distributing access point traffic across all controller ports, as shown in Figure 5-20. This can be especially important with high capacity controllers licensed for many access points, such as the Cisco CT5508-250.

Figure 5-20 LAG in the Cisco 5508 WLC



LAG simplifies controller configuration and improves the overall solution reliability. If any of the controller ports fail, traffic is automatically migrated to one of the remaining ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

The Gigabit Ethernet connections comprising the LAG (up to eight on the Cisco 5508 Wireless Controller) should be distributed among different modular line cards or switch stack members in the services block to the greatest degree possible. This is done to ensure that the failure of a single line card or switch stack member does not result in total failure of the WLAN controller interconnection to the campus network.

For example, if there are four switch stack members in the services block and LAG is configured using all eight WLAN controller interfaces, the Gigabit Ethernet links from the services switch block to the WLAN controller should be distributed two per services block switch stack member. In this way, if any switch stack member fails, six other Gigabit Ethernet links to the WLAN controller remain ready, active, and available to pass data.

The switch features required to implement this connectivity between the WLAN controller and the services block are the same switch features that are otherwise generally used for EtherChannel connectivity between switches.

When using a Cisco 5508 Wireless Controller with link aggregation enabled, it is important to keep the following considerations in mind:

- When the port channel is configured as “on” at both ends of the link, it does not matter if the Cisco Catalyst switch is configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP), because no channel negotiation occurs between the controller and the switch.

The recommended load balancing method for Cisco Catalyst switches is by use of the CLI command **src-dest-ip**.

- You cannot configure the controller ports into separate link aggregation groups. Only one link aggregation group is supported per controller. Therefore, you can connect a controller in link aggregation mode to only one neighbor switch device (note that this can be a switch stack with multiple member switches).
- When you enable link aggregation or make any changes to the link aggregation configuration, you must immediately reboot the controller.
- When you enable link aggregation, only one AP manager interface is needed because only one logical port is needed. The in-band management interface of the Cisco 5508 Wireless Controller can also serve as the AP manager interface.
- When you enable link aggregation, all Cisco 5508 Wireless Controller distribution ports participate in link aggregation by default. Therefore, you must configure link aggregation for all the connected ports in the neighbor switch that have been outfitted with small form-factor plug-in (SFP) modules.
- When you enable link aggregation, only one functional physical distribution port is needed for the controller to pass client traffic. Although Cisco 5508 Wireless Controllers have no restrictions on the number of access points per port, Cisco recommends that if more than 100 access points are connected to the controller, make sure that at least two or more Gigabit Ethernet interfaces are used to connect the controller to the services block.
- As mentioned previously, there are eight SFP interfaces on the Cisco 5508 Wireless Controller. These may be fully deployed to take full advantage of multilayer campus design guidelines regarding the oversubscription of access layer uplinks. By doing so, it is relatively straightforward to design a solution that delivers access layer uplinks from the WLAN controller with an oversubscription rate of between 8:1 and 20:1 (Note that these oversubscription rates are not unique to wireless products and are equivalent with what is typically seen in wired networks as well.)

  Table 5-1 provides information for the Cisco 5508 Wireless Controller deployed with its maximum complement of 250 access points.

Table 5-1 Cisco 5508 Wireless Controller Oversubscription Rates

Throughput per AP (Mbps)	Cisco 5508 Wireless Controller Oversubscription Rate (8 Gbps)
25	1:1
50	2:1
100	4:1
150	5:1
200	7:1
250	8:1

Table 5-1 shows that even if designing for peak 802.11n throughput of 250 Mbps per access point, oversubscription is not expected to exceed campus design guidelines of 8:1 when using all the available controller interfaces with LAG.

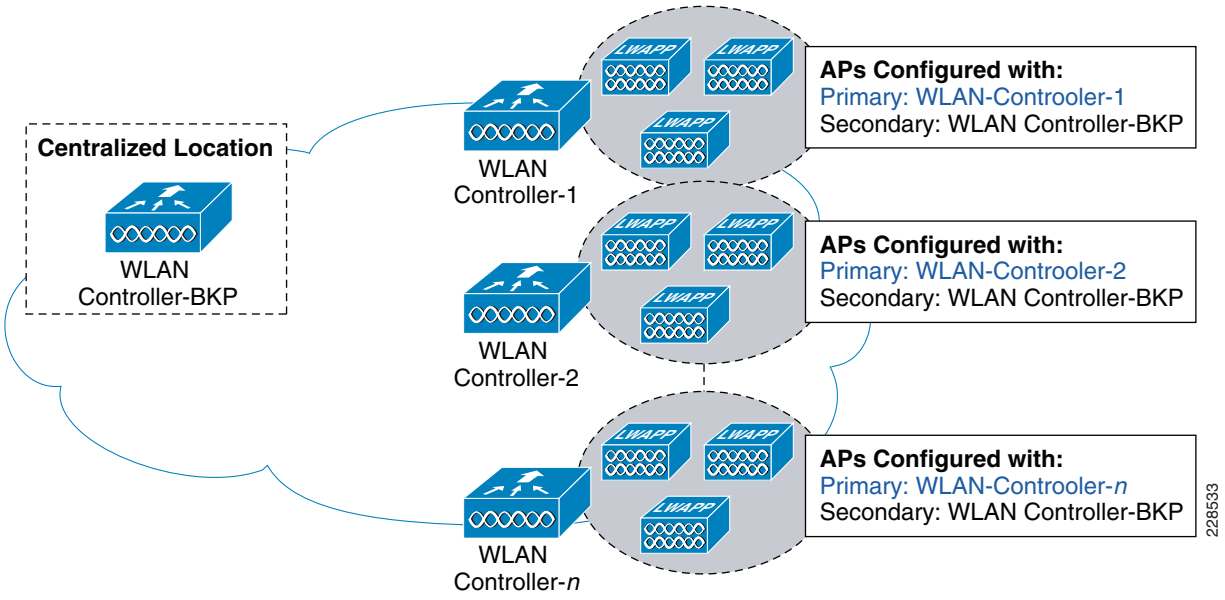
Note For more information concerning WLAN controller link aggregation, see *Deploying Cisco 440X Series Wireless LAN Controllers* at the following URL: http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1062211.

Controller Redundancy

The ability of the solution to recover from a reasonable degree of component failure is important in ensuring the reliability of any WLAN networking solution. This is especially important when there are many users that may rely on a centralized component, such as a WLAN controller, for access into the network. An easy solution is to have a "hot" standby secondary controller always at the ready for each primary controller in active service (otherwise known as 1:1 controller redundancy). Although this offers the highest degree of protection from any number of failed primary controllers, it is also the most costly approach.

In the Cisco Community College reference design, unforeseen controller failures are avoided using an "N+1" controller redundancy model, in which the redundant WLAN controller is placed in a central location and acts as a backup for multiple active WLAN controllers. Each access point is configured with the name or IP address of its primary WLAN controller, but is also configured with the name or IP address of the redundant controller as its secondary WLAN controller. The N+1 controller redundancy approach is based on the assumption that the probability of more than one primary WLAN controller failure occurring simultaneously is very low. Thus, by allowing one centralized redundant controller to serve as the backup for many primary controllers, high availability controller redundancy can be provided at a much lower cost than in a traditional 1:1 redundancy arrangement. Figure 5-21 provides a general illustration of the principle of N+1 controller redundancy.

Figure 5-21 General N+1 WLAN Controller Redundancy



The main tradeoff associated with the N+1 redundancy approach is that the redundant controller may become oversubscribed if multiple primary controllers fail simultaneously. In reality, experience indicates that the probability of multiple controller failures is low, especially at geographically separate

site locations. However, when designing an N+1 redundant controller solution, you should assess the risk of multiple controller failures in your environment as well as the potential consequences of an oversubscribed backup controller. In situations where there is reluctance to assume even this generally small degree of risk, other controller redundancy approaches are available that can provide increasingly greater degrees of protection, albeit with associated increases in complexity and equipment investment.

Note For more details on controller redundancy, see *Deploying Cisco 440X Series Wireless LAN Controllers* at the following URL: http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1060810.

The configuration of N+1 redundancy in any mobility design depends greatly on the licensed capacity of the controllers used and the number of access points involved. In some cases, configuration is rather straightforward, emulating what is shown in Figure 5-21 by having the access points of the main campus as well as all remote campuses address a common redundant controller located in the main campus services block. In other cases, there may be sufficient capacity on the primary controllers located on the main campus themselves to accommodate the access point and user load of a single failed controller on any of the remote campuses. This approach requires that main campus controllers be licensed for a greater number of access points than necessary for the support of the main campus alone. Additional licensing of existing controllers is performed in place of providing a dedicated additional controller platform at the main campus for system-wide redundancy. In this case, the available capacity of the primary main campus WLAN controllers allow them to act as the secondary destination for the access associated with the largest remote campus. Thus, in this particular case, the need to deploy hardware at the main campus site explicitly for the purposes of controller redundancy may be avoided.

For example, assume that the main campus shown in Figure 5-3 contains a total of 250 combined access points across all main campus buildings, and the largest of the remote campuses also contains 250 combined access points across all remote campus buildings. In this case, if the main campus services block is equipped with two Cisco CT5508-250 WLAN controllers (the "-250" signifies that this particular Cisco 5508 Wireless Controller is licensed for 250 access points), the access point load of the main campus alone can be split equally between the two controllers (125 access points on each controller). This leaves ample capacity in the main campus for one of the following scenarios to occur:

- Either of the main campus controllers may fail and allow up to 125 joined access points to migrate (failover) to the other controller in the pair. This results in the remaining functional controller bearing the full load of 250 access points.
- Any remote campus controller may fail and allow its joined access points to migrate (failover) to the main campus controllers. In the case of a failure of the largest remote campus, this results in each of the main campus controllers operating at their full licensed capacity.

Further information regarding WLAN controller redundancy may be found in the following documents:

- *Deploying Cisco 440X Series Wireless LAN Controllers*— http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html#wp1060810
- *Enterprise Mobility 4.1 Design Guide*— http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

AP Controller Failover

The Cisco Unified Wireless Network provides for multiple failover options that can allow access points to determine which WLAN controller to migrate in the event of a controller failure, based on pre-configured priorities. When an access point goes through its discovery process, it learns about all the WLAN controllers in its mobility group. The access point can prioritize which controller it attempts to join based on its high availability configuration, or choose a WLAN controller based on loading.

In the Cisco Community College reference design, a high-speed WAN/MAN is present between campuses, thus making access point failover to a remote WLAN controller feasible, as described in the previous section. To accomplish this in the Cisco Community College reference design, access points can be configured to failover to a WLAN controller that is outside their mobility group. In this scenario, the remote WLAN controller is not in the mobility group that is learned during the AP discovery process, and the IP address of the remote WLAN controller must be provided in the HA configuration.

For this to be effective, however, a common WLAN SSID naming policy for key WLANs must be implemented to ensure that WLAN clients do not have to be reconfigured in the event of an access point failover to the main campus backup controller.

Best practice considerations regarding to AP controller failover include the following:

- After access points initially discover a WLAN controller, access points should be manually assigned to primary and secondary controllers. By doing this, AP assignment and WLAN redundancy behavior is deterministic.
- A common WLAN SSID naming policy is necessary to ensure that WLAN clients do not have to be reconfigured in the event of an access point failover to a central backup controller. The SSID used to access a particular WLAN throughout the multi-campus community college should be the same, regardless of the controller.
- WLAN controllers have a configurable parameter known as *AP Fallback* that causes access points to return to their primary controllers after a failover event, after the primary controller comes back online. This feature is enabled by default. However, leaving this parameter at the default value can have some unintended consequences. When an access point "falls back" to its primary controller, there is a brief window of time, usually approximately 30 seconds or so, during which service to wireless clients is interrupted because the access points are busy re-joining the primary controller. In addition, if connectivity to the primary WLAN controller becomes unstable for some reason, the access point might "flap" between the primary controller and the backup. For this reason, it is preferable to disable AP Fallback and, in the rare event of a controller failure, move the access points back to the primary controller in a controlled fashion during a scheduled service window.

Note For more information and best practices regarding AP controller failover, see the Enterprise Mobility 4.1 Design Guide at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html.

Community College Mission Relevancy

This document attempts to present the mobility design considerations that comprise an important part of a successful implementation of the Cisco Community College reference design. The goal is to provide stakeholders with a reference design that assists in solving the complex business challenges that community colleges must face in the 21st century.

This closing section steps back from the technical intricacies of system design to examine how these design considerations relate to the foundation services described in the opening paragraphs of this document.

Safety and Security

The mission of the Cisco Community College reference design in this area is to enhance safety and security on campus by using a design model that proactively protects students, faculty, and staff. Maintaining safe buildings and grounds while keeping the network secure for today's community colleges. The Cisco Community College reference design helps to facilitate and enhance the effectiveness of physical campus security, track assets, protect the network, and prevent unauthorized network access.

The mobility aspects of Cisco Safety and Security Solutions includes the following three solution sets:

- *Campus physical safety and security*—Is the physical campus protected and safe? The Cisco Community College reference design helps enable community colleges to maintain safe buildings and grounds by the following:
  - Supporting the monitoring of unauthorized behavior and delivering alerts about detected events. Real-time monitoring helps campus security staff to prevent, deter, detect, and respond more quickly to incidents.
  - Providing reliable, secure, and high-performance WLAN communications throughout building interiors and outside buildings to students, faculty, administrators, and community college guests. This level of reliable wireless connectivity can be the key to ensuring rapid notification of campus personnel in the event of a safety incident.
  - Real-time tie-in to wired and wireless video surveillance systems as well as portable security devices and third-party campus safety systems, to ensure that unfolding events are detected quickly and monitored by the right personnel in the right location.
  - Offering WLAN connectivity from strategic campus locations to public safety emergency professionals using licensed 4.9 GHz frequencies as well as traditional 2.4 GHz and 5 GHz unlicensed frequencies. During periods of crisis, indoor and outdoor WLANs can provide first responders with vital tactical information about what is happening within the campus. The 4.9 GHz band that is available on the Cisco Aironet 1524PS Public Safety Lightweight Outdoor Access Point provides access via radio frequencies that are reserved by the FCC for public safety usage only.

  Other Cisco products and solutions that work in collaboration with the Cisco Community College reference design to enable these and other capabilities include the Cisco Mobility Services Engine (MSE), Cisco Context-Aware Mobility Solution, Cisco Unified Communications, the Cisco Unified Wireless IP Phone 7925G, and Cisco Video Surveillance products.
- *Network and data security*—Is the wireless network secure? The Cisco Community College reference design addresses this issue by the following:

  - Protecting confidential data and transmissions by using the highest level of authentication and encryption applicable to the tasks at hand, helping to ensure that wireless transmissions remain secure and protected.
  - Helping to prevent misguided students or malicious intruders from hacking into restricted servers or issuing attacks against the wireless network via the inclusion of the optional Mobility Services Engine with Wireless Intrusion Protection System (wIPS). It also helps quickly locate rogue access points anywhere on campus.
  - Providing an economical guest access solution that furnishes safe and secure guest access for campus guests.

- *Context-aware mobility*—Where is an asset located on campus and what is its status? The Cisco Unified Wireless Network, in conjunction with Cisco Context-Aware Mobility solutions, supports the ability to do the following:
  - Capture and integrate into community college application and administrative processes, detailed contextual information about an asset such as its location, movement, status, and state. This solution helps community colleges automatically collect information about mobile assets, analyze it, and use it to reduce errors, improve asset security, prevent delays, improve scalability beyond manual processes, and enhance learning functions.
    - Any asset that is emitting a Wi-Fi signal can be monitored, tracked, and found with this solution. A Wi-Fi signal can be generated from a built-in wireless card or an attached Wi-Fi tag from third-party vendors including AeroScout, WhereNet, and others.
    - Expensive items such as projectors, televisions, portable plants, lab equipment, tools, laptops, or any asset that moves can be easily tracked.
  - Alerts can be issued about the movement of a device in or out of an area. Costs for misplaced items, loss, and theft can be reduced.
  - Faculty and staff can use context-aware mobility in conjunction with third-party applications to automatically send announcements, assignments, room change notifications, campus event updates, and emergency alerts to students as they roam on campus.
  - Security personnel can use this solution to receive silent alerts and notifications about asset movement and rogue devices, track the areas of the campus they have inspected or secured, and quickly learn the location and of emergency-triggered events.
  - Administrators can use this solution to quickly locate students, faculty, or staff anywhere on campus.

Virtual Learning

The traditional scenario of a mass of students filing into a large lecture hall within a large, monolithic campus building is by no means the only such model available to today's modern-day community college student. High performance, secure wireless technologies can enable "virtual classrooms" even in non-traditional settings, such as leased space in shopping malls, retail plazas and even from homes and offices.

School administrators need secure access to tools, records, and resources, as well as ubiquitous access to mobile voice capabilities throughout the campus.

Using the solutions and technologies presented within the Cisco Community College reference design, state-of-the art instructional sites can be deployed in such non-traditional settings within urban, suburban, and rural venues. These types of facilities can help bring much-needed skills to areas that may not be within convenient reach of conventional community college campuses. For example, a community college location at a shopping mall may operate as a science, technology, engineering, and math learning

center. Such centers may range in size from one or two classroom sites to larger-scale deployments with ten or twelve classrooms, a hundred or more student computers, a science lab, two auditoriums, and even testing, conference, and office space.

Secure Connected Classrooms

Providing connectivity to students while attending class is the foundation of twenty-first century learning. However, it also presents several challenges for community colleges. For example, the density of wireless users in one location can be problematic. Wireless designs must take into consideration the number of users, radio interference, and network utilization.

The Cisco Community College reference design addresses these challenges is a variety of ways, including the following:

- High-performance dual-band access points that provide options to migrate users to 802.11n and better performing bands (5 GHz) that offer increased data rates with less interference.
- Advanced radio resource management algorithms and techniques that can automate the fine-tuning of transmit power and other parameters to best accommodate high-density user populations.
- Comprehensive wireless network management systems (WCS) that can assist in the identification of interference sources and rogue access points, including their location.
- Detailed reporting mechanisms that can enable administrators to better understand the points of congestion in the network and how best to address them.
- A high-performance controller platform, optimized for use with high-performance 802.11n access points, that offers aggregate wired interface bandwidth of up to 8 Gbps.

Operational Efficiencies

Delivering quick and cost-effective broadband access anywhere on campus extends learning beyond the classroom and improves campus operations, collaboration, and productivity. The Cisco Community College reference design supports secure, easy wireless network access to voice, video, and data applications for students, administrators, faculty, staff, and visitors as they roam about the campus.

The operational efficiencies enabled by the Cisco Community College reference design encompass the following solution sets:

- *Pervasive wireless on campus*—Is the WLAN available ubiquitously in all required indoor and outdoor areas? As a key component of the Cisco Community College reference design, the Cisco Unified Wireless Network delivers broadband access quickly and cost-effectively to all the required indoor and outdoor areas in the typical community college. The benefits of this are as follows:
  - When wireless access is available pervasively on campus, users do not need to hunt for wired ports because they can gain access to network resources using their wireless connection.
  - Users can stay connected to their applications as they roam, without having to re-log onto the network while they are in motion.
  - As long as an area is covered by the wireless infrastructure, faculty, students, and guests can work, share resources, collaborate, and communicate.
  - With a pervasive wireless network, instruction is no longer limited to the classroom.
  - Faculty can teach inside or outside the classroom, accessing the Internet and applications while on the move.

  - Access to resources is improved because faculty and administrators do not have to return to their desk to perform online administration tasks, access research information, or check E-mail.
  - Student satisfaction is increased and trouble calls are decreased because wireless access is predictable and consistent.
  - With a pervasive Cisco WLAN, community colleges can deliver network access to locations where hardwiring is too expensive, too difficult, or implausible. Examples are refurbished buildings, older buildings with environmental concerns such as asbestos remediation, or sites with protected-building restrictions such as historical landmarks.
  - Costs for cabling temporary spaces or for providing network access to new faculty or staff can be reduced or eliminated.

  In fact, you may find that it is more cost-effective to provide wireless network access pervasively on campus than it is to install individual wired ports over the same geographic area.

- *High-speed wireless access*—Are bandwidth-intensive applications supported on the WLAN? The Cisco Unified Wireless Network facilitates the creation of solutions that accelerate the delivery of bandwidth-intensive applications and provides a better end-user experience.
  - The Cisco high-speed wireless network, based on the 802.11n standard, delivers unprecedented reliability, greater performance, and extended reach for pervasive wireless connectivity. It excels at supporting bandwidth-intensive applications that are used for research, learning, virtual environments, and social networking. This solution also delivers predictable and continuous WLAN coverage for areas with dense wireless usage such as lecture halls, auditoriums, open spaces, and social areas.
  - Community colleges that deploy 802.11n are demonstrating a commitment to technology innovation and leadership. They are building a solid technology foundation to attract new students and remain competitive in the ever-evolving global community college education marketplace.
- *Secure guest access*—Can visitors easily access the network? The Cisco Community College reference design supports secure wireless guest access that cost-effectively simplifies the process of providing temporary Internet access to visitors such as prospective students, alumni, parents, visiting lecturers, and temporary personnel. Wireless guest access eliminates the frustration that visitors experience when they are limited to wired-only ports in small areas on campus. It also eliminates the costs that community colleges might incur from wiring and maintaining wired ports to accommodate visitors. With the Cisco secure guest access solution, community colleges can do the following:
  - Enhance the community college experience for prospective students
  - Provide Internet access to guests attending campus events
  - Easily support network access for conference attendees and guest lecturers
- *Campus automation*—Are managing and tracking campus resources automated? The solutions enabled by the Cisco Community College reference design can help community colleges reduce costs by supporting Wi-Fi-enabled services that automatically manage, track, and maintain campus resources and assets.
  - The wireless network can assist with better management of real estate components to support green initiatives, improve energy efficiency, and create smart buildings.
  - Alarms, bells, and clocks can be wirelessly enabled to reduce the labor costs associated with managing them. Wi-Fi tags can be placed on assets to automatically track their movement and help reduce costs for misplaced items, loss, and theft.

- *Facilities management*—The Cisco Community College reference design includes adaptive power management capabilities that are built into the Cisco Unified Wireless Network through its Cisco Wireless Control System (WCS) management platform and software release 6.0. Cisco WCS adaptive power management allows community colleges to shrink their carbon footprint immediately through measurable reductions in energy usage and operational expenses.

  By using Cisco WCS adaptive power management to turn access point radios on or off at scheduled intervals (hour, day, and week), power requirements and operating expenses can be reduced almost immediately. The power savings gained vary based on the Cisco Aironet access point model deployed. Using this feature can help organizations create a sustainable culture and gain momentum for “Green IT” initiatives.

CHAPTER 6

Community College Security Design Considerations

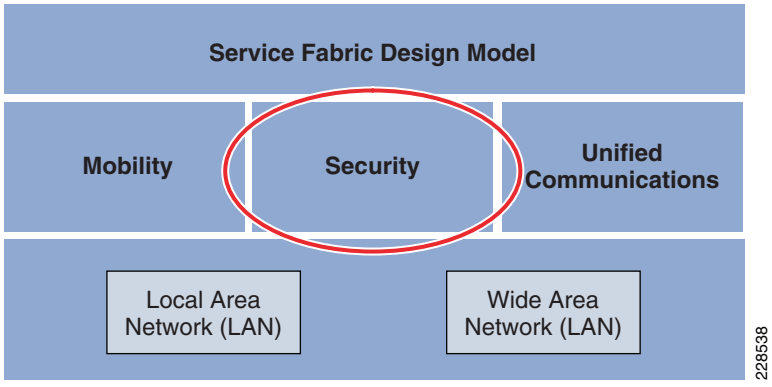
As community colleges embrace new communication and collaboration tools, transitioning from traditional classroom teaching into an Internet-based, media-rich education and learning environment, a whole new set of network security challenges arise. Community college network infrastructures must be adequately secured to protect students, staff, and faculty from harmful content, to guarantee confidentiality of private data, and to ensure the availability and integrity of the systems and data. Providing a safe and secure network environment is a top responsibility for community college administrators and community leaders.

Security Design

Within the Cisco Community College reference design, the service fabric network provides the foundation on which all solutions and services are built to solve the business challenges facing community colleges. These business challenges include building a virtual learning environment, providing secure connected classrooms, ensuring safety and security, and operational efficiencies.

The service fabric consists of four distinct components: LAN/WAN, security, mobility, and unified communications, as shown in Figure 6-1.

Figure 6-1 Service Fabric Design Model



The Community College reference design includes security to protect the infrastructure and its services to provide a safe and secure online environment for teaching and learning. This design leverages the proven design and deployment guidelines of the Cisco SAFE Security Reference Architecture to secure

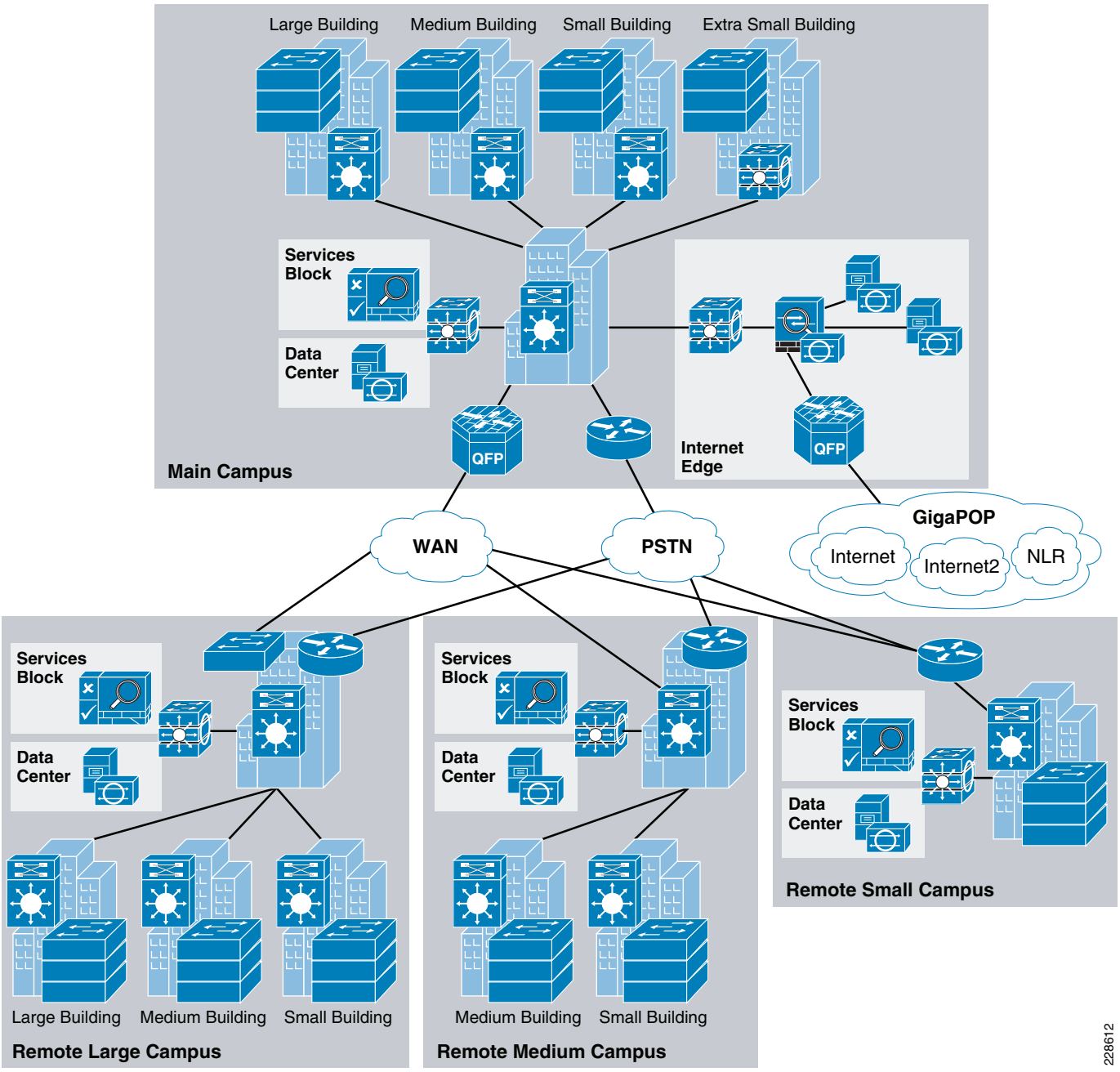
the service fabric by deploying security technologies throughout the entire solution to protect students and faculty from harmful content; to guarantee the confidentiality of student, staff, and faculty private data; and to ensure the availability and integrity of the systems and data.

Protecting the infrastructure and its services requires implementation of security controls capable of mitigating both well-known and new forms of threats. Common threats to community college environments include the following:

- *Service disruption*—Disruption to the infrastructure and learning resources such as computer labs caused by botnets, worms, malware, adware, spyware, viruses, denial-of-service (DoS) attacks, and Layer 2 attacks
- *Network abuse*—Use of non-approved applications by students, faculty, and staff; peer-to-peer file sharing and instant messaging abuse; and access to forbidden content
- *Unauthorized access*—Intrusions, unauthorized users, escalation of privileges, IP spoofing, and unauthorized access to restricted learning and administrative resources
- *Data loss*—Loss or leakage of student, staff, and faculty private data from servers and user endpoints
- *Identity theft and fraud*—Theft of student, staff, and faculty identity or fraud on servers and end users through phishing and E-mail spam

The Community College reference design accommodates a main campus and one or more remote smaller campuses interconnected over a metro Ethernet or managed WAN service. Each of these campuses may contain one or more buildings of varying sizes, as shown in Figure 6-2.

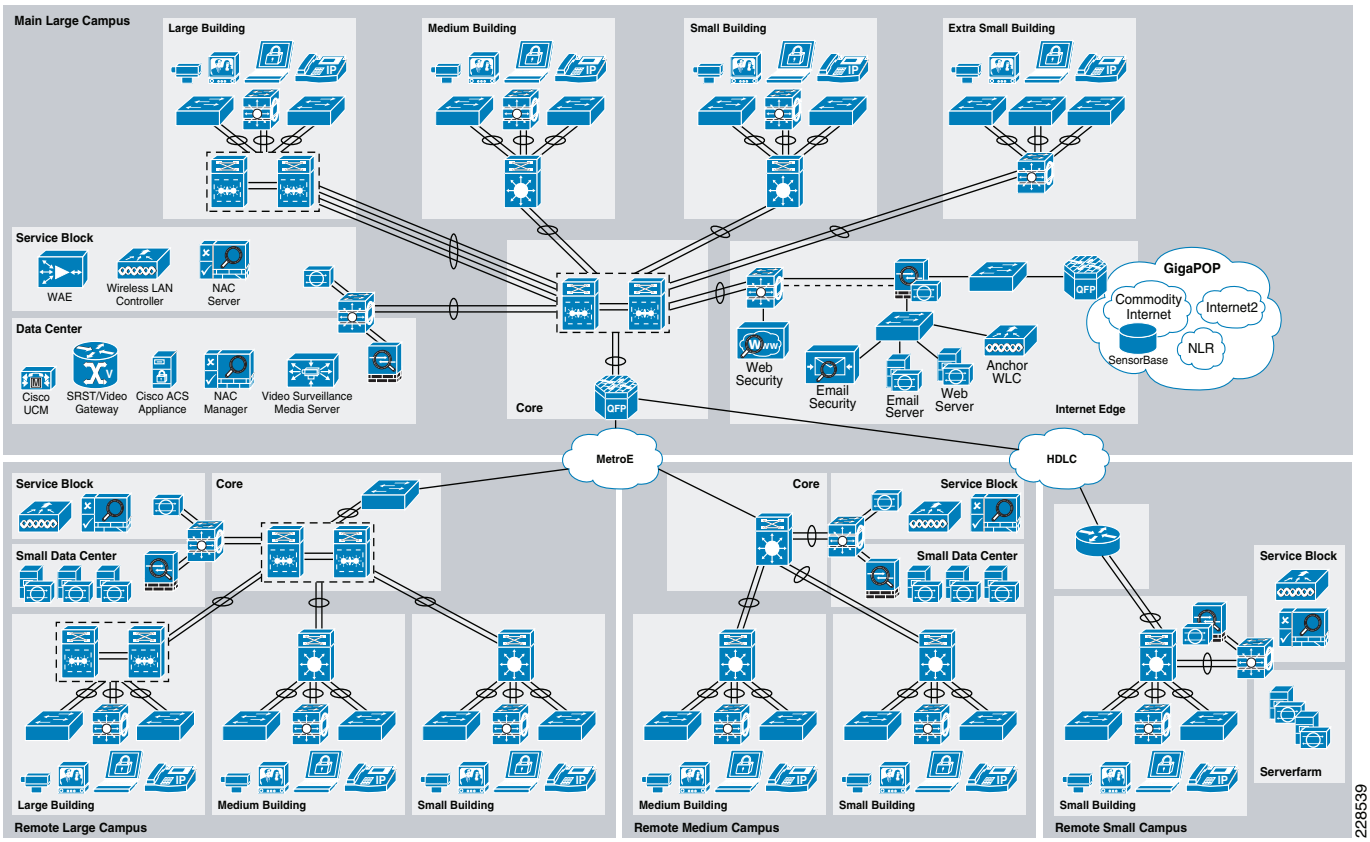
Figure 6-2 Community College Reference Design Overview



Operating on top of this network are all the services used within the community college environment, such as safety and security systems, voice communications, video surveillance equipment, and so on. The core of these services are deployed and managed at the main campus building, allowing each remote campus to reduce the need for separate services to be operated and maintained by community college IT personnel. These centralized systems and applications are served by a data center in the main campus.

The security design uses a defense-in-depth approach where multiple layers of security protection are integrated into the architecture. Various security products and technologies are combined to provide enhanced security visibility and control, as shown in Figure 6-3.

Figure 6-3 Community College Network Security Design Overview



The following security elements should be included in the Community College Security design depicted in Figure 6-3:

- *Endpoint Security*—Desktop endpoint protection for day-zero attack protection, data loss prevention, and signature-based antivirus.
- *Network Foundation Protection*—Device hardening, control, and management plane protection throughout the entire infrastructure to maximize availability and resiliency.
- *Catalyst Integrated Security Features*—Access layer protection provided by port security, Dynamic ARP inspection, IP Source Guard, and DHCP Snooping.
- *Threat Detection and Mitigation*—Intrusion prevention and infrastructure based network telemetry to identify and mitigate threats.
- *Internet Access*—E-mail and Web Security. Stateful firewall inspection. Intrusion prevention and global correlation. Granular access control.
- *Cisco Video Surveillance*—Monitor activities throughout the school environment to prevent and deter safety incidents.
- *Enhanced Availability and Resiliency*—Hardened devices and high availability design ensure optimal service availability. System and interface-based redundancy.
- *Unified Communications*—Security and emergency services, enhanced 911 support. Conferencing and collaboration for planning and emergency response.
- *Network Access Control*—Authentication and policy enforcement via Cisco Identity-Based Networking Services (IBNS). Role-Based access control and device security compliance via Cisco Network Admission Control (NAC) Appliance.

The Community College reference design recognizes that cost and limited resources are common limiting factors. Therefore, architecture topologies and platforms are carefully selected to increase productivity while minimizing the overall cost and operational complexities. In certain cases, tradeoffs are made to simplify operations and reduce costs where needed.

The security design for the community college service fabric focuses on the following key areas.

- *Network foundation protection* (NFP)—Ensuring the availability and integrity of the network infrastructure by protecting the control and management planes to prevent service disruptions network abuse, unauthorized access, and data loss.
- *Internet perimeter protection*
  - Ensuring safe connectivity to the Internet, Internet2, and National LambdaRail (NLR) networks
  - Protecting internal resources and users from botnets, malware, viruses, and other malicious software
  - Protecting students, staff, and faculty from harmful content
  - Enforcing E-mail and web browsing policies to prevent identity theft and fraud
  - Blocking command and control traffic from infected internal bots to external hosts
- *Data center protection*
  - Ensuring the availability and integrity of centralized applications and systems
  - Protecting the confidentiality and privacy of student, staff, and faculty records
- *Network access security and control*
  - Securing the access edges
  - Enforcing authentication and role-based access for students, staff, and faculty residing at the main and remote campuses
  - Ensuring that systems are up-to-date and in compliance with the community college's network security policies
- *Network endpoint protection*
  - Protecting servers and school-controlled systems (computer labs, school-provided laptops, and so on) from viruses, malware, botnets, and other malicious software
  - Enforcing E-mail and web browsing policies for staff and faculty

Together, these key security areas create a defense-in-depth solution for protecting community colleges from common security threats such as service disruption, network abuse, unauthorized access, data loss, and identity theft and fraud. The design guidelines and best practices for each of the above security focus areas are detailed in the following sections. For more detailed information on each of these areas, see the *Cisco SAFE Reference Guide* at the following URL: http://www.cisco.com/go/safe.

Network Foundation Protection

The community college network is built with routers, switches, and other infrastructure network devices that keep the applications and services running. These infrastructure devices must be properly hardened and secured to maintain continued operation and access to these services.

To ensure the availability of the community college network infrastructure, the NFP best practices should be implemented for the following areas:

- *Infrastructure device access*

  - Restrict management device access to authorized parties and via only authorized ports and protocols.
  - Enforce authentication, authorization, and accounting (AAA) with Terminal Access Controller Access Control System (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) to authenticate access, authorize actions, and log all administrative access.
  - Display legal notification banners.
  - Ensure confidentiality by using secure protocols such as Secure Shell (SSH) and HTTPS.
  - Enforce idle and session timeouts.
  - Disable unused access lines.
- *Routing infrastructure*
  - Restrict routing protocol membership by enabling Message-Digest 5 (MD5) neighbor authentication and disabling default interface membership.
  - Enforce route filters to ensure that only legitimate networks are advertised, and networks that are not supposed to be propagated are never advertised.
  - Log status changes of neighbor sessions to identify connectivity problems and DoS attempts on routers.
- *Device resiliency and survivability*
  - Disable unnecessary services.
  - Implement control plane policing (CoPP).
  - Enable traffic storm control.
  - Implement topological, system, and module redundancy for the resiliency and survivability of routers and switches and to ensure network availability.
  - Keep local device statistics.
- *Network telemetry*
  - Enable Network Time Protocol (NTP) time synchronization.
  - Collect system status and event information with Simple Network Management Protocol (SNMP), Syslog, and TACACS+/RADIUS accounting.
  - Monitor CPU and memory usage on critical systems.
  - Enable NetFlow to monitor traffic patterns and flows.
- *Network policy enforcement*
  - Implement access edge filtering.
  - Enforce IP spoofing protection with access control lists (ACLs), Unicast Reverse Path Forwarding (uRPF), and IP Source Guard.
- *Switching infrastructure*
  - Implement a hierarchical design, segmenting the LAN into multiple IP subnets or virtual LANs (VLANs) to reduce the size of broadcast domains.
  - Protect the Spanning Tree Protocol (STP) domain with BPDU Guard and STP Root Guard.
  - Use Per-VLAN Spanning Tree (PVST) to reduce the scope of possible damage.
  - Disable VLAN dynamic trunk negotiation on user ports.
  - Disable unused ports and put them into an unused VLAN.

  - Implement Cisco Catalyst Infrastructure Security Features (CISF) including port security, Dynamic ARP Inspection, DHCP snooping, and IP Source Guard.
  - Use a dedicated VLAN ID for all trunk ports.
  - Explicitly configure trunking on infrastructure ports.
  - Use all tagged mode for the native VLAN on trunks and drop untagged frames.
- *Network management*
  - Ensure the secure management of all devices and hosts within the community college network infrastructure.
  - Authenticate, authorize, and keep records of all administrative access.
  - If possible, implement a separate out-of-band (OOB) management network (hardware- or VLAN-based) to manage systems local to the main campus.
  - Secure the OOB management access by enforcing access controls, using dedicated management interfaces or virtual routing and forwarding (VRF) tables.
  - Provide secure in-band management access for systems residing at remote campus sites by deploying firewalls and ACLs to enforce access controls, using Network Address Translation (NAT) to hide management addresses, and using secure protocols such as SSH and HTTPS.
  - Ensure time synchronization by using NTP.
  - Secure management servers and endpoints with endpoint protection software and operating system (OS) hardening best practices.

For more detailed information on the NFP best practices including configuration examples, see "Chapter 2, Network Foundation Protection" in the *Cisco SAFE Reference Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap2.html.

Internet Perimeter Protection

The Community College reference design assumes a centralized connection to the Internet, Internet2, and National LambdaRail (NLR) networks at the main campus site. This connection serves students, staff, and faculty at the main campus as well as all remote campus sites. Common services typically provided by this connection include the following:

- E-mail for staff and faculty
- Internet browsing for everyone
- Community college web portal accessible over the Internet
- Connectivity to other educational institutions over the Internet2 and NLR network
- Remote access to the community college network

The Internet2 network is a not-for-profit advanced networking consortium comprised of more than 200 U.S. universities in cooperation with 70 leading corporations, 45 government agencies, laboratories, and other institutions of higher learning as well as over 50 international partner organizations. Internet2 provides its members both leading-edge network capabilities and unique partnership opportunities that together facilitate the development, deployment, and use of revolutionary Internet technologies. The physical implementation of Internet2 network consists of an advanced IP network, virtual circuit network, and core optical network. The Internet2 network provides the necessary scalability for member institutions to efficiently provision resources to address the bandwidth-intensive requirements of their

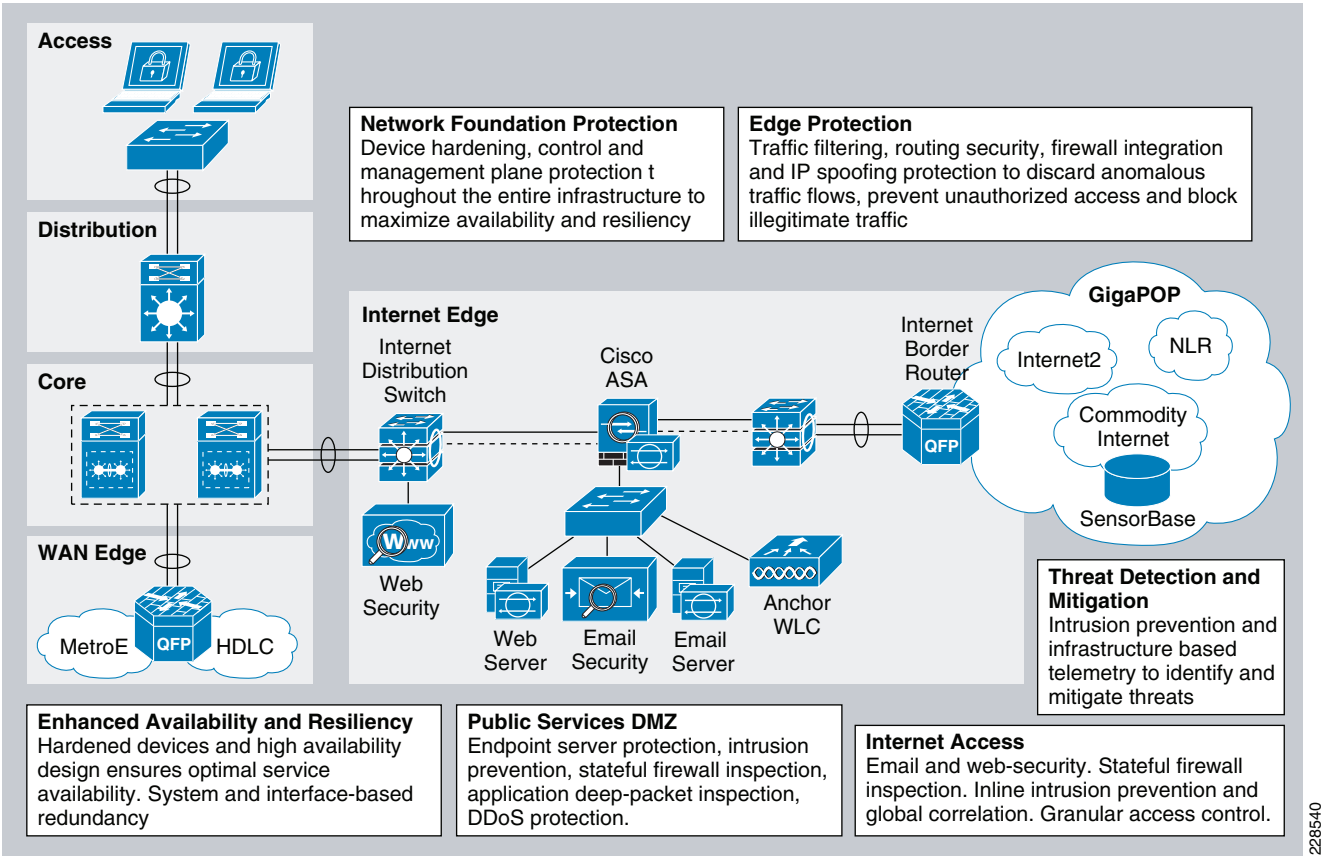
campuses, such as collaborative applications, distributed research experiments, grid-based data analysis, and social networking. For more information on the Internet2 network, see the following URL: http://www.internet2.edu/network/.

The National LambdaRail (NLR) network is a high-speed fiber optic network infrastructure linking over 30 cities in 21 states. It is owned by the U.S. research and education community and is dedicated to serving the needs of researchers and research groups. The NLR high-performance network backbone offers unrestricted usage and bandwidth, a choice of cutting-edge network services and applications, and customized service for individual researchers and projects. NLR services include high-capacity 10 Gigabit Ethernet LAN-PHY or OC-192 lambdas, point-to-point or multi-point Ethernet-based transport, routed IP-based services, and telepresence video conferencing services. For more information on the NLR network and its services, see the following URL: http://www.nlr.net/.

Community colleges typically connect to a local Gigabit point-of-presence (GigaPOP) or regional network service provider to gain access to the Internet, Internet2, and NLR networks. The same security controls are applicable regardless of whether they connect to a GigaPOP or regional network. For details on how community colleges connect to these networks, see Chapter 4, "Community College WAN Design Considerations."

The part of the network infrastructure that provides connectivity to the Internet, Internet2, and NLR is defined as the Internet perimeter, as shown in Figure 6-4.

Figure 6-4 Internet Perimeter



The Internet perimeter provides safe and secure access to the Internet, Internet2, and NLR networks for students, staff, and faculty. It also provides access to public services such as the community college web portal without compromising the confidentiality, integrity, and availability of the resources and data of the educational institution. To provide secure access, the Internet perimeter should incorporate the following security functions:

- *Internet border router*—The Internet border router is the gateway responsible for routing traffic between the community college and the Internet, Internet2, and NLR networks. It may be administered by the community college IT staff or may be managed by the Internet, Internet2, or NLR service provider. This router provides the first line of protection against external threats and should be hardened according to the NFP best practices.
- *Internet firewall*—A Cisco Adaptive Security Appliance (ASA) provides stateful access control and deep packet inspection to protect community college resources and data from unauthorized access and disclosure. The ASA monitors network ports for rogue activity and detects and blocks traffic from infected internal endpoints, sending command and control traffic back to a host on the Internet. The ASA is configured to control or prevent incoming and outgoing access for the Internet, Internet2, and NLR networks; to protect the community college web portal and other Internet public services; and to control student, staff, and faculty traffic bound towards the Internet. The security appliance may also provide secure remote access to faculty, staff, and students in the form of a Secure Socket Layer (SSL) or IPSec virtual private network (VPN).
- *Intrusion prevention*—An Advanced Inspection and Prevention Security Service Module (AIP SSM) on the Cisco ASA or a separate IPS appliance can be implemented for enhanced threat detection and mitigation. The IPS module or appliance is responsible for identifying and blocking anomalous traffic and malicious packets recognized as well-known attacks. IPS can be configured either in inline or promiscuous mode. IPS may also be configured to help block certain Internet applications such as AOL Messenger, BitTorrent, Skype, and so on.
- *Public services DMZ*—The community college external Internet web portal, mail server, and other public facing servers and services are placed on a demilitarized zone (DMZ) for security and control purposes. The DMZ acts as a middle stage between the Internet and community college private resources, preventing external users from directly accessing any internal servers and data. The Internet firewall is responsible for restricting incoming access to the public services in the DMZ, and controls outbound access from DMZ resources to the Internet. Systems residing within the DMZ should be hardened with endpoint protection software (such as Cisco Security Agent) and OS hardening best practices.
- *E-mail security*—A Cisco IronPort C Series E-Mail Security Appliance (ESA) is deployed in the DMZ to inspect incoming and outgoing E-mails and eliminate threats such as E-mail spam, viruses, and worms. The ESA appliance also offers E-mail encryption to ensure the confidentiality of messages, and data loss prevention (DLP) to detect the inappropriate transport of sensitive information.
- *Web security*—A Cisco IronPort S Series Web Security Appliance (WSA) is deployed at the distribution switches to inspect HTTP and HTTPS traffic bound to the Internet. The WSA enforces URL filtering policies to block access to websites containing content that may be harmful for students, staff, and faculty such as sites known to be sources of spyware, adware, botnets, or other types of malware. The WSA may also be configured to block certain Internet applications such as AOL Messenger, BitTorrent, Skype, and so on, and for monitoring Layer 4 traffic for rogue activity and infected systems.
- *Guest access wireless LAN controller*—The Cisco Unified Wireless LAN Guest Access option offers a flexible, easy-to-implement method for deploying wireless guest access via Ethernet over IP (RFC3378). Ethernet over IP (EoIP) tunneling is used between two wireless LAN controller (WLC) endpoints in the centralized network design. A WLC is located in the Internet perimeter DMZ, where it is referred to as an *anchor controller*. The anchor controller is responsible for

terminating EoIP tunnels originating from centralized campus WLCs located in the services block, and interfacing the traffic from these controllers to a firewall or border router. Traffic to and from this guest access WLAN is tunneled to the DMZ transparently, with no visibility by, or interaction with, other traffic in the community college. For more information on the wireless guest access solution, see Chapter 5, "Community College Mobility Design Considerations."

The following subsections describe the design guidelines for implementing the above security functions.

Internet Border Router Security

The Internet border router connects to a local GigaPOP and provides connectivity to the Internet, Internet2, and NLR networks for the community college. The router acts as the first line of defense against unauthorized access, distributed DoS (DDoS), and other external threats. ACLs, uRPF, and other filtering mechanisms should be implemented for anti-spoofing and to block invalid packets. NetFlow, Syslog, and SNMP should be used to gain visibility on traffic flows, network activity, and system status. In addition, the Internet border router should be hardened and secured following the best practices explained in Network Foundation Protection, page 6-5. This includes restricting and controlling administrative access, protecting the management and control planes, and securing the dynamic exchange of routing information.

For more information on how to secure the Internet border router, see "Chapter 6, Enterprise Internet Edge" in the *Cisco SAFE Reference Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap6.html.

Internet Firewall

A Cisco ASA firewall should be deployed at the Internet perimeter to protect community college internal resources and data from external threats by doing the following:

- Preventing incoming access from the Internet, Internet2, and NLR networks
- Protecting public resources deployed in the DMZ by restricting incoming access to the public services and by limiting outbound access from DMZ resources out to the Internet
- Controlling user Internet-, Internet2- and NLR-bound traffic
- Monitoring network ports for rogue activity and preventing infected internal endpoints from sending command and control traffic back to a host on the Internet

The ASA should be configured to enforce access policies, keep track of connection status, and inspect packet payloads. Examples of the needed access policies include the following:

- Deny or control any connection attempts originating from the Internet, Internet2, and NLR to internal resources and subnets.
- Allow outbound Internet HTTP/HTTPS access for students, staff, and faculty residing at any of the community college campuses.
- Allow outbound SSL access to the Internet for devices requiring administrative updates such as SensorBase, IPS signature updates, and so on.
- Deny or control access between the community college internal network and the external Internet, Internet2, or NLR networks.

- Allow students, staff, and faculty access to DMZ services such as the community college web portal, E-mail, and domain name resolution (HTTP, HTTPS, Simple Mail Transfer Protocol (SMTP), point-of-presence [POP], Internet Message Access Protocol (IMAP), Domain Name Service [DNS]).
- Restrict inbound Internet access to the DMZ for the necessary protocols and servers (HTTP to web server, SMTP to Mail Transfer Agent, DNS to DNS servers, and so on).
- Restrict connections initiated from the DMZ to only necessary protocols and sources (DNS from DNS server, SMTP from mail server, HTTP/SSL from Cisco IronPort ESA).
- Enable stateful inspection for the outbound protocols being used to ensure returning traffic is dynamically allowed by the firewall.
- Prevent access to the anchor WLC deployed in the DMZ for guest access except for tunneled traffic coming from the centralized campus WLCs (UDP port 16666 and IP protocol ID 97) and traffic needed to manage it (SNMP, TFTP, HTTP, HTTPS, SSH).
- Implement NAT and Port Address Translation (PAT) to shield the internal address space from the Internet.

In addition, the Cisco ASA Botnet Traffic Filter feature can be enabled to monitor network ports for rogue activity and to prevent infected internal endpoints from sending command and control traffic back to an external host on the Internet. The Botnet Traffic Filter on the ASA provides reputation-based control for an IP address or domain name, similar to the control that Cisco IronPort SenderBase provides for E-mail and web servers.

The Cisco Botnet Traffic Filter is integrated into all Cisco ASA appliances, and inspects traffic traversing the appliance to detect rogue traffic in the network. When internal clients are infected with malware and attempt to phone home to an external host on the Internet, the Botnet Traffic Filter alerts the system administrator of this through the regular logging process and can be automatically blocked. This is an effective way to combat botnets and other malware that share the same phone-home communications pattern.

The Botnet Traffic Filter monitors all ports and performs a real-time lookup in its database of known botnet IP addresses and domain names. Based on this investigation, the Botnet Traffic Filter determines whether a connection attempt is benign and should be allowed, or is a risk and should be blocked.

The Cisco ASA Botnet Traffic Filter has three main components:

- *Dynamic and administrator blacklist data*—The Botnet Traffic Filter uses a database of malicious domain names and IP addresses that is provided by Cisco Security Intelligence Operations. This database is maintained by Cisco Security Intelligence Operations and is downloaded dynamically from an update server on the SensorBase network. Administrators can also configure their own local blacklists and whitelists.
- *Traffic classification and reporting*—Botnet Traffic Filter traffic classification is configured through the **dynamic-filter** command on the ASA. The dynamic filter compares the source and destination addresses of traffic against the IP addresses that have been discovered for the various lists available (dynamic black, local white, local black), and logs and reports the hits against these lists accordingly.
- *Domain Name System (DNS) snooping*—To map IP addresses to domain names that are contained in the dynamic database or local lists, the Botnet Traffic Filter uses DNS snooping in conjunction with DNS inspection. Dynamic Filter DNS snooping looks at User Datagram Protocol (UDP) DNS replies and builds a DNS reverse cache (DNSRC), which maps the IP addresses in those replies to the domain names they match. DNS snooping is configured via the Modular Policy Framework (MPF) policies

The Botnet Traffic Filter uses two databases for known addresses. Both databases can be used together, or the dynamic database can be disabled and the static database can be used alone. When using the dynamic database, the Botnet Traffic Filter receives periodic updates from the Cisco update server on the Cisco IronPort SensorBase network. This database lists thousands of known bad domain names and IP addresses.

The ASA uses this dynamic database as follows:

1. When the domain name in a DNS reply matches a name in the dynamic database, the Botnet Traffic Filter adds the name and IP address to the DNS reverse lookup cache.
2. When the infected host starts a connection to the IP address of the malware site, the ASA sends a syslog message reporting the suspicious activity and optionally drops the traffic if the ASA is configured to do so.
3. In some cases, the IP address itself is supplied in the dynamic database, and the Botnet Traffic Filter logs or drops any traffic to that IP address without having to inspect DNS requests.

The database files are stored in running memory rather than Flash memory. The database can be deleted by disabling and purging the database through the configuration.

Note To use the database, be sure to configure a domain name server for the ASA so that it can access the URL of the update server. To use the domain names in the dynamic database, DNS packet inspection with Botnet Traffic Filter snooping needs to be enabled; the ASA looks inside the DNS packets for the domain name and associated IP address.

In addition to the dynamic database, a static database can be used by manually entering domain names or IP addresses (host or subnet) that you want to tag as bad names in a blacklist. Static blacklist entries are always designated with a Very High threat level. Domain names or IP addresses can also be entered in a whitelist,

When a domain name is added to the static database, the ASA waits one minute, and then sends a DNS request for that domain name and adds the domain name/IP address pairing to the DNS host cache. This action is a background process, and does not affect your ability to continue configuring the ASA. Cisco also recommends that DNS packet inspection be enabled with Botnet Traffic Filter snooping. When enabled, the ASA uses Botnet Traffic Filter snooping instead of the regular DNS lookup to resolve static blacklist domain names in the following circumstances:

- The ASA DNS server is unavailable.
- A connection is initiated during the one minute waiting period before the ASA sends the regular DNS request.

If DNS snooping is used, when an infected host sends a DNS request for a name on the static database, the ASA looks inside the DNS packets for the domain name and associated IP address and adds the name and IP address to the DNS reverse lookup cache.

If Botnet Traffic Filter snooping is not enabled, and one of the above circumstances occurs, that traffic is not monitored by the Botnet Traffic Filter.

Note It is important to realize that a comprehensive security deployment should include Cisco Intrusion Prevention Systems (IPS) with its reputation-based Global Correlation service and IPS signatures in conjunction with the security services provided by the ASA security appliance such as Botnet Traffic Filter.

For more information on the Cisco ASA Botnet Traffic Filter feature, see the following URL: http://www.cisco.com/en/US/prod/vpndevc/ps6032/ps6094/ps6120/botnet_index.html.

When deploying the Internet firewall, it is important to understand the traffic and policy requirements when selecting a firewall. An appropriately sized ASA model should be chosen so that it does not become a bottleneck. The Cisco ASA should also be hardened following the NFP best practices as described in Network Foundation Protection, page 6-5. This includes restricting and controlling administrative access, securing dynamic exchange of routing information with MD5 authentication, and enabling firewall network telemetry with SNMP, Syslog, and NetFlow.

Given budget and resource constraints for community colleges, high availability is achieved by using redundant physical interfaces, which provides a cost-effective solution. As an alternative, a pair of firewall appliances can be deployed in stateful failover using separate boxes at a higher cost.

Intrusion Prevention

IPS is responsible for identifying and blocking anomalous traffic and packets recognized as well-known attacks. An IPS module on the Cisco ASA Internet firewall or a separate IPS appliance can be implemented in the Internet perimeter for enhanced threat detection and mitigation. IPS may also be configured to help block certain Internet applications such as AOL Messenger, BitTorrent, Skype, and so on.

Integrating IPS on a Cisco ASA appliance using an AIP SSM provides a cost-effective solution for community colleges. The AIP SSM is supported on Cisco ASA 5510 and higher platforms. The AIP SSM runs advanced IPS software providing proactive, full-featured intrusion prevention services to stop malicious traffic before it can affect the community college network.

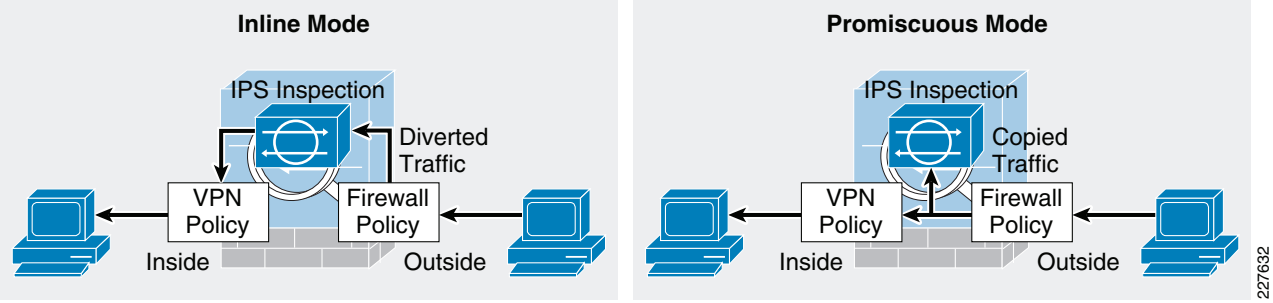
The AIP SSM module may also participate in Cisco Global Correlation for further threat visibility and control. If enabled, the participating IPS sensor receives threat updates from the Cisco SensorBase network at regular intervals. The Cisco SensorBase network contains detailed information about known threats on the Internet, including serial attackers, botnet harvesters, malware outbreaks, and dark nets. It then incorporates the global threat data into its system to detect and prevent malicious activity even earlier. The IPS uses this information to filter out the worst attackers before they have a chance to attack critical assets.

For more information on IPS Global Correlation including configuration information, see the following URL:
http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_collaboration.html.

The AIP SSM may be deployed in inline or promiscuous mode:

- *Inline mode*—The AIP SSM is placed directly in the traffic flow (see the left side of Figure 6-5). Traffic identified for IPS inspection cannot continue through the ASA without first passing through and being inspected by the AIP SSM. This mode is the most secure because every packet that has been identified for inspection is analyzed before being allowed through. Also, the AIP SSM can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput if not designed or sized appropriately.
- *Promiscuous mode*—A duplicate stream of traffic is sent to the AIP SSM. This mode is less secure, but has little impact on traffic throughput. Unlike inline mode, in promiscuous mode the AIP SSM can block traffic only by instructing the ASA to shun the traffic or by resetting a connection on the ASA. Also, while the AIP SSM is analyzing the traffic, a small amount of traffic might pass through the ASA before the AIP SSM can shun it. The right side of Figure 6-5 shows the AIP SSM in promiscuous mode.

Figure 6-5 IPS Inline and Promiscuous Modes



The recommended IPS deployment mode depends on the goals and policies of the community college. IPS inline mode is more secure because of its ability to stop malicious traffic in real-time; however, it may impact traffic throughput if not properly designed or sized. Conversely, IPS promiscuous mode has less impact on traffic throughput but is less secure because there may be a delay in reacting to the malicious traffic.

Although the AIP SSM runs as a separate application within the Cisco ASA, it is integrated into the traffic flow. The AIP SSM contains no external interfaces itself, except for the management interface on the SSM itself. When traffic is identified for IPS inspection on the ASA, traffic flows through the ASA and the AIP SSM in the following sequence:

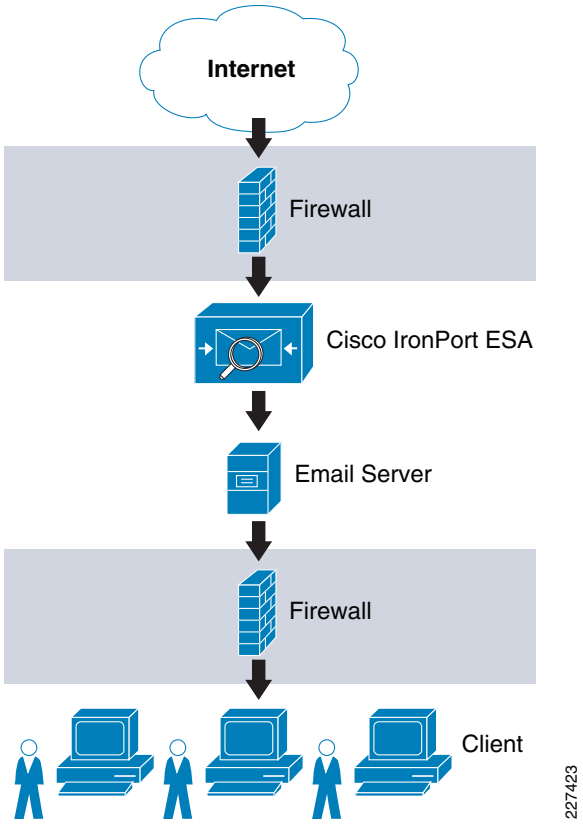
1. Traffic enters the ASA.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM over the backplane.
4. The AIP SSM applies its security policy to the traffic and takes appropriate actions.
5. (Inline mode only) Valid traffic is sent back to the ASA over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
6. Remote access VPN policies are applied (if configured).
7. Traffic exits the ASA.

The AIP SSM card may be configured to fail open or close when the module becomes unavailable. When configured to fail open, the ASA allows all traffic through, uninspected, if the AIP SSM becomes unavailable. Conversely, when configured to fail close, the ASA blocks all traffic in case of an AIP SSM failure.

E-Mail Security

Cisco recommends that the Cisco IronPort C Series E-Mail Security Appliance (ESA) be deployed in the DMZ to inspect E-mails and prevent threats such as E-mail spam, viruses, and worms. The ESA acts as a firewall and threat monitoring system for SMTP traffic (TCP port 25). Logically, the ESA acts as a Mail Transfer Agent (MTA) within the E-mail delivery chain, as shown in Figure 6-6.

Figure 6-6 Logical E-Mail Delivery Chain



Note Figure 6-6 shows a logical implementation of a DMZ hosting the E-mail server and ESA appliance. This can be implemented physically by either using a single firewall or two firewalls in a "sandwich" configuration.

When the ESA receives the E-mails, they are evaluated using a reputation score mechanism based on the SensorBase network, which is an extensive network that monitors global E-mail and web traffic for anomalies, viruses, malware, and other abnormal behavior. The SensorBase network consists of Cisco IronPort appliances, Cisco ASA, and IPS appliances installed in more than 100,000 organizations worldwide. This provides a large and diverse sample of Internet traffic patterns. By leveraging the information in the SensorBase network, messages originating from domain names or servers known to be the source of spam or malware, and therefore with a low reputation score, are automatically dropped or quarantined by preconfigured reputation filters.

In addition, a community college may optionally choose to implement some of the other functions offered by the ESA appliance, including anti-virus protection with virus outbreak filters and embedded anti-virus engines (Sophos and McAfee); encryption to ensure the confidentiality of messages; and data loss prevention (DLP) for E-mail to detect the inappropriate transport of sensitive information.

There are two options for deploying the ESA appliance, depending on the number of interfaces used:

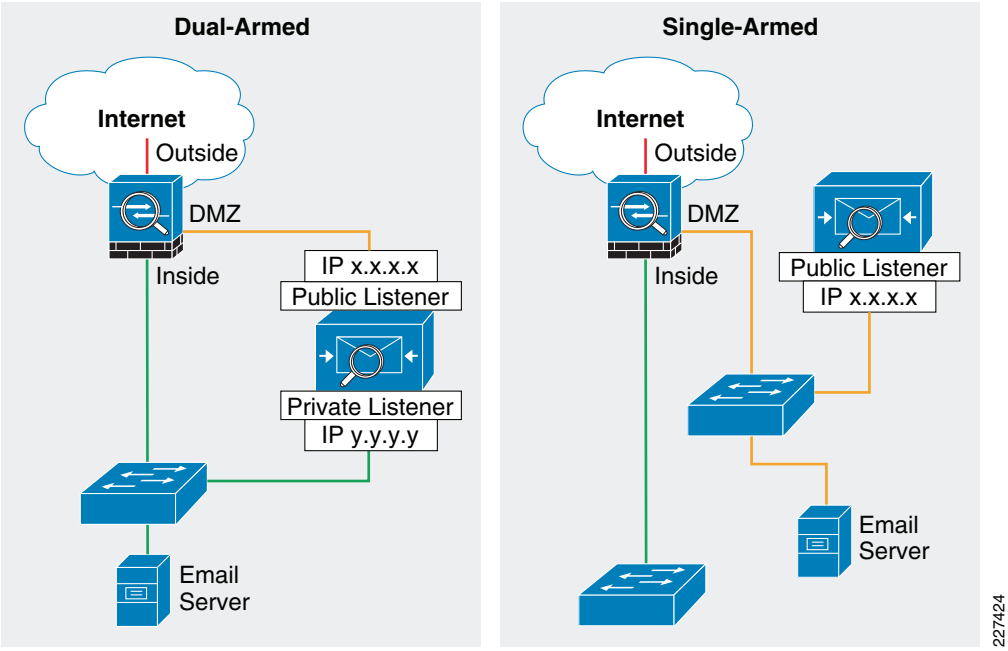
- *Dual-armed configuration*—Two physical interfaces are used to serve as a public mail listener and a private mail listener where each interface is configured with a separate logical IP address. The public listener receives E-mail from the Internet and directs messages to the internal mail servers.

The private listener receives E-mail from the internal servers and directs messages to the Internet. The public listener interface would connect to the DMZ and the private listener interface can connect to the inside of the firewall closer to the mail server.

- *One-armed configuration*—A single interface is configured on the ESA with a single IP address and used for both incoming and outgoing E-mail. A public mail listener is configured to receive and relay E-mail on that interface. The best practice is to connect the ESA interface to the DMZ where the E-mail server resides.

Figure 6-7 shows both configurations.

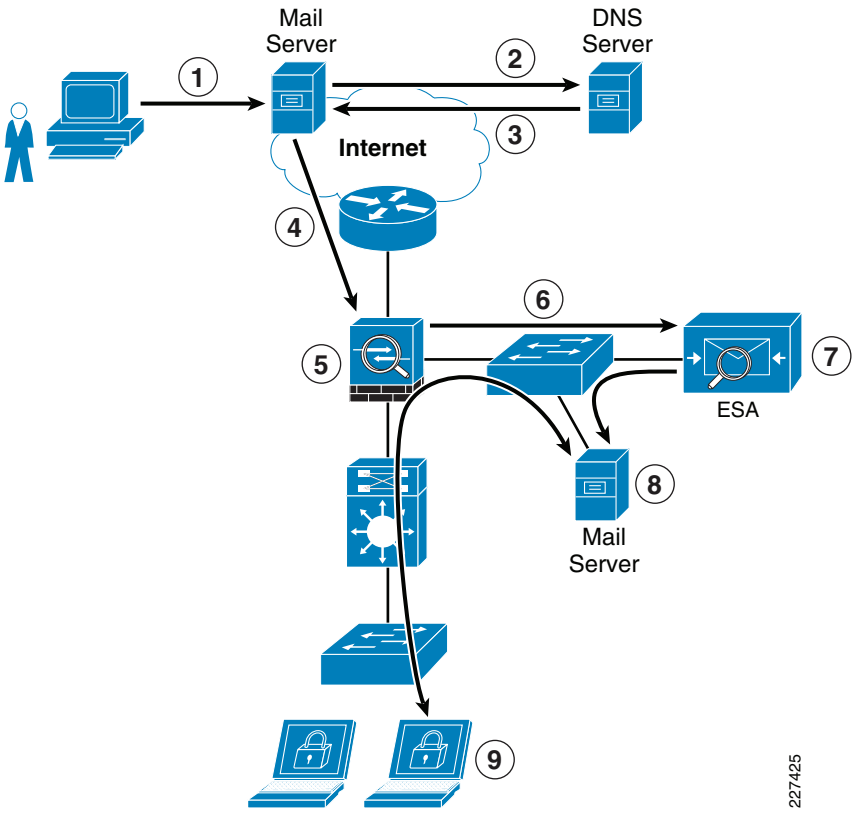
Figure 6-7 Common ESA Deployments



For simplicity, Cisco recommends that the community college network implement the ESA with a single interface in a single-armed configuration. This also leaves the other data interfaces available for redundancy.

Figure 6-8 shows the logical location of the ESA within the E-mail flow chain and the typical data flow for inbound E-mail traffic.

Figure 6-8 Typical Data Flow for Inbound E-Mail Traffic



The following steps explain what is taking place in Figure 6-8:

Step 1 Sender sends an E-mail to xyz@domain X.

Step 2 What's the IP address of domain X?

Step 3 It is a.b.c.d (public IP address of ESA).

Step 4 E-mail server sends message to a.b.c.d using SMTP.

Step 5 Firewall permits incoming SMTP connection to the ESA, and translates its public IP address.

Step 6 ESA performs a DNS query on sender domain and checks the received IP address in its reputation database, and drops, quarantines E-mail based on policy.

Step 7 ESA forwards E-mail to preconfigured inbound E-mail server.

Step 8 E-mail server stores E-mail for retrieval by receiver.

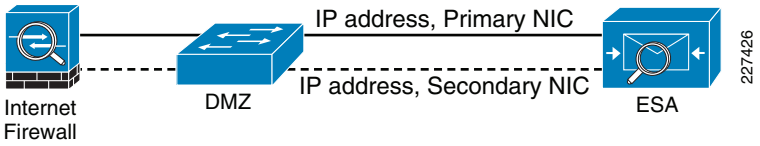
Step 9 Receiver retrieves E-mail from server using POP or IMAP.

The ESA appliance functions as an SMTP gateway, also known as a mail exchange (MX). The following outlines some of the deployment design points for the ESA within the community college design:

- The ESA appliance needs to be accessible via the public Internet and is the first hop in the E-mail infrastructure. The IP address of the sender is needed to identify and distinguish the senders in the Mail Flow Monitor to query the SensorBase Reputation Service for the SensorBase Reputation Service Score (SBRS) of the sender. Therefore, a separate MTA should not be deployed at the network perimeter to handle the external connections.
- The ESA needs to be registered in DNS for features such as IronPort Anti-Spam, Virus Outbreak Filters, MacAfee Antivirus, and Sophos Antivirus. A DNS "A" record should be created to map the appliance hostname to its public IP address, and an MX record that maps the public domain to the appliance hostname. A priority is specified for the MX record to advertise the ESA appliance as the primary MTA for the domain.
- A static IP address translation entry on the Internet firewall should be defined to map the public IP address of the ESA to its private internal address.
- All the local domains for which the ESA appliances accept mail need to be added to the recipient access table (RAT). Inbound E-mail destined to domains not listed in the RAT is rejected. External E-mail servers connect directly to the ESA appliance to transmit E-mail for the local domains, and the ESA appliance relays the mail to the appropriate groupware servers (for example, Exchange™, GroupWise™, Domino™) via SMTP routes.
- For each private listener, the host access table (HAT) must be configured to indicate the hosts that are allowed to send E-mails. The ESA appliance accepts outbound E-mail based on the settings of the HAT table. Configuration includes the definition of sender groups associating groups or users, and on which mail policies can be applied. Policies include the following:
  - Mail flow policies—A way of expressing a group of HAT parameters; access rule, followed by rate limit parameters and custom SMTP codes and responses
  - Reputation filtering—Allows the classification of E-mail senders, and restricting E-mail access based on sender trustworthiness as determined by the IronPort SensorBase Reputation Service.
- SMTP routes are defined to direct E-mail to the appropriate internal mail servers.
- If an OOB management network is available, a separate interface for administration should be used.

Because a failure on the ESA appliance may cause a service outage, a redundant design is recommended. One way to implement redundancy is to use IronPort NIC pairing, as shown in Figure 6-9.

Figure 6-9 Cisco IronPort ESA NIC Pairing



IronPort NIC pairing provides redundancy at the network interface card level by teaming two of the Ethernet interfaces in the ESA appliance. If the primary interface fails, the IP address and MAC address are moved to the secondary interface. IronPort NIC pairing is the most cost-effective solution because it does not require the deployment of multiple ESA appliances and other hardware. However, it does not provide redundancy in case of chassis failure.

Alternative redundant designs include the following:

- *Multiple MTAs*—Adding a second ESA appliance or MTA and using a secondary MX record with an equal cost to load balance between the MTAs.
- *Load balancer*—Using a load balancer such as the Cisco Application Control Engine (ACE) to load balance traffic across multiple ESA appliances.

To accommodate traffic to and from the IronPort ESA provisioned in the DMZ, the Internet firewall needs to be configured to allow this communication. Protocols and ports to be allowed vary depending on the services configured on the ESA.

The following are some of the common services required to be allowed through the Internet firewall:

- Outbound SMTP (TCP/25) from ESA to any Internet destination
- Inbound SMTP (TCP/25) to ESA from any Internet destination
- Outbound HTTP (TCP/80) from ESA to downloads.ironport.com and updates.ironport.com
- Outbound SSL (TCP/443) from ESA to updates-static.ironport.com and phonehome.senderbase.org
- Inbound and outbound DNS (TCP and UDP port 53)
- Inbound IMAP (TCP/143), POP (TCP/110), SMTP (TCP/25) to E-mail server from any internal client

For more information on how to configure the ESA, see the following guides:

- Cisco SAFE Reference Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html
- Cisco IronPort ESA User Guide—http://www.ironport.com/support

Web Security

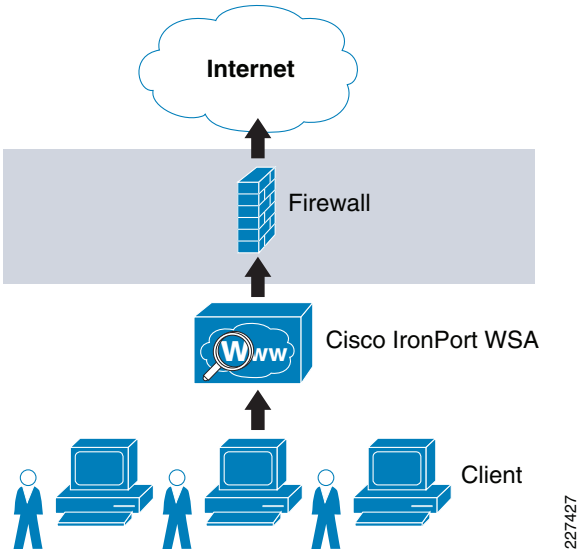
The Community College reference design implements a Cisco IronPort S Series Web Security Appliance (WSA) to block HTTP and HTTPS access to sites on the Internet with content that may be harmful, and to protect the community college network from web-based malware and spyware.

The following services may be enabled on the WSA:

- *Web proxy*—Provides URL filtering, web reputation filters, and optionally anti-malware services. The URL filtering capability defines the handling of each web transaction based on the URL category of the HTTP requests. Leveraging the SensorBase network, the web reputation filters analyze the web server behavior and characteristics to identify suspicious activity and protect against URL-based malware. The anti-malware service leverages anti-malware scanning engines such as Webroot and McAfee to monitor for malware activity.
- *Layer 4 traffic monitoring (L4TM)*—Monitors all Layer 4 traffic for rogue activity, and to detect infected clients.

The community college design assumes a centralized Internet connection implemented at the main campus site. The WSA should be implemented at the distribution layer in the Internet perimeter network. This allows for the inspection and enforcement of web access polices to all students, staff, and faculty located at any of the community college campuses. Logically, the WSA sits in the path between web users and the Internet, as shown in Figure 6-10.

Figure 6-10 Cisco IronPort WSA



There are the following two deployment modes when enabling the Cisco IronPort WSA Web Proxy service:

- *Explicit forward proxy*—Client applications, such as web browsers, are aware of the web proxy and must be configured to point to the WSA as its proxy. The web browsers can be configured either manually or by using proxy auto configuration (PAC) files. Manual configuration does not allow for redundancy, while the use of PAC files allows the definition of multiple WSAs for redundancy and load balancing. If supported by the browser, the Web Proxy Auto-discovery Protocol (WPAD) can be used to automate the deployment of PAC files. WPAD allows the browser to determine the location of the PAC file using DHCP and DNS lookups.
- *Transparent proxy*—Client applications are unaware of the web proxy and do not have to be configured to connect to the proxy. This mode requires the implementation of a Web Cache Communications Protocol (WCCP)-enabled device or a Layer 4 load balancer to intercept and redirect traffic to the WSA before going to the Internet. Both WCCP and Layer 4 load balancer options provide for redundancy and load balancing.

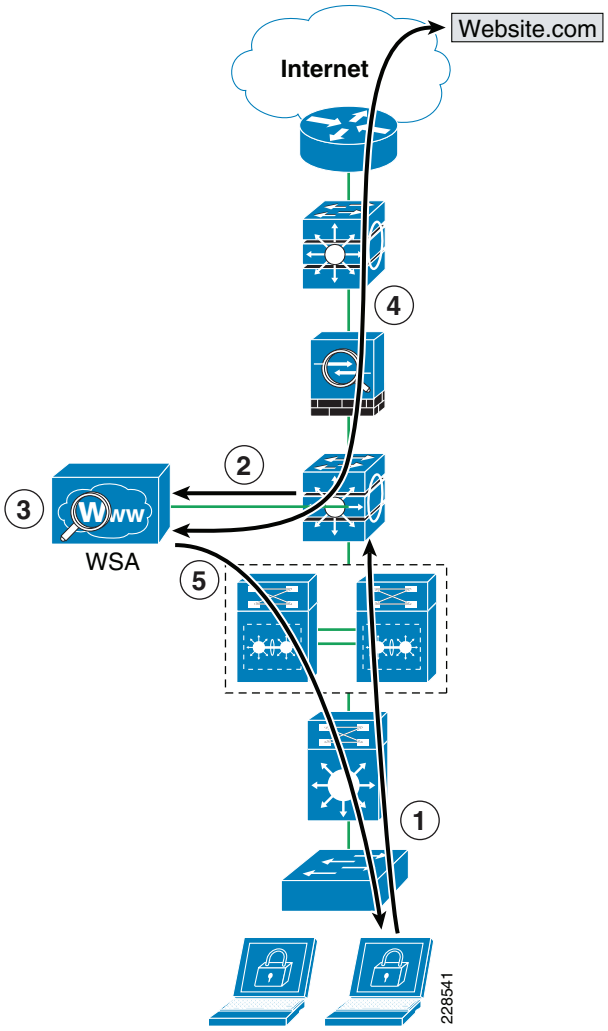
Explicit forward proxy mode requires administrators to have control over the configuration of the endpoints, which is often not the case in community college environments. For example, community colleges may allow students, guests, or visiting professors to use personal laptops, smart phones, or other devices outside the administration of the institution. Conversely, transparent proxy mode provides transparent integration of WSA without requiring any configuration control over the endpoints. In addition, transparent proxy also eliminates the possibility of users reconfiguring their web browsers to bypass the WSA appliance without the knowledge of the administrators. For these reasons, Cisco recommends that community colleges implement transparent proxy mode with WCCP. In the Community College reference design, the Cisco Catalyst 3750 Stackwise distribution switches deployed in the Internet perimeter can be leveraged as the WCCP server while the WSA acts as a WCCP traffic processing entity.

The Cisco Catalyst 3750 switches support WCCP version 2, which has a built-in failover and load balancing mechanism. Per the WCCPv2 specifications, multiple appliances (up to 32 entities) can be configured as part of the same service group. HTTP and HTTPS traffic is load balanced across the active WSA appliances based on source and destination IP addresses. The WCCP server (Cisco Catalyst 3750 switch) monitors the availability of each appliance in the group and can identify the appliance failures in 30 seconds. After failure, the traffic is redirected across the remaining active appliances. In the case

where no appliances are active, WCCP takes the entire service group offline and subsequent requests bypass redirection. In addition, WCCPv2 supports MD5 authentication for the communication between the WCCP server and the WSA appliances.

Figure 6-11 shows how WCCP redirection works in conjunction with the Cisco Catalyst 3750 StackWise distribution switches.

Figure 6-11 WCCP Redirection



As shown in Figure 6-11, the following steps take place:

Step 1 The client browser requests a connection to http://website.com.

Step 2 The Cisco Catalyst 3750 Internet perimeter distribution switch intercepts and redirects HTTP/HTTPS requests to WSA via Layer 2 redirection.

Step 3 If the content is not present in the local cache, WSA performs a DNS query on the destination site and checks the received IP address against URL and reputation rules, and allows/denies the request accordingly.

Step 4 If allowed, WSA fetches the content from the destination website.

Step 5 The content is inspected and then delivered to the requesting client.

Note In the event that the entire service group fails, WCCP automatically bypasses redirection, allowing users to browse the Internet without the web controls. If it is desired to handle a group failure by blocking all traffic, an inbound ACL may be configured on the Cisco ASA inside interface to permit only HTTP/HTTPS traffic originated from the WSA appliance itself, and to block any direct requests from clients. The ACL may also have to be configured to permit HTTP/HTTPS access from IPS and other systems requiring direct access to the Internet without going through the WSA proxy.

WCCPv2 supports Generic Route Encapsulation (GRE) and Layer 2-based redirection. The Cisco Catalyst 6500 and 3750 switches support Layer 2-based redirection, and the redirection is supported in hardware. Therefore, the WSA must be directly connected to the switch running WCCP. In addition, WCCP is supported only on the ingress of an interface. For these reasons, WSA should connect directly to the Internet perimeter distribution switch using a VLAN that is different than the VLAN from where the client traffic is coming.

Note The Cisco Catalyst 4500 does not provide the ability to create WCCP traffic redirect exception lists, which is an important component of the design. If a Cisco Catalyst 4500 is implemented as the distribution layer switch, another device, such as the Cisco ASA, should be used as the WCCP server.

The following describes some of the design considerations and caveats for implementing a Cisco IronPort WSA with WCCP on a Cisco Catalyst 3750 switch:

- The WSA must be Layer 2-adjacent to the Cisco Catalyst 3750 switch.
- The WSA and switches in the same service group must be in the same subnet directly connected to the switch that has WCCP enabled.
- Configure the switch interfaces that are facing the downstream web clients, the WSA(s), and the web servers as Layer 3 interfaces (routed ports or switch virtual interfaces [SVIs]).
- Use inbound redirection only.
- WCCP is not compatible with VRF-Lite. WCCP does not have visibility into traffic that is being used by the virtual routing tables with VRFs.
- WCCP and policy-based routing (PBR) on the same switch interface are not supported.
- WCCP GRE forwarding method for packet redirection is not supported.
- Use MD5 authentication to protect the communication between the Cisco Catalyst 3750 switches and the WSA(s).
- Use redirect-lists to specifically control what hosts/subnets should be redirected.
- Cisco Catalyst 3750 switches support switching in hardware only at Layer 2; therefore, no counters increment when the command **show ip wccp** is issued on the switch.
- In an existing proxy environment, deploy the WSA downstream from the existing proxy servers (closer to the clients).
- If an OOB management network is available, use a separate interface for WSA administration.

For more information on WCCP in relation to the Cisco Catalyst 3750 switch, see the following URL: http://www.cisco.com/en/US/docs/switches/lan/catalyst3750e_3560e/software/release/12.2_46_se/configuration/guide/swwccp.html.

Note WCCP, firewall, and other stateful features typically require traffic symmetry where traffic in both directions should flow through the same stateful device. Care should be taken when implementing active-active firewall pairs because they may introduce asymmetric paths.

The WSA appliance may also be configured to control or block peer-to-peer file sharing and instant messaging applications such as AOL Messenger, BitTorrent, Skype, Kazaa, and so on. Depending on the port used for transport, the WSA handles these applications as follows:

- Port 80—Applications that use HTTP tunneling on port 80 can be handled by enforcing access policies within the web proxy configuration. Applications access can be controlled based on applications, URL categories, and objects. Applications are matched based on their user agent pattern, and the use of regular expressions. URLs can be blocked based on specific categories, such as predefined chat and peer-to-peer categories, or custom categories defined by the administrator. Peer-to-peer access can also be filtered based on object and Multipurpose Internet Mail Extensions (MIME) types.
- Ports other than 80—Applications using ports other than 80 can be handled with the L4TM feature. L4TM can block access to specific applications by preventing access to the server or IP address blocks to which the client application must connect.

In the community college design, the Internet perimeter firewall can be configured to allow only web traffic (HTTP and HTTPS) outbound to the Internet from only the WSA. This prevents users from bypassing the WSA to browse the Internet.

Note Peer-to-peer file sharing and Internet instant messaging applications can also be blocked using Cisco IPS appliances and modules and the Cisco ASA firewall (using modular policy framework).

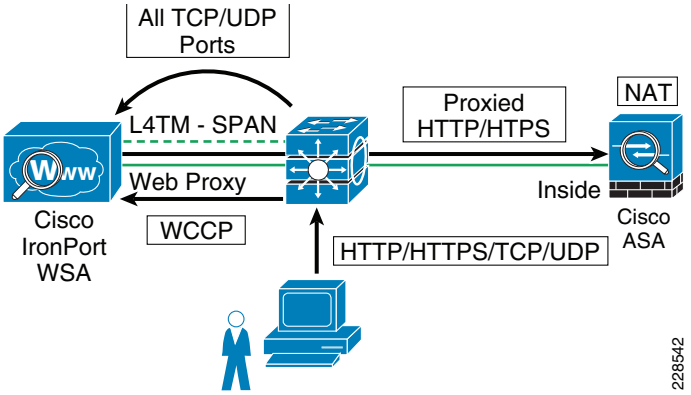
The WSA L4TM service is deployed independently from the web proxy functionality. L4TM monitors network traffic for rogue activity and for any attempts to bypass port 80. It works by listening to all UDP and TCP traffic and by matching domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic. The L4TM internal database is continuously updated with periodic updates from the Cisco IronPort update server (https://update-manifests.ironport.com).

The following are some of the key guidelines when deploying L4TM:

- *Physical connection*—L4TM requires a copy of the traffic to be redirected to the WSA for monitoring. This can be done by connecting a physical network tap, configuring Switch Port Analyzer (SPAN) port mirroring on a Cisco Catalyst switch, or using a hub. Network TAPs forward packets in hardware, while SPAN port mirroring is generally done in software. However, SPAN port mirroring can be easily reconfigured, providing more flexibility.
- *Location*—L4TM should be deployed in the network where it can see as much traffic as possible before going out to the Internet through the firewall. Monitoring should occur before any device that performs NAT on client IP addresses.
- *Action setting*—The default action setting for L4TM is to passively monitor only. Optionally, you can configure L4TM to monitor and actively block suspicious traffic. TCP connections are reset by the generation of TCP resets, and UDP sessions are torn down using ICMP unreachables. The use of L4TM blocking requires that the L4TM and web proxy services are placed on the same network so that all clients are accessible on routes that are configured for data traffic.

In the community college design, L4TM can be deployed by configuring a SPAN session on the Internet perimeter distribution switch to monitor all TCP and UDP traffic on the links connecting to the core distribution switches. Using SPAN provides greater flexibility. Monitoring the distribution switches link to the core switches ensures that all client traffic is inspected before NAT and before traffic is sent to the Internet. Figure 6-12 shows this L4TM deployment option.

Figure 6-12 L4TM Deployment



If the Internet perimeter firewall is configured to block all traffic bound to the Internet except HTTP and HTTPS traffic from the WSA, or the ASA Botnet Traffic Filter feature is enabled, L4TM may not provide any additional benefit. Also, if active mitigation is required, the Cisco ASA Botnet Traffic Filter Feature or a Cisco IPS appliance or module deployed in inline mode is recommended. Both the ASA Botnet Traffic Filter and inline IPS provide better mitigation by blocking traffic automatically inline, stopping malicious traffic before it reaches the intended target.

For more information on how to configure the WSA, see the following guides:

- Cisco SAFE Reference Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html.
- IronPort WSA User Guide—http://www.ironport.com/support.

Data Center Protection

Community colleges typically implement a data center that hosts the systems that serve the administrative and educational applications and store the data accessible to internal users. The infrastructure supporting them may include application servers, storage media, routers, switches, load balancers, off-loaders, application acceleration devices, and other systems. In addition, they may also host foundational services as part of the Community College reference design such as identity and security services, unified communication services, mobility services, video services, partner applications, and other services.

Depending on the need and the size of the community college, a single data center may be deployed in the main campus. Smaller data centers or server farms may also be deployed in remote campuses as required.

Securing the data center is beyond the scope of this document. For more information on the best practices for securing a data center, see “Chapter 4: Intranet Data Center” of the Cisco SAFE Reference Guide at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap4.html.

Network Access Security and Control

One of the most vulnerable points of a network is at the access edge. The access layer is where end users such as students, staff, and faculty connect to the network. In the past, network administrators have largely relied on physical security to protect this part of the network. Unauthorized users were not allowed to enter secure buildings where they could plug into the network, and students did not carry computers with them. Today, with the proliferation of wireless networks, increased use of laptops and smart mobile devices, the community college IT department cannot simply rely on physical controls to prevent these unauthorized devices from plugging into ports of the access switches. Contractors and consultants regularly have access to secure areas, and students carrying laptops are common. There is nothing preventing a contractor or student from plugging into a wall jack in a classroom, lab, or conference room to gain access to the community college network. When connected to the network, everyone has access to all resources on the network.

Protection needs to be embedded into the network infrastructure, leveraging the native security features available in switches and routers. In addition, the network infrastructure should also provide dynamic identity or role-based access controls for all devices attempting to gain access. Implementing role-based access controls for users and devices help reduce the potential loss of sensitive information by enabling administrators to verify a user or device identity, privilege level, and security policy compliance before granting access to the network. Security policy compliance can consist of requiring anti-virus software, OS updates, or patches. Unauthorized or noncompliant devices can be placed in a quarantine area where remediation can occur before network access.

The Community College reference design achieves access security and control by leveraging the following technologies:

- Cisco Catalyst Integrated Security Features (CISF)
- Cisco Network Admission Control (NAC) Appliance
- Cisco Identity-Based Network Services (IBNS)

Cisco Catalyst Integrated Security Features

Cisco CISF is a set of security features available on Cisco Catalyst switches designed to protect the access layer infrastructure and users from spoofing, man-in-the-middle (MITM), DoS, and other network-based attacks. CISF should be considered part of the security baseline of any network and should be deployed on all access switches and ports within the community college network architecture.

CISF includes the following features:

- *Port Security*—Mitigates MAC flooding and other Layer 2 CAM overflow attacks by restricting the MAC addresses that are allowed to send traffic on a particular port. After Port Security is enabled on a port, only packets with a permitted source MAC address are allowed to pass through the port. A permitted MAC address is referred to as a secure MAC address.
- *DHCP Snooping*—Inspects and filters DHCP messages on a port to ensure DHCP server messages come only from a trusted interface. Additionally, it builds and maintains a DHCP snooping binding table that contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information corresponding to the local untrusted interfaces of a switch. This binding table is used by the other CISF features.
- *Dynamic ARP inspection (DAI)*—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 (using the DHCP snooping binding table) to prevent ARP spoofing and MITM attacks.

- *IP Source Guard*—Restricts IP traffic on a port based on DHCP or static IP address MAC bindings to prevent IP spoofing attacks. IP address bindings are validated using information in the DHCP Snooping binding table.
- *Storm Control*—Prevents broadcast and multicast storms by monitoring packets passing from an interface to the switching bus and determines whether 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. When the suppression-level threshold is reached, the port blocks traffic until the traffic falls below the threshold level.

Cisco Identity-Based Network Services

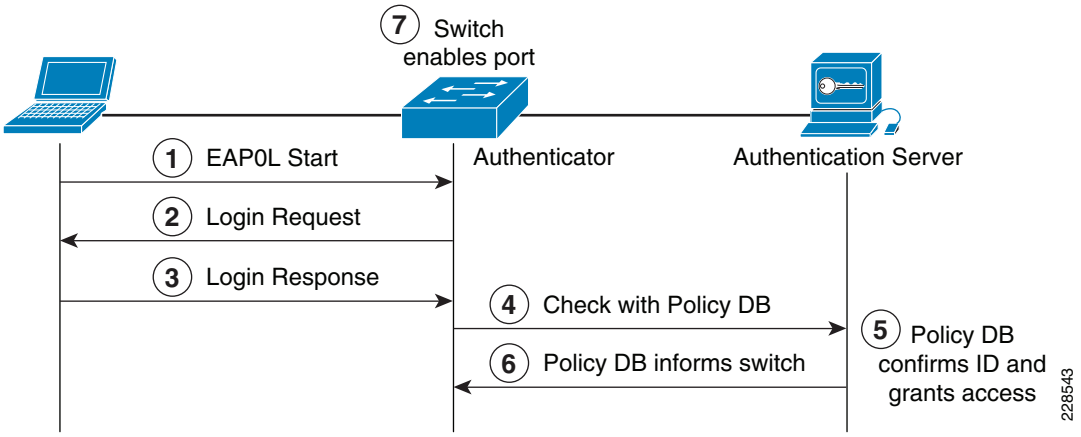
The Cisco IBNS solution is a set of Cisco IOS software services that provide secure user and host access to enterprise networks powered by Cisco Catalyst switches and wireless LANs. It provides standards-based network access control at the access layer by using the 802.1X protocol to secure the physical 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. 802.1X is a well-known way to secure wireless network access and is also capable of securing wired network access.

IEEE 802.1X Protocol

The IEEE 802.1X protocol allows Cisco Catalyst switches to offer network access control at the port level. Every port on the switch is individually enabled or disabled based on the identity of the user or device connecting to it. When 802.1X is first enabled on a port, the switch automatically drops all traffic received on the port except the request to start 802.1X authentication. After the 802.1X authentication successfully completes, the switch starts accepting other kinds of traffic on the port.

The high-level message exchange shown in Figure 6-13 illustrates how port-based access control works within an identity-based system.

Figure 6-13 Port-Based Access Control



The following steps describe the port-based access control flow shown in Figure 6-13:

Step 1 A client, such as a laptop with an 802.1X supplicant, connects to an IEEE 802.1X-enabled network and sends a start message to the LAN switch (the authenticator).

Step 2 When the start message is received, the LAN switch sends a login request to the client.

Step 3 The client replies with a login response.

Step 4 The switch forwards the response to the policy database (authentication server).

Step 5 The authentication server authenticates the user.

Step 6 After the user identity is confirmed, the policy database authorizes network access for the user and informs the LAN switch.

Step 7 The LAN switch then enables the port connected to the client.

The user or device credentials are processed by a AAA server. The AAA server is able to reference user or device profile information either internally, using the integrated user database, or externally using database sources such as Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), Novelle Directory, or Oracle databases. This enables the IBNS solution to be integrated into existing user management structures and schemes, which simplifies overall deployment.

802.1X and EAP

When authenticating users for network access, the client must provide user and/or device identification using strong authentication technologies. IEEE 802.1X does not dictate how this is achieved. Instead, the 802.1X protocol defines an encapsulation for the transport of the Extensible Authentication Protocol (EAP) from the client to the switch. The 802.1X encapsulation is sometimes referred to as EAP over LAN (EAPoL). The switch in turn relays the EAP information to the authentication server using the RADIUS protocol (EAP over RADIUS).

EAP is defined by RFC 3748. EAP is a framework and not a specific authentication method. It provides a way for the client and the authentication server to negotiate an authentication method that they both support. There are many EAP methods, but the ones used more frequently for 802.1X wired authentication include EAP-TLS, EAP-PEAP, and EAP-FAST.

Impacts of 802.1X on the Network

When 802.1X is enabled on a port, the default security posture is to drop all traffic except 802.1X EAPoL packets. This is a fundamental change from the traditional model, where traffic is allowed from the moment a port is enabled and a device is plugged into the port. Ports that were traditionally open are now closed by default. This is one of the key elements of the strong security and network access control provided by 802.1X. Understanding and accommodating for this change in access behavior facilitates a smooth deployment of 802.1X network access control.

Non-802.1X-Enabled Devices

802.1X must be enabled on both the host device and on the switch to which it connects. If a device without an 802.1X supplicant attempts to connect to a port that is enabled for 802.1X, it is subjected to the default security posture. The default security posture says that 802.1X authentication must succeed before access to the network is granted. Therefore, by default, non-802.1X-capable devices cannot get access to a 802.1X-protected network.

Although an increasing number of devices support 802.1X, there are always devices that require network connectivity but do not and/or cannot support 802.1X. Examples of such devices include network printers, badge readers, legacy servers, and Preboot Execution Environment (PXE) boot machines. Some provisions must be made for these devices.

The Cisco IBNS solution provides two features to accommodate non 802.1X devices. These are MAC Authentication Bypass (MAB) and Guest VLAN. These features provide fallback mechanisms when there is no 802.1X supplicant. After 802.1X times out on a port, the port can move to an open state if MAB succeeds or if a Guest VLAN is configured. Application of either or both of these features is required for a successful 802.1X deployment.

Note Network-specific testing is required to determine the optimal values for the 802.1X timers to accommodate the various non-802.1X-capable devices on your network.

802.1X in Community Colleges

As mentioned in the previous sections, 802.1X authentications require a supplicant on the host device. This typically poses a problem in community college environments that have a wide range of host devices and limited or no management of many of these devices. This makes a community college-wide 802.1X deployment very challenging. However, there may be pockets of a community college network where 802.1X may be a good choice.

For example, 802.1X protected ports may be a good choice for the network ports in the school administration office or shared labs where PCs are managed. Other locations in the community college network still need protection, but student and faculty network access may be better served by a NAC Appliance Solution (discussed in the next section). In addition, for networks requiring role-based access control using posture assessments to ensure security compliance, Cisco NAC Appliance should be considered.

For more information on the Cisco IBNS 802.1X network access solution, see the following URL: http://www.cisco.com/go/ibns.

Cisco NAC Appliance

Cisco Network Admission Control (NAC) Appliance (formerly known as Cisco Clean Access) uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With Cisco NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines before network access. The NAC Appliance identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network security policies, and can repair any vulnerability before permitting access to the network.

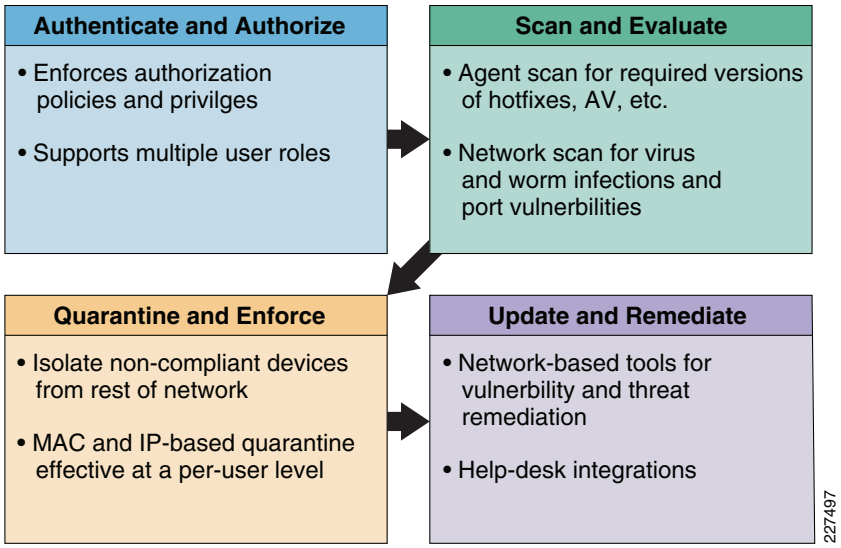
When deployed, Cisco NAC Appliance provides the following benefits:

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

The NAC solution provides the following four functions, as shown in Figure 6-14:

- Authenticates and authorizes
- Scans and evaluates
- Quarantines and enforces
- Updates and remediates

Figure 6-14 Four Functions of the NAC Solution



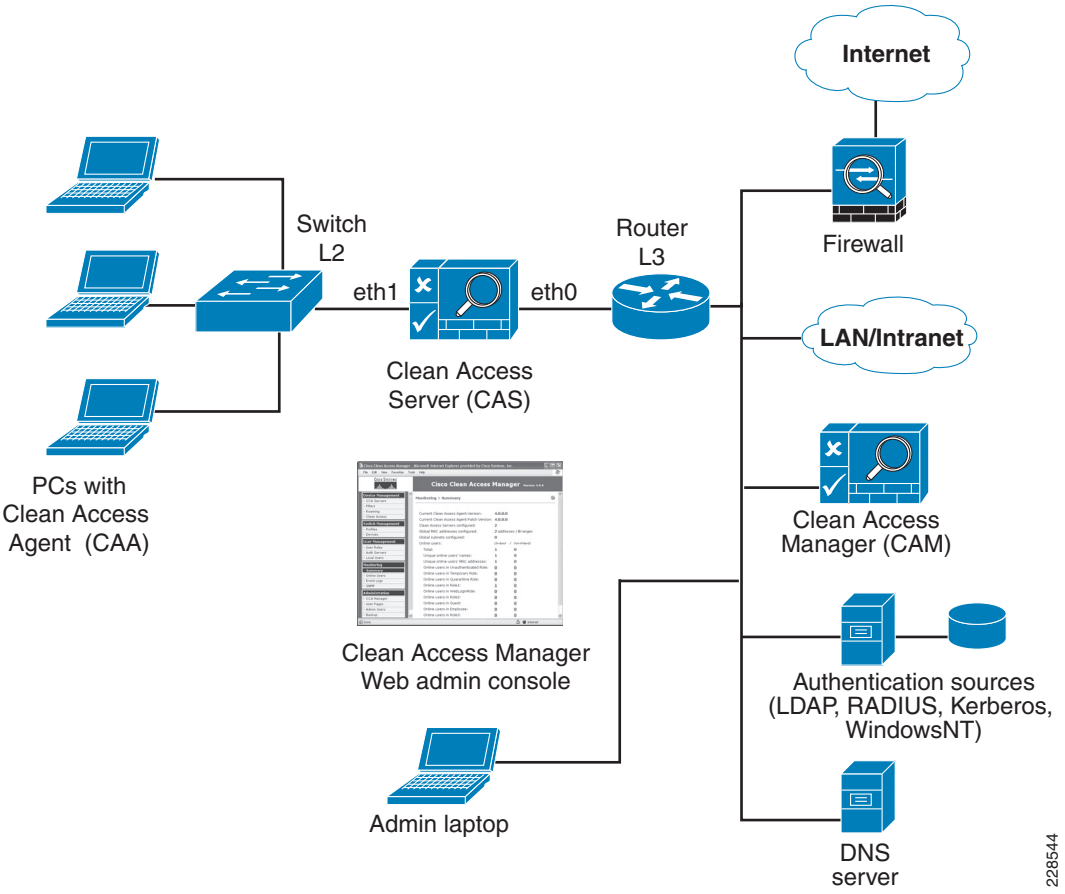
For more details of the NAC Appliance Solution, see the following URL: http://www.cisco.com/go/nacappliance.

NAC Appliance Components

Cisco NAC Appliance is a network-centric, integrated solution administered from the Cisco Clean Access Manager (CAM) web console and enforced through the Cisco Clean Access Server (CAS) and (optionally) the Clean Access Agent (CAA) or NAC Web Agent. Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and antivirus software, and quarantines vulnerable or infected clients for remediation before clients access the network.

Figure 6-15 shows Cisco NAC Appliance components.

Figure 6-15 NAC Appliance Components



Cisco Clean Access Manager

The Cisco CAM is the administration server for NAC Appliance deployments. The secure web console of the CAM is the single point of management for up to 20 Clean Access Servers in a deployment (or 40 CASs if using a SuperCAM). For OOB deployments, the web administration console controls the switches and VLAN assignment of user ports through the use of SNMP. In the Community College reference design, the CAM is located in the data center at the main campus site.

Cisco Clean Access Server

The Cisco CAS is the enforcement server between the untrusted network and the trusted network. The CAS enforces the policies defined by the CAM web administration console. Policies can include network access privileges, authentication requirements, bandwidth restrictions, and system requirements. The CAS can be installed as either a standalone appliance (like the Cisco NAC-3300 Series) or as a network module (Cisco NME-NAC-K9) in a Cisco ISR chassis. The CAS can be deployed in in-band (always inline with user traffic) or OOB (inline with user traffic only during authentication and posture assessment).

Additionally, the CAS can be deployed in Layer 2 mode (users are Layer 2-adjacent to the CAS) or Layer 3 mode (users are multiple Layer 3 hops away from the CAS). Multiple CASs of varying size/capacity can be deployed to fit the needs of various network segments. For example,

Cisco NAC-3300 Series appliances can be installed in a main campus core to handle thousands of users, and one or more Cisco NAC network modules can be simultaneously installed in ISR platforms to accommodate smaller groups of users in a satellite office.

In the Community College reference design, the CAS would be located at the main campus and the remote campus sites, and deployed in Layer 2 OOB (for wireless clients) and Layer 3 OOB (for wired clients) modes for authentication and posture assessments.

Cisco Clean Access Agent

The Cisco CAA is an optional read-only agent that resides on Windows clients. It checks applications, files, services, or registry keys to ensure that clients meet the specified network and software requirements before gaining access to the network.

Note There is no client firewall restriction with CAA posture assessment. The agent can check the client registry, services, and applications even if a personal firewall is installed and running.

In the community college, Cisco recommends that the CAA be used for the managed PCs, such as those for administrators and faculty.

Cisco NAC Web Agent

The Cisco NAC Web Agent provides temporal posture assessment for client machines. Using a Web browser, users launch the Cisco Web Agent executable file, 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 the network and their user ID disappears from the online users list.

In the Community College reference design, the NAC Web Agent is used for unmanaged clients such as student laptops and guest professors.

Clean Access Policy Updates

Regular updates of prepackaged policies/rules can be used to check the up-to-date status of operating systems, anti-virus (AV), anti-spyware (AS), and other client software. Built-in support is provided for 24 AV and 17 AS vendors.

NAC Appliance Modes and Positioning

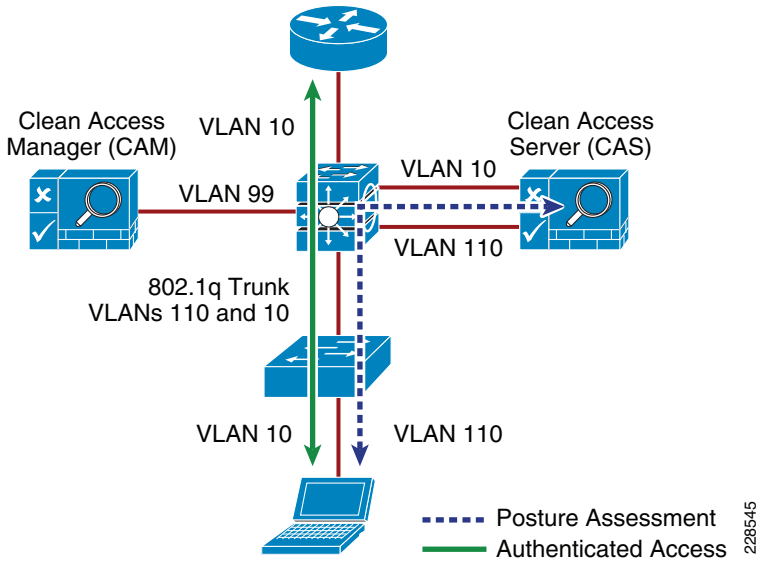
The NAC Appliance can be deployed in multiple deployment options and placed at various locations in the network. The modes of operation can be generally defined as follows:

- Out-of-band (OOB) virtual gateway
- OOB real IP gateway
- In-band (IB) virtual gateway
- IB real IP gateway

OOB Modes

OOB deployments require user traffic to traverse through the NAC Appliance only during authentication, posture assessment, and remediation (see Figure 6-16). When a user is authenticated and passes all policy checks, their traffic is switched normally through the network and bypasses the NAC Appliance.

Figure 6-16 Layer 2 OOB Topology



To deploy the NAC Appliance in OOB mode, the client device must be directly connected to the network via a Cisco Catalyst switch port. After the user is authenticated and passes posture assessment, the CAM instructs the switch to map the user port from an unauthenticated VLAN (which switches or routes user traffic to the CAS) to an authenticated (authorized) VLAN that offers full access privileges. For example, as shown in Figure 6-16, the client PC is connected through VLAN 110 to the NAC CAS for the authentication and posture assessment, and is moved to VLAN 10 after it successfully completes the authentication/authorization and scan/evaluation phases of the NAC Appliance solution.

In-Band Modes

When the NAC Appliance is deployed in-band, all user traffic, both unauthenticated and authenticated, passes through the NAC Appliance. The CAS may be positioned logically or physically between the end users and the networks being protected. Figure 6-17 shows a logical in-band topology example, and Figure 6-18 shows a physical in-band topology example.

Figure 6-17 In-Band Virtual Gateway Topology

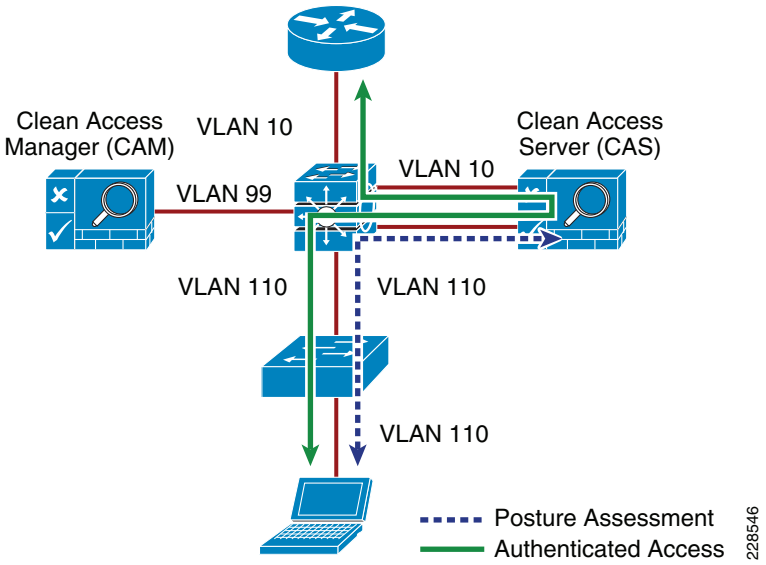
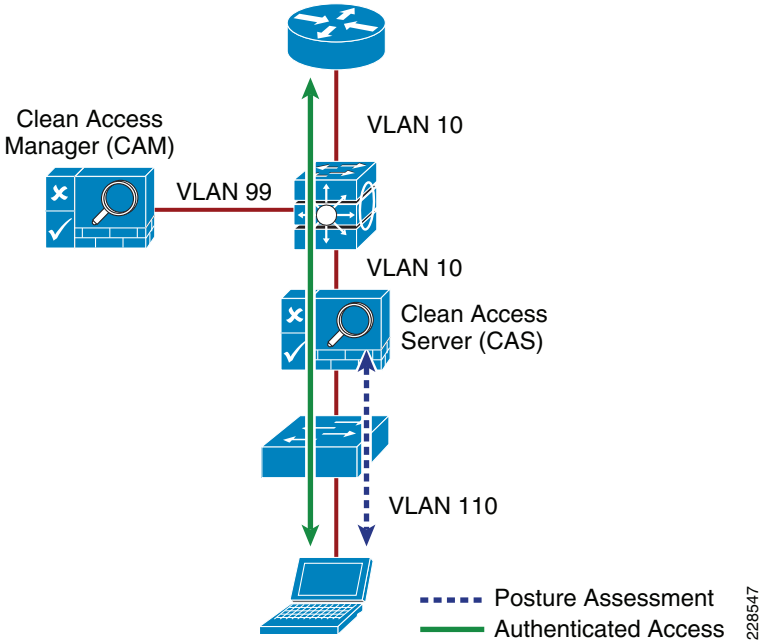


Figure 6-18 Physical In-Band Topology



In-Band Virtual Gateway

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

- *Transparent*—For a given client VLAN, the NAC server bridges traffic from its untrusted interface to its trusted interface. The NAC server is aware of "upper layer" protocols and is able to permit those protocols that are necessary for a client to connect to the network, authenticate, and undergo

posture assessment and remediation. By default, it blocks all traffic except for Bridge Protocol Data Unit (BPDU) frames (spanning tree), and those protocols explicitly permitted in the "unauthorized" role, such as DNS and DHCP. This option is viable when the NAC server is positioned physically in-band between the end users and the upstream network(s) being protected, as shown in Figure 6-18.

- *VLAN mapping*—This is similar in behavior to the transparent option except that rather than bridging the same VLAN from the untrusted side to the trusted side of the NAC server, two separate VLANs are used. For example, client VLAN 110 is defined for the untrusted interface of the NAC server. There is no routed interface or SVI associated with VLAN 110. VLAN 10 is configured between the trusted interface of the NAC server and the next-hop router interface (or SVI) for the client subnet. A mapping rule is made in the NAC server that forwards packets arriving on VLAN 110 and forwards them out VLAN 10 by swapping VLAN tag information. The process is reversed for packets returning to the client. Also, in this mode, BPDUs are not passed from the untrusted-side VLANs to their trusted-side counterparts.

The VLAN mapping option is typically used when the NAC server is positioned logically in-band between clients and the network(s) being protected, as shown in Figure 6-17. This is the bridging option that should be used if the NAC Appliance is deployed in virtual gateway mode.

In-Band Real IP Gateway

When the NAC server is configured as a "real" IP gateway, it behaves like a router and routes packets between its interfaces. In this scenario, one or more client VLAN/subnets resides behind the untrusted interface. The NAC server acts as a default gateway for all clients residing on those networks. Conversely, a single VLAN/subnet is defined on the trusted interface, which represents the path to the protected upstream network(s). After successful client authentication and posture assessment, the NAC server by default routes traffic from the untrusted networks to the trusted interface, where it is then forwarded based on the routing topology of the network.

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

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

Depending on the topology, multiple options exist to facilitate routing clients to and from the NAC server, including ACLs, static routes, PBR, VRF-Lite, Multiprotocol Label Switching (MPLS) VPN, and other segmentation techniques. These options are discussed in later sections.

In-Band Versus Out-of-Band

Table 6-1 summarizes various characteristics of the two deployment types.

Table 6-1 In-Band versus Out-of-Band Characteristics

In-Band Deployment Characteristics	Out-of-Band Deployment Characteristics
The CAS is always inline with user traffic (both before and after authentication, posture assessment, and remediation). Enforcement is achieved through being inline with traffic.	The CAS is inline with the user traffic only during the process of authentication, posture assessment, and remediation. After that, user traffic does not go to the CAS. Enforcement is achieved through the use of SNMP to control switches and VLAN assignments to end-user ports.

Table 6-1 In-Band versus Out-of-Band Characteristics (continued)

The CAS can be used to securely control authenticated and unauthenticated user traffic policies (based on port, protocol, subnet), bandwidth policies, and so on.	The CAS can control user traffic during the authentication, posture assessment, and remediation phases but cannot do so post remediation because traffic is out-of-band.
Does not provide switch port level control.	Provides port-level control by assigning ports to specific VLANs as necessary using SNMP.
In-band deployment is supported for wired and wireless clients.	OOB deployments support wired and wireless clients. Wireless OOB requires a specific network topology.[1]
Cisco NAC in-Band deployment with supported Cisco switches is compatible with 802.1X.	Cisco does not recommend using 802.1X in an OOB deployment, because conflicts will likely exist between Cisco NAC Appliance OOB and 802.1X in setting the VLAN on the switch interfaces/ports.

1. OOB NAC deployments for wireless require the NAC server to be deployed in Layer 2 OOB virtual gateway (bridge) mode, and the NAC server must be placed Layer 2-adjacent to the wireless LAN controller (WLC).

Out-of-Band Requirements

OOB implementation of Cisco NAC Appliance requires the access switches and WLCs to be supported by the NAC Appliance software for the NAC Manager to make the necessary changes to the switch ports and WLCs during the authentication, assessment, and remediation process. If access switches are to be used that are not supported, the NAC Solution must be deployed in in-band mode.

To obtain the latest list of supported devices, see the latest version of the *Cisco NAC Appliance-Clean Access Manager Installation and Administration Guide* at the following URL: http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/47cam-book.html.

Layer 2 and Layer 3 Out-of-Band

The recommended deployment option for the Community College reference design is an OOB design. This provides the highest possible performance and scalability for traffic that has completed the authentication, posture assessment, and remediation stages of NAC. For wireless clients, a Layer 2 OOB solution should be deployed and for wired users, a Layer 2 OOB or Layer 3 OOB solution can be deployed, depending on the topology of your network.

NAC Deployment in the Community College Reference Design

Within the Community College reference design, a NAC Appliance solution is deployed at each of the site types; main campus, remote large campus, remote medium campus, and remote small campus. A centralized CAM is deployed at the main campus and is deployed within the data center at that site. A CAS is deployed at each of the campus sites (main and remote sites) and is connected within the service block connecting to the core switches at each of the sites.

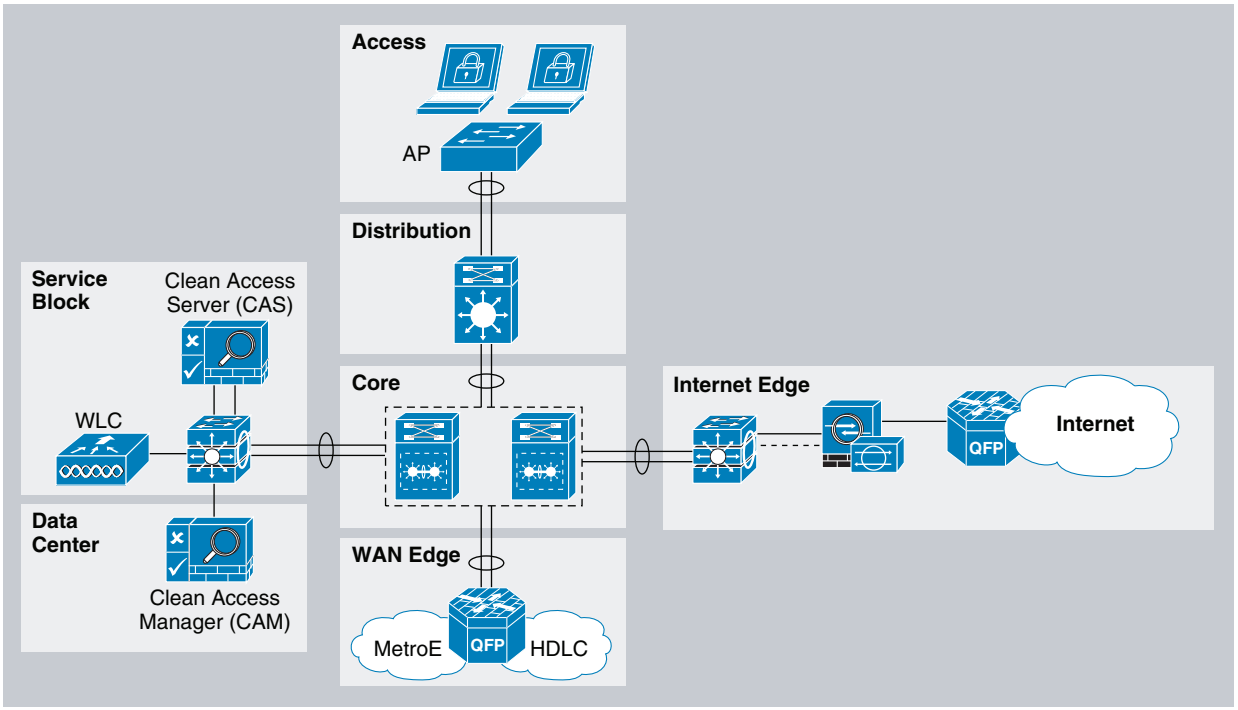
The Community College reference design provides host network connectivity using wired and wireless technologies. As such, the NAC Appliance solution must provide a solution for both connectivity options. For wireless clients, a Layer 2 OOB NAC solution is deployed, and for wired clients, a Layer 2 OOB or a Layer 3 OOB NAC solution may be deployed.

NAC Deployment for Wireless Clients

To provide network access control for wireless clients within the Community College reference design, the recommended design is the virtual gateway (bridge mode) and central deployment OOB solution. In this design, the NAC server must be placed Layer 2-adjacent to the WLC. In the Community College reference design, the WLCs are centrally deployed at each campus and are implemented in the service block off the core switches, as detailed in Chapter 5, "Community College Mobility Design Considerations."

Therefore, the NAC server must also be implemented in the service block. The NAC Manager is implemented in the data center block, as shown in Figure 6-19.

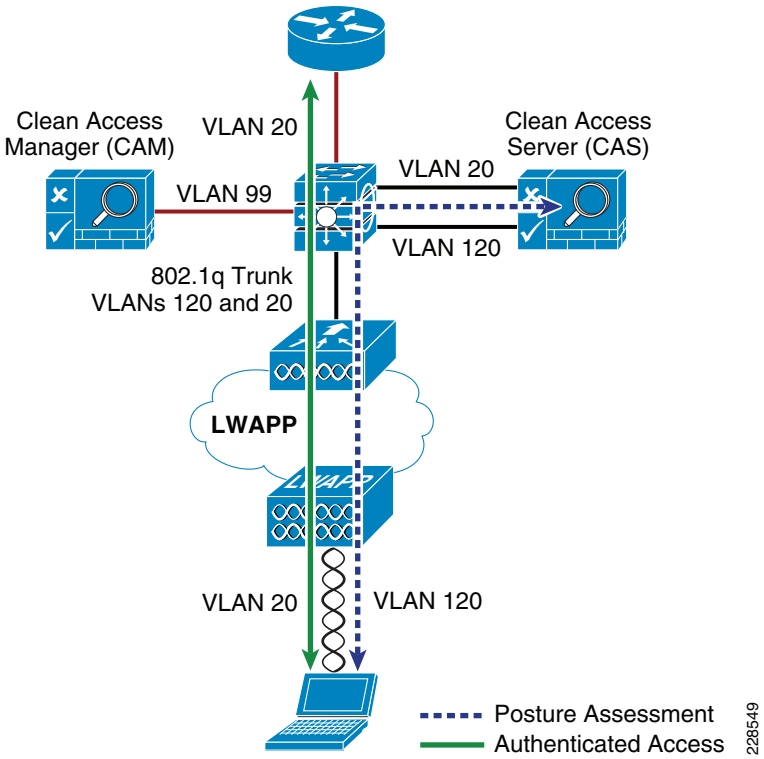
Figure 6-19 NAC OOB Deployment for Wireless Clients



The WLC connects to the service block switch using a trunk port carrying the unauthenticated quarantine VLAN and authenticated access VLAN (VLAN 20 and 120). On the switch, the quarantine VLAN is trunked to the untrusted interface on the NAC server (CAS), and the access VLAN is trunked directly to the Layer 3 switch interface. Traffic that reaches the quarantine VLAN on the CAS is mapped to the access VLAN based on a static mapping configuration within the CAS.

When a wireless client associates to the WLC, it initially maps the WLAN/SSID to the quarantine VLAN interface and the client traffic flows in the quarantine VLAN (VLAN 120), which is trunked to the CAS untrusted interface. When NAC authentication, posture assessment, and remediation stages are complete and the user is certified, the NAC Manager sends an SNMP set message to the WLC that updates the VLAN ID from the quarantine VLAN to the access VLAN. After this occurs, the traffic then bypasses the NAC server and goes directly to the network. (See Figure 6-20.)

Figure 6-20 Wireless NAC OOB Traffic Flow



When implementing the NAC OOB wireless solution, Cisco also recommends enabling RADIUS single sign-on (SSO), which is an option that does not require user intervention and is relatively easy to implement. This option makes use of the VPN SSO capability of the NAC solution, coupled with the Clean Access Agent software that runs on the client PC. VPN SSO uses RADIUS accounting records to notify the NAC Appliance about authenticated remote access users that connect to the network. In the same way, this feature can be used in conjunction with the WLAN controller to automatically inform the NAC server about authenticated wireless clients that connect to the network.

The most transparent method to facilitate wireless user authentication is to enable VPN SSO authentication on the NAC server and configure the WLCs to forward RADIUS accounting to the NAC server. In the event that accounting records need to be forwarded to a RADIUS server upstream in the network, the NAC server can be configured to forward the accounting packet to the RADIUS server.

Note If VPN SSO authentication is enabled without the Clean Access Agent installed on the client PC, users are still automatically authenticated. However, they are not automatically connected through the NAC Appliance until their web browser is opened and a connection attempt is made. In this case, when users open their web browser, they are momentarily redirected (without a logon prompt) within the agentless phase. When the SSO process is complete, they are connected to their originally requested URL.

For more information on deploying NAC OOB for wireless environments, see the *NAC Out-Of-Band (OOB) Wireless Configuration Example* at the following URL: http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml.

NAC Deployment for Wired Clients

For wired clients, the Community College reference design also uses a central OOB NAC deployment with a NAC server implemented at each of the campus sites deployed in the service block off the core switch. Depending on the type of network topology deployed, a Layer 3 OOB or Layer 2 OOB solution can be deployed. If the Layer 2 OOB solution is used, the same NAC server can be leveraged for both wired and wireless clients. However, if the Layer 3 OOB solution is deployed, separate NAC servers must be deployed for wired and wireless users.

Layer 3 Out-of-Band Deployment

Layer 3 (L3) OOB is best suited for routed access designs and has rapidly become one of the most popular deployment methodologies for NAC. By deploying NAC in an L3 OOB methodology, a single NAC Appliance can scale to accommodate more users. This deployment also allows NAC Appliances to be centrally located rather than distributed across the campus or organization. Thus, L3 OOB deployments are much more cost-effective, both from a capital and operational expense standpoint.

For the main, large, and medium remote campus locations, an L3 OOB NAC deployment is recommended, given the 3-tier hierarchical design. In the L3 OOB NAC solution, when a user connects to the access switch before being certified by the NAC server, the user is placed in the authentication VLAN (also called “dirty” 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. After users are certified by the NAC server, they are placed in the authenticated access VLAN, where their traffic is switched normally through the network and bypasses the NAC server.

The following are three widely deployed techniques for redirecting client traffic from the dirty VLAN to the NAC server for authentication, posture assessment, and remediation purposes:

- Access control lists—Use ACLs on the edge access switches to allow traffic from the unauthenticated VLAN only to the NAC server untrusted interface and specific infrastructure resources needed to get on the network for authentication purposes such as DHCP, DNS, and remediation servers. All other traffic from the dirty VLAN must be blocked.
- VRFs/GRE/MPLS—Use VRFs to route unauthenticated traffic to the CAS. Traffic policies configured on the NAC server (CAS) are used for enforcement on the dirty network. This approach has two sub-approaches. In the first approach, VRFs are pervasive throughout the infrastructure, in which case all Layer 3 devices participate in the tag switching. The second approach uses VRF-Lite and GRE tunnels to tunnel the VRFs through the Layer 3 devices that do not understand the tag switching. The benefit to the second approach is that minimal configuration changes are required to your core infrastructure. For more information on this approach, see the following URL: http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a3a8a7.shtml.
- Policy-based routing—Use PBR to redirect all traffic in the dirty VLAN to the NAC server. PBR needs to be configured on every Layer 3 hop between the dirty VLAN and the NAC server to ensure that traffic is appropriately redirected.

The most common approach used for isolating the dirty VLAN traffic is to use ACLs. The ACLs on the Layer 3 edge access switches act as the enforcement point to ensure segregation between the “clean” and “dirty” networks. When clients first attach to the network, they are placed in a quarantine or dirty VLAN on the access switches. ACLs should be applied on the SVIs for the dirty VLAN. This ACL should block all access from the dirty VLAN going to the internal networks and allow traffic only to the untrusted interface on the NAC server, the needed remediation servers, and a few infrastructure devices needed for network access such as the DNS, DHCP, and Active Directory servers.

The clients need to communicate with the NAC server untrusted interface for the certification process. The ACLs on the access switches act as the enforcement point for path isolation for the dirty VLAN traffic. Methods for getting the dirty VLAN traffic to the untrusted interface vary, depending on whether the NAC Client Agent is used.

When the NAC agent is used, the NAC Agent communicates with the NAC server untrusted interface to initiate the login process. The NAC Agent tries to discover the NAC server based on the known discovery host value. The discovery host value in the NAC Agent points to the untrusted interface of the NAC server. In the Community College reference design, the NAC Agent can be used for managed PCs such as administrative staff and faculty.

Web login is typically required for student login sessions because student laptops are typically not managed. With the ACL isolation technique, the NAC server untrusted interface is not directly in the path of the data traffic; therefore, the user is not automatically redirected to the login page when first opening the browser. The following two options can enable the end host to get the login page:

- Option 1—Have a guest login URL known to the users (for example, *guest.nac.local*). In this case, the guest must open a browser and manually enter this URL, which redirects them to the login page.
- Option 2—Create a dummy DNS server for the unauthenticated user subnet. This dummy DNS server resolves every URL to the untrusted interface of the NAC server. When guests open a browser, regardless of which URL they are trying to reach, they are redirected to the login page. When users are then moved to the respective Role/VLAN, they get a new DNS address assignment when performing IP release/renew on a successful login.

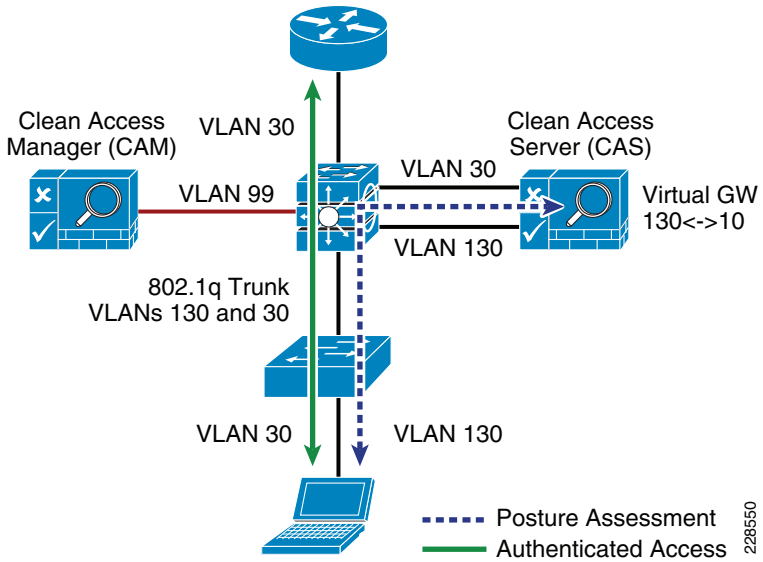
Layer 2 Out-of-Band Deployment

For the small remote campus locations, a two-tier, collapsed core/distribution LAN design is recommended, as explained in Chapter 3, "Community College LAN Design Considerations."

In a collapsed core/distribution design, the CAS should be deployed in the services block connected to the core/distribution switch. In this simple topology, a Layer 2 Out-of-Band (L2 OOB) NAC deployment can be used.

In the L2 OOB NAC design for the small remote campus, the unauthenticated and authenticated VLANs on the access switch (VLANs 30 and 130) are extended to the core/distribution switch using a trunk connection, as shown in Figure 6-21.

Figure 6-21 Layer 2 OOB Topology



When a client device initially connects to the access switch before authentication, it is placed in the unauthenticated VLAN (VLAN 130), which connects the client directly to the untrusted interface of the CAS. The CAS maps VLAN 130 to the VLAN 30 trusted interface, allowing the client to obtain an IP address that belongs on VLAN 30. After the client is authenticated and passes the posture assessment, the access switch is instructed, via SNMP from the CAM, to change the client VLAN to the authenticated VLAN (VLAN 30), where the traffic now bypasses the CAS to access the rest of the network. Although the client has changed Layer 2 VLANs, its Layer 3 network connections are unchanged.

NAC Availability Considerations

Both the CAS and CAM are highly involved in client network access. Consideration must be given to the impact on clients if either a CAS or CAM fails or needs to be taken out of service for a period of time.

The CAS is inline with client devices during the authentication, authorization, and posture assessment phases of NAC, and if NAC is deployed in in-band mode, it is inline even after authentication and certification. A CAS outage for inline clients prevents access for all clients. However, if NAC is deployed in OOB mode, a CAS outage does not affect already connected clients but does prevent network access for new clients.

In situations where availability of a CAS is critical, a high availability (HA) CAS solution can be implemented where a pair of CAS servers are installed using a primary CAS, and a secondary in hot standby. For more information, see the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide* at the following URL: http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/461/cas/461cas-book.html.

The CAM is also a critical part of the authentication, authorization, and posture assessment phases of NAC. Although it does not pass client traffic, the impact of its availability needs to be considered in the network design as well. Like the CAS, the CAM has an HA solution that provides for a primary server and a hot standby secondary server. In addition, each CAS may be configured with a fallback option that defines how it manages client traffic in a situation where the CAM is unavailable.

The use of the CAM and CAS HA features depends on the requirements of the community college. However, CAS fallback should always be configured to ensure that critical network services are available, even during a network outage.

Endpoint Protection

Servers, desktop computers, laptops, printers, and IP phones are examples of the diverse network endpoints found in community college environments. Properly securing the endpoints requires not only adoption of the appropriate technical controls but also end-user awareness. The community college security strategy must include security awareness campaigns and programs. Students, staff, and faculty must be continuously educated in current threats, Internet-use best practices, and the security measures needed for keeping endpoints up-to-date with the latest updates, patches, and fixes.

The Community College reference design implements a range of security controls designed to protect the endpoints, which include Cisco host-based IPS, network-based IPS, and web and E-mail traffic security.

For host-based IPS, the Community College reference design leverages the Cisco Security Agent on managed end-user workstations and servers. Cisco Security Agent uses behavior-based security to take a proactive approach to preventing malicious activity on the hosts. When an application attempts an operation on the host, Cisco Security Agent checks the operation against the security policy of the application, and makes a real-time decision to allow or deny the operation along with determining whether to log the operation request. Security policies are assigned by IT or security administrators individually, per department, or organization-wide.

Cisco Security Agents are centrally managed with the Cisco Security Agent Management Center, which is placed in a secure segment in the data center. Cisco Security Agent Management Center also provides centralized reporting and global correlation.

Community College Mission Relevancy

The service fabric provides the network foundation for the Community College reference design. The network service fabric is a collection of products, features, and technologies that provide a robust routing and switching foundation on which all solutions and services are built to solve the business challenges facing community colleges. These business challenges include the following:

- Virtual learning environments
- Secure connected classrooms
- Safety and security
- Operational efficiencies

The previous sections of this chapter focused on the specific design considerations for securing the community college service fabric network. This section discusses how these security design considerations relate to these business challenges.

Virtual Learning Environments

One of the key challenges that face community colleges is extending their learning environments beyond brick and mortar campuses to allow online/distance learning, professor collaboration, and anytime, anywhere access for students to obtain course materials. Maintaining a secure virtual learning environment is critical for community colleges. The community college security design helps establish the foundation for providing a secure virtual learning environment in the following areas:

- *Secure remote access*

  - Allows community colleges to extend their network to anyone, anytime, anywhere by providing a secure client-based or web-based remote access solution.
  - Provides granular and encrypted access to learning resources based on user or security requirements.
- *Internet perimeter*—Protects and controls access to the community college network infrastructure from remote students, faculty, staff, and guest professors by properly securing the Internet perimeter by using firewalls, intrusion prevention systems, and a DMZ to protect against unauthorized access and malicious attacks.
- *Securing Video Portal*—Secures the network and data center to prevent misdirected students or malicious intruders from hacking into restricted servers or issuing attacks on the video portal learning infrastructure.
- *Network telemetry and monitoring*—Provides visibility into attacks or malicious activity on the network by monitoring the network using NetFlow, Syslog, and SNMP.

Secure Connected Classrooms

Although providing connectivity to students while attending class is the foundation of twenty-first century learning, this poses many problems for community colleges. They must ensure that the person accessing the network should be allowed on the network, and that the computer accessing the network is free from viruses and other malware that might adversely affect the network and other users. In addition, while connectivity is provided, steps should be taken to prevent unauthorized access to restricted resources and protect against inadvertent or deliberate network attacks. The security design within the community college service fabric helps to address these challenges in the following ways:

- *Network access control*—Implementing role-based network access controls for wired, wireless, and remote users and devices to help reduce the potential loss of sensitive information by enabling administrators to verify a user or device identity, privilege level, and security policy compliance before granting access to the network.
- *Access layer security*—Enabling Cisco CISF on the access layer switches to protect the access layer infrastructure and users from spoofing, man-in-the-middle, DoS and other network-based attacks. CISF includes features such as Port Security, DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard.
- *Web security*—Deploying a Cisco IronPort Web Security Appliance (WSA) to block access to sites with content that may be harmful or inappropriate, and to protect community colleges from web-based malware or spyware.
- *Network and data security*—Securing the network and data center to prevent misdirected students or malicious intruders from hacking into restricted servers or issuing attacks on the network infrastructure.

Safety and Security

Providing a safe and secure environment is a top responsibility for community college administrators and community leaders. Without adequate protection, schools may be threatened by harmful or inappropriate content that can put the well-being of the students at risk, the theft of student records and private data, the loss of school network and service availability, as well as the abuse of internal applications and network resources. A safe community college is one that successfully uses the right

tools to ensure the safety and security of students, staff, and faculty, and guarantees an immediate and effective response to security and safety incidents. The most effective strategy is one that combines physical and network controls, not in isolation but rather in collaboration and with a common purpose.

Because many of the physical security components such as video surveillance and unified communication services rely on the IP infrastructure, it is critical to ensure the availability and integrity of this infrastructure. The security design within the Community College reference design helps to ensure the availability and the integrity of the network infrastructure that the physical security components rely on by focusing on the following key areas:

- *Network Foundation Protection (NFP)*—Ensuring the availability and integrity of the network infrastructure, protecting the control and management planes.
- *Internet perimeter protection*
  - Ensuring safe connectivity to the Internet, Internet2, and NLR networks and protecting internal resources and users from malware, viruses, and other malicious software.
  - Protecting students, staff, and faculty from harmful content.
  - Enforcing E-mail and web browsing policies.
- *Data center protection*—Ensuring the availability and integrity of centralized applications and systems. Protecting the confidentiality and privacy of student, staff, and faculty records.
- *Network access security and control*
  - Securing the access edges.
  - Enforcing authentication and role-based access for students, staff, and faculty residing at the main and remote campuses.
  - Ensuring systems are up-to-date and in compliance with the community colleges network security policies.
- *Network endpoint protection*
  - Protecting servers and school-controlled systems (computer labs, school-provided laptops, and so on) from viruses, malware, botnets, and other malicious software.
  - Enforcing E-mail and web browsing policies for staff and faculty.

Operational Efficiencies

Community colleges are faced with the daunting task of doing more with less, facing explosive growth as budgets and resources are reduced. The Community College reference design leverages the network as a platform to deliver expanded educational services and data center optimizations to create operational efficiencies to reduce costs and capitalize on under-used network capacity. The network as a platform goes beyond merely consolidating voice, video, and data services on a single converged network; rather it consolidates all IP-based services to use the network (wired or wireless) to extend cost reduction, improve utilization on under-used networks, and add flexibility to community colleges through business process improvements.

With these critical services relying heavily on the network infrastructure, it is imperative that the IP infrastructure remains operational at all times, and it is critical that security be implemented throughout the network infrastructure to ensure the availability and the integrity of the network.

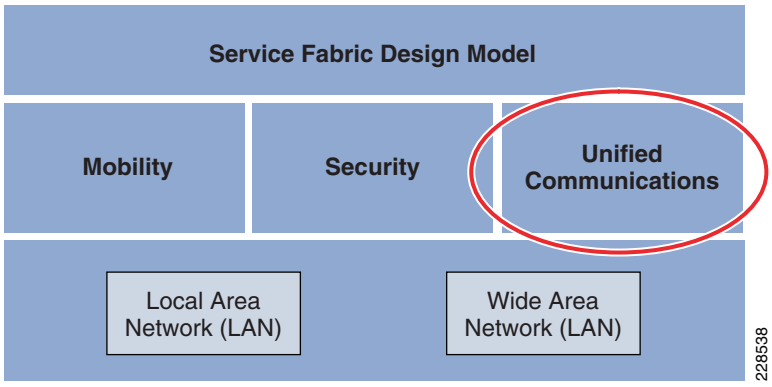
CHAPTER 7

Community College Unified Communications Design Considerations

Unified Communications Design

As mentioned earlier in this document, the service fabric is made up of 4 distinct components: local and wide area network (LAN/WAN), security, mobility, and unified communications. This chapter focuses on the unified communications area within the service fabric. See Figure 7-1.

Figure 7-1 Unified Communication Design



In today's environment, we observe community college and vocational education campuses moving towards a model that makes it convenient for the students to attend by not traveling to a central campus. This requires many smaller locations that still require the network facilities and voice communications features of the main campus. Instructors in this environment may teach classes at several locations within the same day or week. If these instructors had to contend with different phone systems at each location with no unified dial plan, the frustration level would be high and missed information would ultimately impact the customer, in this case the students. For this reason, it is important to have a unified communication architecture that allows uniformity in features and dialing as well as providing a high level of availability.

The SRA for CCVE solution is designed with unified communications considerations for the following:

- LAN design
- Call processing
- PSTN trunk sizing
- Dial plan

- High availability

LAN Design

Proper LAN design is critical to the performance of all IP telephony components. Telephony is expected to be always available. In order for this to be accomplished, a well designed LAN with considerations end-to-end QoS is required.

Layer 2 Access

The following are the access layer recommendations:

- Single IP subnet per virtual LAN (VLAN). Typically, a VLAN should not span multiple wiring closet switches; that is, a VLAN should have presence in one and only one access layer switch. Confining a VLAN to a single access layer switch serves to limit the size of the broadcast domain. There is the potential for large numbers of devices within a single VLAN or broadcast domain to generate large amounts of broadcast traffic periodically, which can be problematic.
- Typical access layer switches Power-over-Ethernet (PoE) capable include the stackable Cisco Catalyst 2950, 3500XL, 3550, and 3750, as well as the Cisco 3560 and the larger, higher-density Catalyst 4000 and 6000 switches fixed configuration Cisco Catalyst 2960-E, 3560-E and 3750-E series switches. Cisco Catalyst modular switching platform like 4500-E or 6500-E Series switches can be deployed in large size access-layer network domain that requires higher port-density and control-plane redundancy for resilient network services to critical endpoints (i.e., Cisco TelePresence, fixed configuration Cisco Catalyst 2960-E, 3560-E and 3750-E Series switches. Cisco Catalyst modular switching platform like 4500-E or 6500-E Series switches can be deployed in large size access-layer network domain that requires higher port-density and control-plane redundancy for resilient network services to critical end-points (i.e., Cisco TelePresence).

Cisco recommends enabling two VLANs at the access layer: a native VLAN for data traffic and a voice VLAN under Cisco IOS.

Separate voice and data VLANs are recommended for the following reasons:

- Address space conservation and voice device protection from external networks private addressing of phones on the voice or auxiliary VLAN ensures address conservation and ensures that phones are not accessible directly via public networks. PCs and servers are typically addressed with publicly routed subnet addresses; however, voice endpoints should be addressed using RFC 1918 private subnet addresses.
- QoS trust boundary extension to voice devices QoS trust boundaries can be extended to voice devices without extending these trust boundaries and, in turn, QoS features to PCs and other data devices.
- Protection from malicious network attacks VLAN access control, 802.1Q, and 802.1p tagging can provide protection for voice devices from malicious internal and external network attacks such as worms, denial-of-service (DoS) attacks, and attempts by data devices to gain access to priority queues via packet tagging.
- Ease of management and configuration. Separate VLANs for voice and data devices at the access layer provide ease of management and simplified QoS configuration.

To provide high-quality voice and to take advantage of the full voice feature set, access-layer switches should provide support for the following:

- 802.1Q trunking and 802.1p for proper treatment of Layer-2 CoS packet marking on ports with phones connected.

- Multiple egress queues to provide priority queuing of RTP voice packet streams.
- The ability to classify or reclassify traffic and establish a network trust boundary.
- Inline power capability (Although inline power capability is not mandatory, it is highly recommended for the access layer switches.)
- Layer 3 awareness and the ability to implement QoS access control lists. These features are required if you are using certain IP telephony endpoints, such as a PC running a softphone application, that cannot benefit from an extended trust boundary.)

Spanning Tree Protocol (STP)

To minimize convergence times and maximize fault tolerance at Layer 2, enable the following STP features:

- *PortFast*—Enable PortFast on all access ports. The phones, PCs, or servers connected to these ports do not forward bridge protocol data units (BPDUs) that could affect STP operation. PortFast ensures that the phone or PC, when connected to the port, is able to begin receiving and transmitting traffic immediately without having to wait for STP to converge.
- *Root guard or BPDU guard*—Enable root guard or BPDU guard on all access ports to prevent the introduction of a rogue switch that might attempt to become the Spanning Tree root, thereby causing STP re-convergence events and potentially interrupting network traffic flows. Ports that are set to **errdisable** state by BPDU guard must either be re-enabled manually or the switch must be configured to re-enable ports automatically from the errdisable state after a configured period of time.
- *UniDirectional Link Detection (UDLD)*—Enable this feature to reduce convergence and downtime on the network when link failures or misbehaviors occur, thus ensuring minimal interruption of network service. UDLD detects and takes out-of-service links where traffic is flowing in only one direction. This feature prevents defective links from being mistakenly considered as part of the network topology by the spanning tree and routing protocols.

Note With the introduction of RSTP 802.1w, features such as PortFast and UplinkFast are not required because these mechanisms are built into this standard. If RSTP has been enabled on the Catalyst switch, these commands are not necessary.

Routed Access

For designs requiring simplified configuration, common end-to-end troubleshooting tools, and the fastest convergence, a distribution block design using Layer-3 switching in the access layer (routed access) in combination with Layer-3 switching at the distribution layer provides the fastest restoration of voice and data traffic flows.

In both the traditional Layer 2 and the Layer 3 routed access designs, each access switch is configured with unique voice and data VLANs. In the Layer 3 design, the default gateway and root bridge for these VLANs is simply moved from the distribution switch to the access switch. Addressing for all end stations and for the default gateway remains the same. VLAN and specific port configurations remain unchanged on the access switch. Router interface configuration, access lists, "**ip helper**," and any other configuration for each VLAN remain identical but are configured on the VLAN Switched Virtual Interface (SVI) defined on the access switch instead of on the distribution switches. There are several notable configuration changes associated with the move of the Layer 3 interface down to the access

switch. It is no longer necessary to configure an HSRP or GLBP virtual gateway address as the "router" interfaces because all the VLANs are now local. Similarly, with a single multicast router, for each VLAN it is not necessary to perform any of the traditional multicast tuning such as tuning PIM.

query intervals or ensuring that the designated router is synchronized with the active HSRP gateway.

The many potential advantages of using a Layer-3 access design include the following:

- Improved convergence
- Simplified multicast configuration
- Dynamic traffic load balancing
- Single control plane
- Single set of troubleshooting tools (for example, ping and traceroute)

Of these advantages, perhaps the most significant is the improvement in network convergence times possible when using a routed access design configured with EIGRP or OSPF as the routing protocol. Comparing the convergence times for an optimal Layer 2 access design (either with a spanning tree loop or without a loop) against that of the Layer 3 access design, you can obtain a four-fold improvement in convergence times, from 800 to 900 msec for the Layer 2 design to less than 200 msec for the Layer 3 access design.

Call Processing

When considering a design for unified communications, many factors come into play in making an overall call processing decision such as number of sites, number of users, functionality requirements (Call Center, IVR, etc.), network capabilities (WAN), etc.

If a Community College has one large campus that houses the primary data center and many small remote sites then a Centralized Call Processing model with Survivable Remote Site Telephony (SRST) might be the best choice. In this design, the remote sites depend on the primary campus Unified CM components for normal operation. If the WAN fails, the remote sites would resort to their local SRST router for primary call control until the WAN recovers. This model requires less administration since all call control is accomplished within one cluster.

If a very large Community College has multiple large campuses, it might require Distributed Call Processing. Within this model, you will find a Unified CM cluster at each large site for call control. Each cluster would communicate with the other clusters but administration is accomplished on a per-cluster basis. This design does not allow for some features that might be important in a Community College environment such as shared lines across clusters. Extension Mobility is not easily accomplished across clusters as well. In a campus environment Extension Mobility might be a very important feature for those instructors that might teach at multiple locations.

For this document, it is assumed that the main campus and large remote campus each have a data center and several hundred handsets. Instead of administering two clusters, clustering over the IP WAN will be implemented. Each of the smaller sites will then depend on this cluster for primary call control and SRST in case of WAN failure.

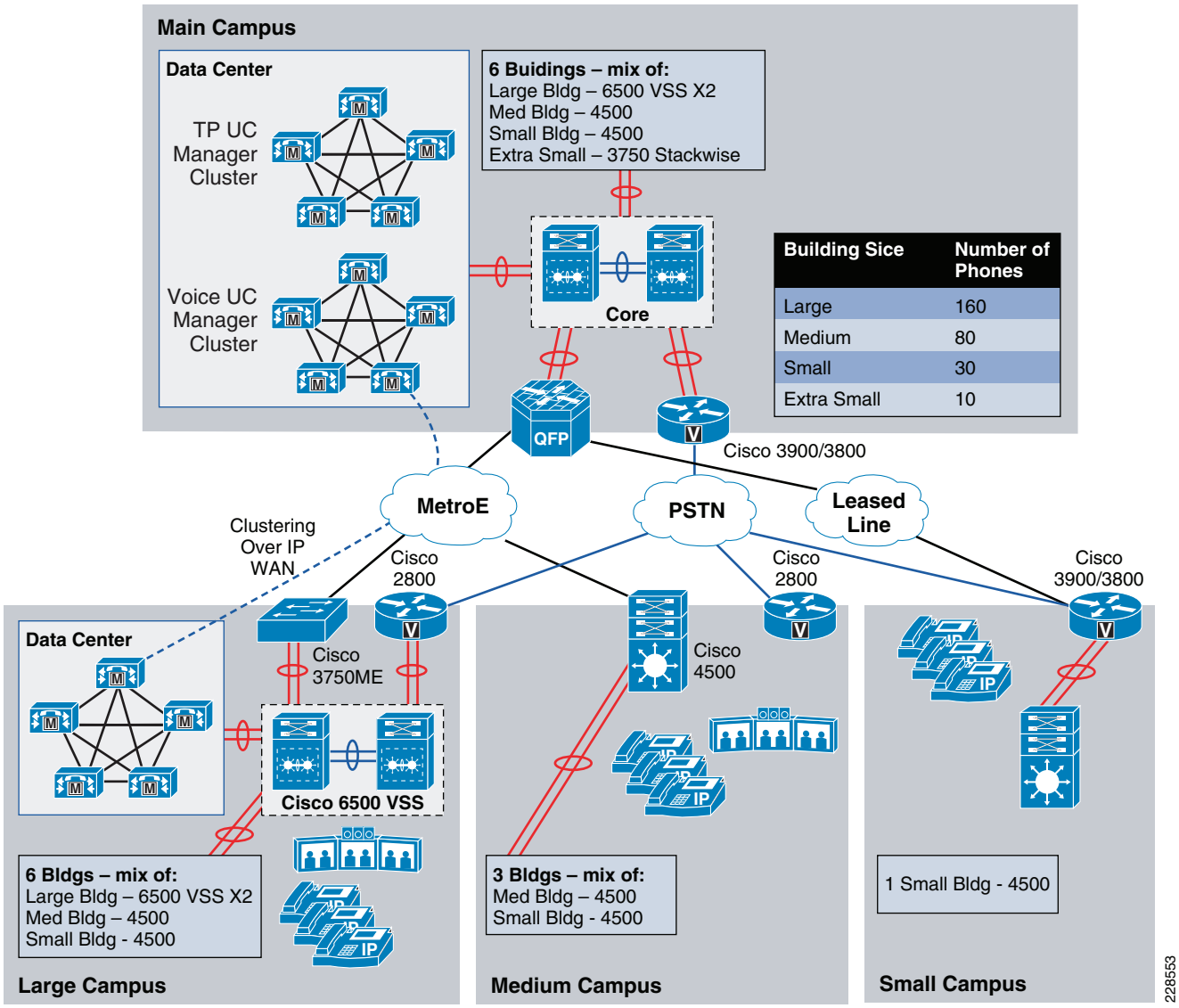
Follow these guidelines and best practices when implementing multisite centralized call processing deployments:

- Minimize delay between Unified CM and remote locations to reduce voice cut-through delays (also known as clipping).
- Configure locations (static or RSVP-enabled) in Unified CM to provide call admission control into and out of remote branches.

- The number of IP phones and line appearances supported in Survivable Remote Site Telephony (SRST) mode at each remote site depends on the branch router platform, the amount of memory installed, and the Cisco IOS release. SRST on a Cisco IOS gateway supports up to 720 phones, while Unified CME running in SRST mode supports 240 phones. (For the latest SRST or Unified CME platform and code specifications, refer to the SRST and Unified CME documentation available at http://www.cisco.com.) Generally speaking, however, the choice of whether to adopt a centralized call processing or distributed call processing approach for a given site depends on a number of factors such as the following:
  - IP WAN bandwidth or delay limitations
  - Criticality of the voice network
  - Feature set needs
  - Scalability
  - Ease of management
  - Cost

In Figure 7-2, each location is indicated with number of phones anticipated.

Figure 7-2 Main Campus



For more information on the different call processing models, refer to the *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager* 7.x at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html

Clustering over the IP WAN

Clustering over the IP WAN Advantages

Clustering over the IP WAN best fits the needs of this Community College design for the following reasons:

- Single point of administration
- Feature transparency
- Shared line appearances (even across locations)

- Extension Mobility
- Unified Dial Plan

In the education vertical this model allows educators to move from campus to campus and retain their phone identity with Extension Mobility. It also allows for features such as shared lines that might not be possible in other deployment models. Clustering over the IP WAN does however have some very strict requirements in regard to bandwidth and latency.

Before providing details on clustering it might be good to have some background on what components exist in a cluster.

In every Communications Manager Cluster there is only one publisher but there can be several subscribers. The publisher server replicates a partial read-only copy of the master database to all other servers in the cluster. Most of the database modifications are done on the publisher. If changes such as administration updates are made in the publisher's master database during a period when another server in the cluster is unreachable, the publisher will replicate the updated database when communications are re-established. Database modifications for user-facing call processing features are made on the subscriber servers to which the IP phones are registered. These features include:

- Call Forward All (CFA)
- Message Waiting Indication (MWI)
- Privacy Enable/Disable
- Do Not Disturb (DND) Enable/Disable
- Extension Mobility Login (EM)
- Hunt Group Logout
- Device Mobility
- CTI Certificate Authority Proxy Function (CAPF) status for end users and application users
- Credential hacking and authentication

Each subscriber replicates these changes to every other server in the cluster. Any other configuration changes cannot be made on the database during the period when the publisher is unreachable or offline.

Most normal operations of the cluster, including the following, will *not* be affected during the period of publisher failure:

- Call processing
- Failover
- Registration of previously configured devices

Other services or applications might also be affected, and their ability to function without the publisher should be verified when deployed.

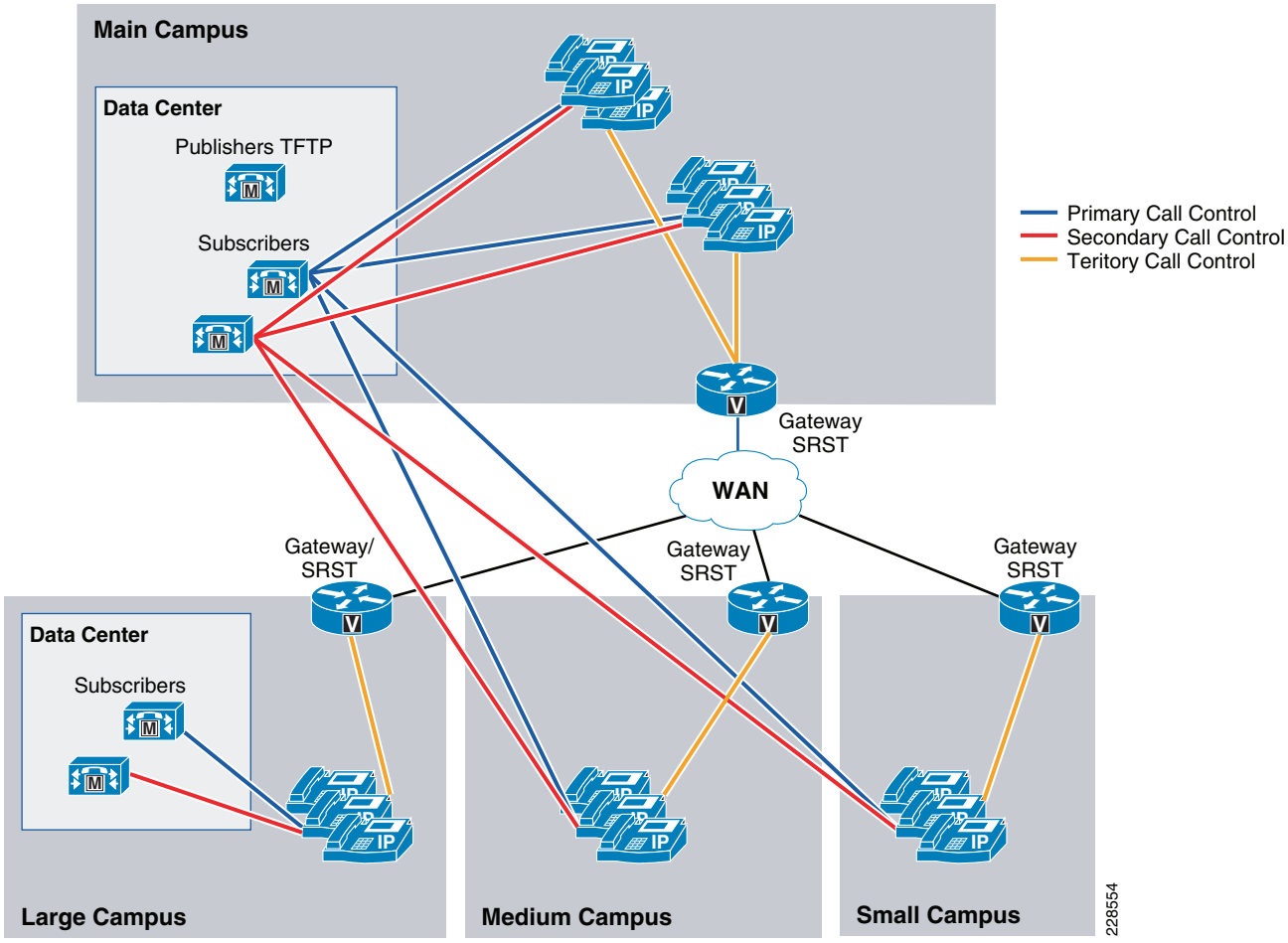
Within the clustering over the IP WAN deployment scenario there are two possible failover models:

- *Option 1*—Local Failover Deployment Model
  - This deployment scenario provides the highest level of redundancy since each site that contains cluster servers houses a primary subscriber/s and a backup subscriber. Users within the site would fail from their assigned subscriber at the site to the backup subscriber at the same site. If by chance all subscribers at the site fail SRST is the final failover call control target.
- *Option 2*—Remote Failover Deployment Model

– In this model, each site that contains a cluster server does not contain a backup server target. The backup servers might be within the primary campus for all users or users might not have a backup target at all and uses SRST during server failures. If a backup server is used at primary campus then users would register with that server over the WAN. This additional traffic must be considered when designing for failover.

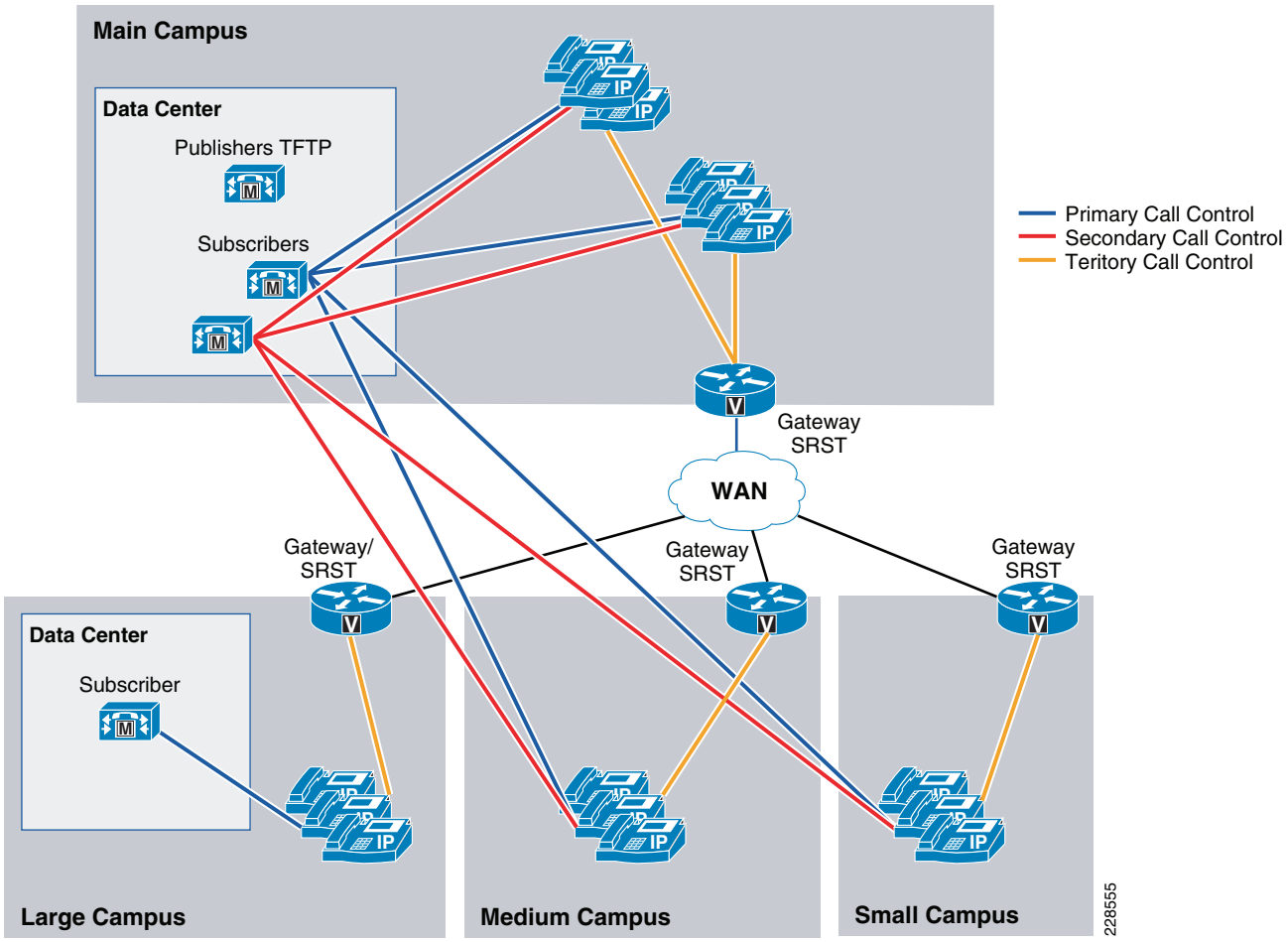
In Figure 7-3, option 1 is depicted with a backup server at the main campus and also at the remote large campus.

Figure 7-3 Option 1—Local Failover Deployment Model



In Figure 7-4, Option 2 is depicted with a backup server at the main campus only. Users at the remote large campus would failover to the main campus subscriber over the WAN and then to their local SRST target.

Figure 7-4 Option 2—Remote Failover Deployment Model



WAN Requirements

For clustering over the WAN to be successful, you must carefully plan, design, and implement various characteristics of the WAN itself. The Intra-Cluster Communication Signaling (ICCS) between Unified CM servers consists of many traffic types. The ICCS traffic types are classified as either priority or best-effort. Priority ICCS traffic is marked with IP Precedence 3 (DSCP 24 or PHB CS3). Best-effort ICCS traffic is marked with IP Precedence 0 (DSCP 0 or PHB BE).

ICCS consists of the following:

- *Database traffic*
  - Configuration information
- *Firewall management traffic*
  - Used to authenticate the subscribers to the publisher to access the publisher's database
- *ICCS real-time traffic*
  - Signaling, call admission control, and info about calls as they are initiated or completed
  - Uses TCP connection to all servers with Cisco CallManager Service-enabled

  - Full mesh between all servers (maximum of 8 servers in a cluster running CM Service so there may be up to seven connections on each server)
- *CTI Manager*
  - Used for CTI devices involved in calls or for controlling or monitoring other third-party devices

In order for the ICCS traffic to traverse the WAN there are very specific WAN requirements:

- *Delay*
  - Maximum one-way delay between any 2 servers can not exceed 40 msec (or 80msec round-trip). If clustering over the WAN is being used between data centers, any additional security that is applied both within and between those data centers has to fit within the maximum round-trip time that is allowed between nodes in a cluster.
- *Jitter*
  - Jitter for the IP Precedence 3 ICCS traffic must be minimized using Quality of Service (QoS)
- *Packet loss and errors*
  - The network should be engineered to provide sufficient prioritized bandwidth for all ICCS traffic, especially the priority ICCS traffic. Standard QoS mechanisms must be implemented to avoid congestion and packet loss. If packets are lost due to line errors or other "real-world" conditions, the ICCS packet will be retransmitted because it uses the TCP protocol for reliable transmission. The retransmission might result in a call being delayed during setup, disconnect (teardown), or other supplementary services during the call. Some packet loss conditions could result in a lost call, but this scenario should be no more likely than errors occurring on a T1 or E1, which affect calls via a trunk to the PSTN/ISDN.
- *Bandwidth*
  - Provision the correct amount of bandwidth between each server for the expected call volume, type of devices, and number of devices. This bandwidth is in addition to any other bandwidth for other applications sharing the network, including voice and video traffic between the sites. The bandwidth provisioned must have QoS enabled to provide the prioritization and scheduling for the different classes of traffic.
  - A minimum of 1.544 Mbps (T1) is required for ICCS for 10,000 busy hour call attempts (BHCA) between the sites that are clustered over the WAN. The *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager* 7.x contains the calculations for establishing how much bandwidth is required.
  - In addition to the bandwidth required for Intra-Cluster Communication Signaling (ICCS) traffic, a minimum of 1.544 Mbps (T1) bandwidth is required for database and other inter-server traffic for every subscriber server remote to the publisher.
  - When directory numbers are shared between sites that are clustered over the WAN, additional bandwidth must be reserved.
- *QoS*
  - The network infrastructure relies on QoS engineering to provide consistent and predictable end-to-end levels of service for traffic. Neither QoS nor bandwidth alone is the solution; rather, QoS-enabled bandwidth must be engineered into the network infrastructure.

Intra-Cluster Communications

Intra-cluster communications represents all traffic between the servers in a cluster. The real-time protocol called Intra-Cluster Communication Signaling (ICCS) provides the communications with the Cisco CallManager Service process.

The intra-cluster traffic between the servers consists of the following:

- Database traffic from the IBM Informix Dynamic Server (IDS) database that provides the main configuration information. The IDS traffic may be reprioritized in line with Cisco QoS recommendations to a higher priority data service (for example, IP Precedence 1, if required by the particular business needs).
- Firewall management traffic, which is used to authenticate the subscribers to the publisher to access the publisher's database. The management traffic flows between all servers in a cluster. The management traffic may be prioritized in line with Cisco QoS recommendations to a higher priority data service (for example, IP Precedence 1, if required by the particular business needs).
- ICCS real-time traffic, which consists of signaling, call admission control, and other information regarding calls as they are initiated and completed. ICCS uses a Transmission Control Protocol (TCP) connection between all servers that have the Cisco CallManager Service-enabled. The connections are a full mesh between these servers. Because only eight servers may have the Cisco CallManager Service enabled in a cluster, there may be up to seven connections on each server. This traffic is priority ICCS traffic and is marked dependant on release and service parameter configuration.
- CTI Manager real-time traffic is used for CTI devices involved in calls or for controlling or monitoring other third-party devices on the Unified CM servers. This traffic is marked as priority ICCS traffic and exists between the Unified CM server with the CTI Manager and the Unified CM server with the CTI device.

For detailed information on various types of traffic between Unified CM servers, refer to the port usage document at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/7_0/CCM_7.0PortList.pdf.

Gateways

In this design, gateways will be configured at every location. If a location has cluster servers within that location, gateways at that location will register with the local servers via device pools. Partitions and Calling Search Spaces will also be configured so local gateways are the first choice for PSTN calls. In some cases, overflow to other location gateways is allowed but WAN bandwidth must be considered so as to not oversubscribe it. Another consideration for overflow is in the event of local gateway failure causing all PSTN calls to overflow to another locations gateway. This could suddenly oversubscribe not only the WAN but the remote locations PSTN call handling ability (number of available trunks). Having PSTN access at every location is necessary for emergency services and also as a means of making and receiving calls when in SRST mode. Every location will also support SRST as a last resort call control mechanism.

PSTN Trunk Sizing

Calculating Traffic

In voice communications, it is important to understand how much traffic is being carried or is expected to be carried by the public switched telephone network (PSTN) circuits. This traffic is measured in Erlangs. 1 Erlang can be considered as 1 hour of traffic. As an example, a single call lasting 1 hour would be 1 Erlang of carried traffic.

There are several ways to calculate how much traffic is currently being carried over a trunk group. A traffic study on the existing telephony system or a traffic study from the carrier. In a new installation, this is hard to project. The following subsections describe this.

Traffic in an Existing Location

Existing Phone System Traffic Reports

If a location already has a telephony system installed, traffic reports can usually be run from the perspective of that telephony system. In general terms, you are looking for the worst case scenario: busy day and busy hour. These traffic reports come in many varieties and measure in many different ways. The goal is to calculate how many seconds of use per phone user is consumed during the busy hour. Some reports break traffic into the following three parts:

- In (inbound from an external trunk)
- Out (outbound to an external trunk)
- Station to station (calls between two phones on the same system).

In calculating trunk traffic, we are not concerned with station to station call traffic so it should be subtracted from the total. Station to station traffic might be a consideration for calls over the WAN to another station but not for local PSTN traffic.

Typically, traffic from the station perspective is measured in Centum Call Seconds (CCS). A CCS is equal to 100 seconds so 400 seconds would be expressed as four CCS. There are 3600 seconds (36 CCS) in an hour so the most traffic a user could theoretically consume is 36 CCS. In a call center, each user that will be on-line is usually considered to be able to use trunk facilities for a full 36 CCS.

For example, a report that might indicate that the average phone usage (In + Out) per user is 400 seconds during the busy hour (09:00 to 10:00). In telephony, this would be called 4 Centum Call Seconds (4 CCS) per user.

After deriving the CCS/user, the total trunk traffic can be calculated. Trunk traffic is usually measured in Erlangs or hours of traffic. If a location has 125 users at 4 CCS/user, then the total busy hour traffic for that location would be 500 CCS or 50,000 seconds. 50,000/3600 (seconds in an hour) = 13.9 Erlangs (hours) of traffic. Another way to calculate is 500 CCS/36 CCS (36 CCS in an hour) = 13.9 Erlangs.

After calculating the total busy hour traffic (13.9 Erlangs), it is now possible to estimate how many trunks are required. Before doing this, a couple decisions need to be made. The calculators that suggest the number of trunks required will ask for a Grade-of-Service (GoS) or level of acceptable blockage. In most cases, a GoS of .01 (1 call in 100 will be blocked) is used. The other question that usually asked is what calculation method should be used. The following are the typical methods:

- Erlang B
  - Unsuccessful calls are blocked (typical non-call center)
- Erlang C
  - Unsuccessful calls are queued (call center based)

There are several other methods however, these are the most widely used.

To continue the example, in this instance we will be using 13.9 (round up to 14 Erlangs), a blockage factor (GoS) of .01, and the Erlang B calculation method. If these values are used in one of the many on-line traffic calculators, it will provide a value of 23 lines (trunks).

One on-line calculator can be found at the following URL: http://www.erlang.com/calculator/erlb/

Carrier Traffic Reports

If reports are not available from an existing telephony system, the carrier can usually provide this information. They do not usually store this data, so a traffic report is usually requested for a specific date and time. In some cases, the carrier will provide a “Peg” report that is only a count of calls without duration. This is not very helpful unless you have some other way of deriving the average call length. If

users are complaining of not being able to make an external call or customers are complaining of getting a busy on inbound calls, these reports will also usually show call blockage patterns so more trunks can be added.

After receiving the data from the carrier, a busy hour calculation can be made to see what the total traffic is and the same methods as above can be used to arrive at the total number of trunks used. In many cases companies are over-trunked so this can be used to reduce the financial burden associated with too many trunks.

Traffic in a New Location

If traffic reports are available for existing locations, this can be used to project the traffic for a new location. If no traffic is available some assumptions can be made. The rule of thumb is that most hospitals and universities are in the 3 CCS to 4 CCS/user range and most Enterprise customers in the 5 CCS-7 CCS range. Hospitals and universities are usually on the lower end because they have a large number of rarely used phones (patient rooms, classrooms, etc.). The typical Enterprise has fewer phones, therefore the traffic per phone goes up. The nature of the business can also drive the average CCS/user higher as well. It is always better to over-trunk, monitor and fine tune than to under-trunk and cause employee and customer frustration.

Dial Plan Considerations

In many cases, the dial plan is conceived when a system is very small and there is no expectation that multiple locations will be added in the future. For a community college that might be in the initial phases of designing a system, it would be very important to design a dial plan that can be expanded without users having to change their DN. This not only causes user frustration, but ultimately causes customer confusion and added expense since stationary, business cards, Web Sites, etc. must all be updated.

For this design a variable-length on-net dial plan will be used. This allows users within a site to dial a 4 or 5 digit number. To reach users in other sites, an access code (usually 8) followed by the location code and then extension would be dialed. This dial plan allows for future growth and more flexibility within each site.

For more information on dial plans, refer to the following documents:

- *Cisco Service Ready Architecture for Schools Design Guide*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Education/SchoolsSRA_DG/SchoolsSRA-DG.html

- *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager* 7.x

  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html

SRST

Cisco Unified SRST provides Cisco Unified Communications Manager with fallback support for Cisco Unified IP phones that are attached to a Cisco router on the local network. Cisco Unified SRST enables routers to provide call-handling support for Cisco Unified IP phones when they lose connection to remote primary, secondary, or tertiary Cisco Unified Communications Manager installations or when the WAN connection is down.

When Cisco Unified IP phones lose contact with primary, secondary, and tertiary Cisco Unified Communications Managers, they must establish a connection to a local Cisco Unified SRST router to sustain the call-processing capability necessary to place and receive calls. The Cisco Unified IP phone retains the IP address of the local Cisco Unified SRST router as a default router in the Network Configuration area of the Settings menu. The Settings menu supports a maximum of five default router entries; however, Cisco Unified Communications Manager accommodates a maximum of three entries. When a secondary Cisco Unified Communications Manager is not available on the network, the local Cisco Unified SRST Router's IP address is retained as the standby connection for Cisco Unified Communications Manager during normal operation.

Configuration examples, compatibility, etc. can be at the following URL: http://www.cisco.com/en/US/partner/products/sw/voicesw/ps2169/tsd_products_support_series_home.html

Community College Mission Relevancy

This chapter discusses the possibilities of a comprehensive Unified Communications architecture for community colleges. The following subsections provide a non-technical discussion of how the UC considerations might fit into the foundation services or introduced earlier in this document. These foundation services are as follows:

- Virtual Learning Environment
- Secure Connected Classrooms
- Safety and Security
- Operational Efficiencies

Virtual Learning Environment

This UC architecture provides a base call processing platform that allows remote student or instructor softphone or hardphone connectivity incorporating all of the features and capabilities of an on-site handset. This design also provides the call processing and media ready network for high bandwidth video applications such as Telepresence

Secure Connected Classrooms

Secure Connected Classrooms typically implies network connectivity. From a UC perspective this could also include secure handsets within the classroom. With the use of Extension Mobility the classroom phones would have very basic capabilities like 911 service and internal station to station access. When an instructor enters the room and logs on to the phone it now takes on the characteristics assigned to that instructor that include voicemail indicator, calling capabilities like long distance or international. The instructor can also then be reached regardless of campus location.

Safety and Security

Safety and security within the Unified Communications infrastructure can pose many questions:

- Is the system secure from network intrusion?
  - Is this covered in security section?
- Does the UC platform offer any features or design considerations to assist campus security or emergency services?
  - Although not covered in this document the UC platform can interface with a Cisco Product called Emergency Responder. Cisco Emergency Responder enhances the existing emergency 9-1-1 functionality offered by Cisco Unified Communications Manager. It assures that Cisco Unified Communications Manager will send emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary. In addition, the system automatically tracks and updates equipment moves and changes.

    Cisco Emergency Responder includes the following features:

  - Real-time location-tracking database and enhanced routing capabilities
  - Supports automatic notification of customer security personnel when an emergency call is in progress and provides the caller's location
  - Requires no administrative support for moving phones or staff from one location to another
  - The design does include PSTN trunks at every location. This will provide an address for each location to the PSAP but not offer the granularity provided by CER.
- Does the system offer high availability and survivability so communication can continue even when the WAN is down?
  - At the main campus each device has a primary, secondary, and tertiary target for call control.
  - Al other locations have a primary and secondary target for call control. The key point is that call control for these locations is typically the main campus under normal conditions. If a WAN component fails then each site has a local SRST router that can act as call control and still offer station to station as well as PSTN access.

Operational Efficiencies

The UC design set forth in this document provides for a single system with one system administration location. Regardless of the location of the phone all system administration is handled within a single administration access.

APPENDIX A

Reference Documents

Document Title	URL
CCVE SRA Solution Overview	http://www.cisco.com/en/US/docs/solutions/Verticals/Education/srajrcollegesoverview.html
Cisco SAFE Reference Guide	http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html
Enterprise Mobility Design Guide 4.1	http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html
Cisco Wireless LAN Controller Configuration Guide, Release 6.0	http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/Controller60CG.html
Cisco 802.11n Design and Deployment Guidelines	http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_80211n_design_and_deployment_guidelines.html
Cisco 5500 Series Wireless Controllers Data Sheet	http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/data_sheet_c78-521631.html
RFC 5415 Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification	http://www.ietf.org/rfc/rfc5415.txt
Voice over Wireless LAN 4.1 Design Guide	http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html
Cisco Aironet 1520, 1130, 1240 Series Wireless Mesh Access Points, Design and Deployment Guide, Release 6.0	http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP_60.html
Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet0900aecd8066a157.html
Cisco NAC Guest Server Overview	http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd806e98c9.html
Cisco Wireless Control System (WCS) Overview	http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html
Cisco Wireless Control System Configuration Guide, Release 6.0	http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/WCS60cg.html

Document Title	URL
Deploying Cisco 440X Series Wireless LAN Controllers	http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html
Cisco ASA Botnet Traffic Filter	http://www.cisco.com/en/US/prod/vpndevc/ps6032/ps6094/ps6120/botnet_index.html
Configuring Global Correlation	http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_collaboration.html
Cisco IronPort Support	http://www.ironport.com/support/
WCCP Configuration Guide	http://www.cisco.com/en/US/docs/switches/lan/catalyst3750e_3560e/software/release/12.2_46_se/configuration/guide/swwccp.html
Identity Based Networking Services	http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html
NAC Appliance Support	http://www.cisco.com/go/nacappliance
Clean Access Manager Configuration Guide	http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/47cam-book.html
Clean Access Server Configuration Guide	http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/461/cas/461cas-book.html
NAC Out-Of-Band Wireless Configuration Example	http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml