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 significant reduction in funding for institutions of higher learning, which in turn have tightened budgets and increased tuition rates. Increased tuition costs, as well as the reduction of available income due to the high unemployment rate worldwide, have led students that may have attended 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 two-year Associate's degree, while having the option to continue on to an institution of higher learning to earn a traditional undergraduate degree.

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

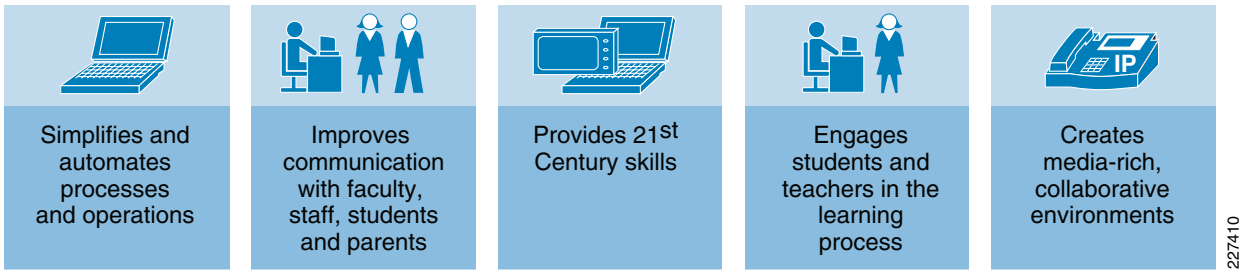
The 21st century learning environment will be an environment where anyone, from anywhere, at anytime can access community college resources. The traditional classroom will be extended by the use of online communities of learning. Students will be able to access their course work online, receive instruction 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 are flat or decreasing similar to institutions of higher learning, 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 "more green", 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

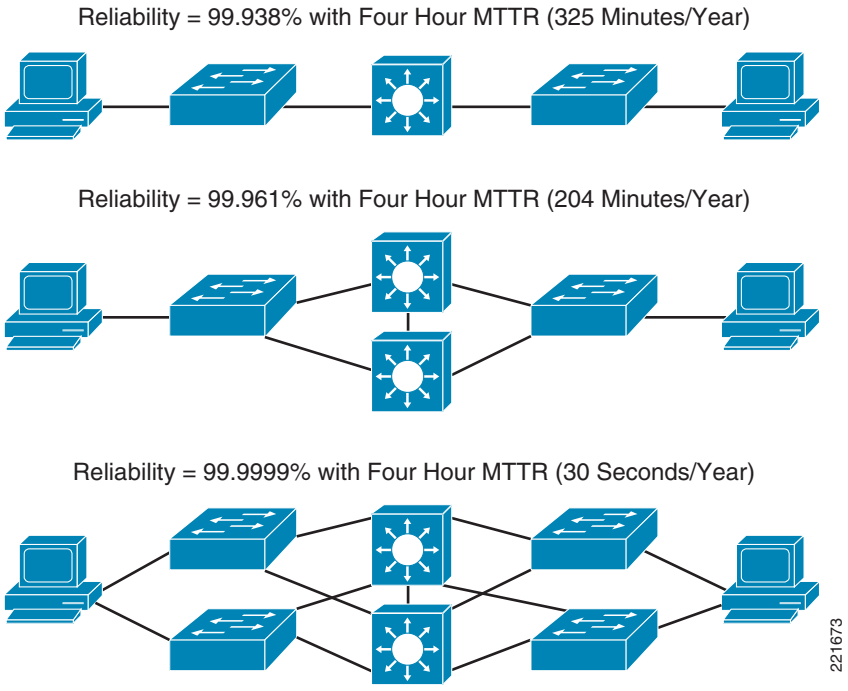
The high availability technologies used in the Cisco Community College reference design allow network equipment to eliminate the effects of any unplanned link or network failures by understanding the typology of the infrastructure and using that information to immediately re-route network traffic without 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:

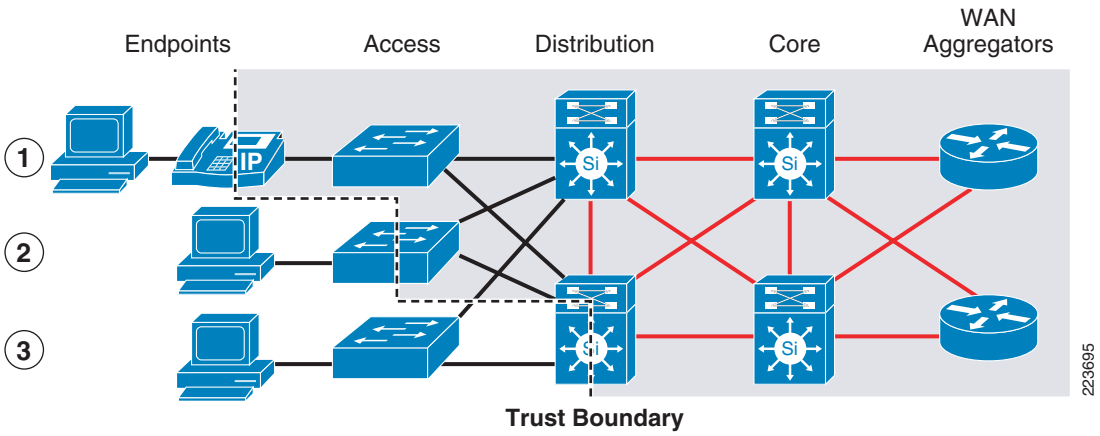
- The introduction of 10Gbps (and higher) link speeds is creating greater mismatches between high-speed and low-speed links in the campus. This increases the need to buffer and prioritize traffic.
- Well-known applications ports, like HTTP, are being used by a large number of applications. There is a 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

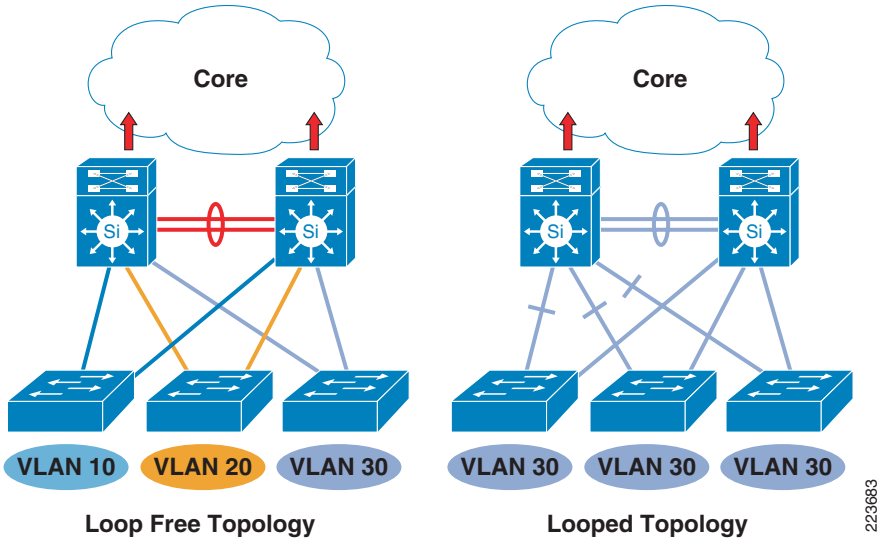
In a hierarchical network design, the core and distribution layers can reconverge in less than 1 second after most types of failures. The access layer typically has longer convergence times due to the inherent deficiencies of a flat Layer-2 architecture. Bridging loops, broadcast storms, and slow reconvergence 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.

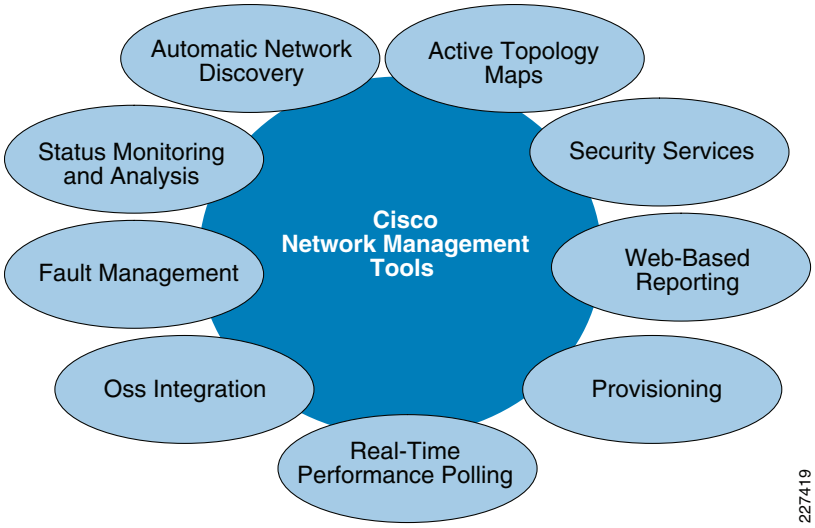
- *IP telephony*—At the foundation of the Cisco Unified Communications solution is its proven, industry-leading call processing system, Cisco Unified Communications Manager. This highly available, enterprise-class system delivers call processing, video, mobility, and presence services to IP phones, media 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

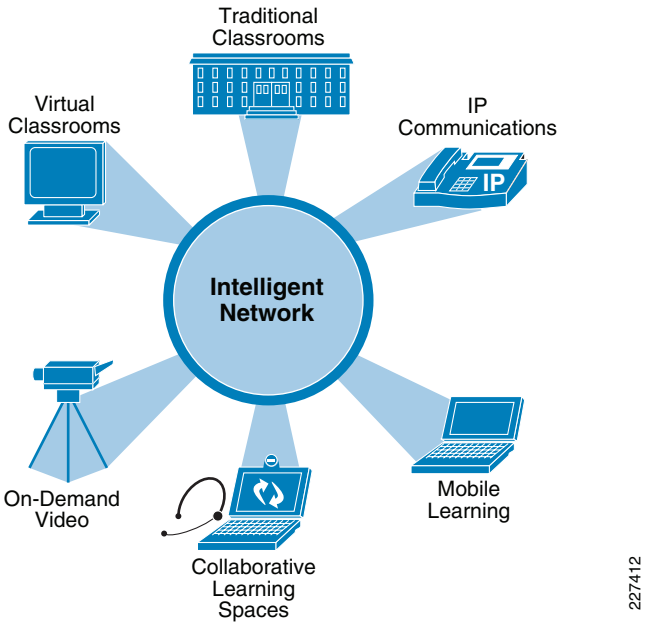
One of the key challenges that face community colleges is extending their learning environments beyond the campus to allow for online/distance learning, professor collaboration, and anytime/anywhere access for students to obtain course and educational materials. This virtual learning environment is key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

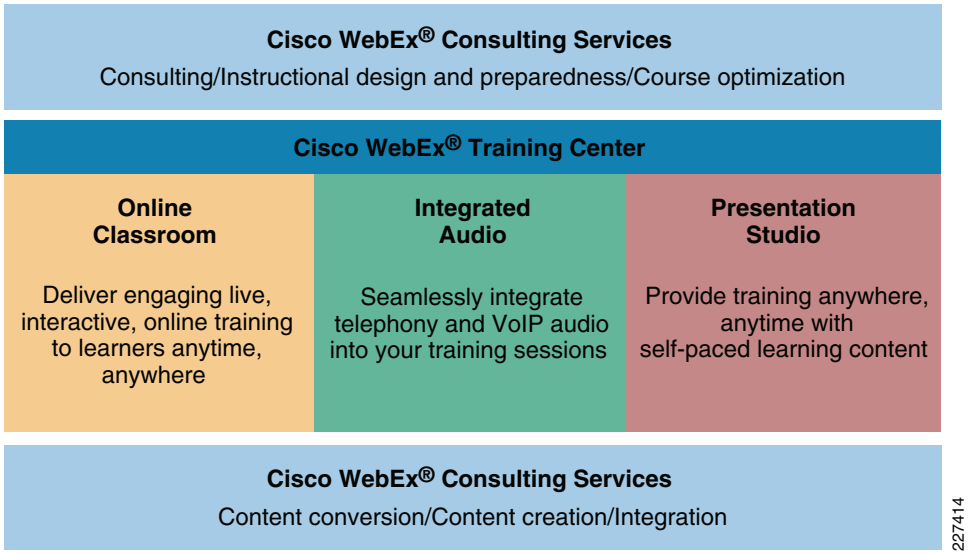
The Virtual Classroom solution is composed of campus-hosted technologies:

- 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.

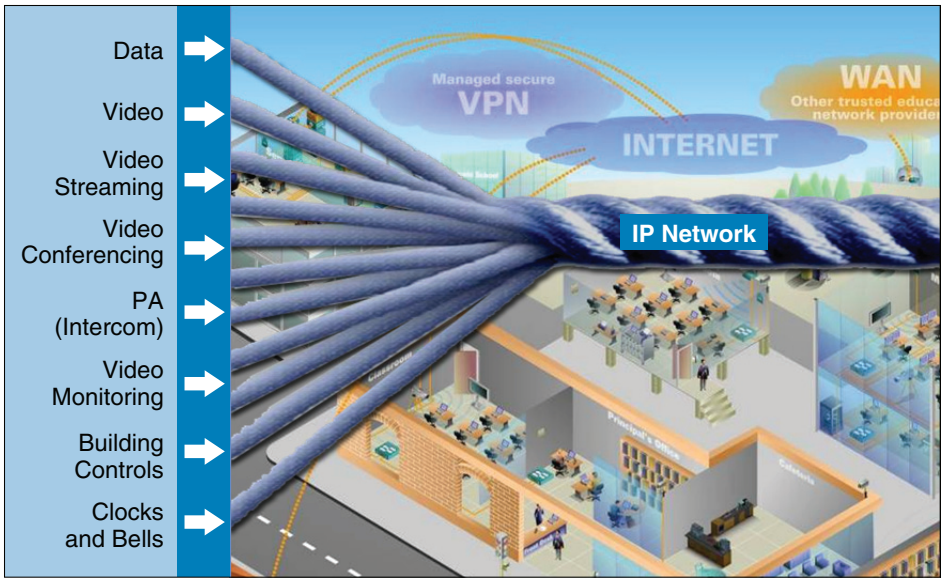
Operational Efficiencies

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.

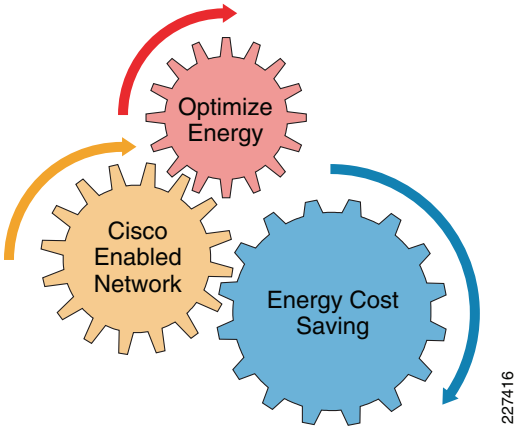
Facilities Management

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).

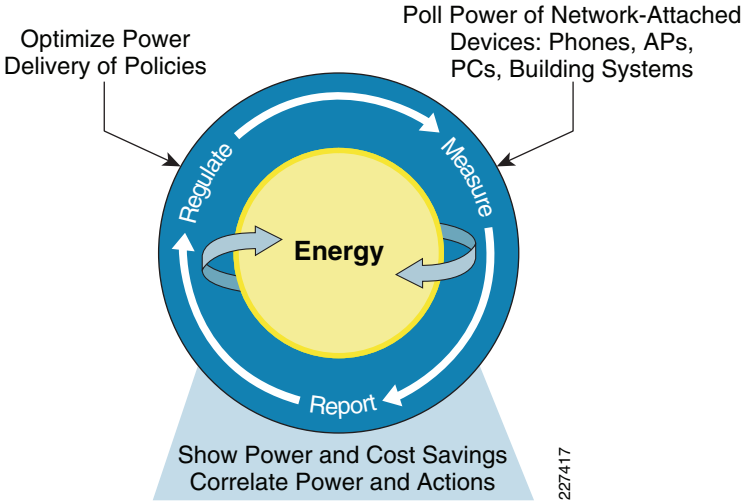
Figure 1-9 Cisco EnergyWise Optimize and Cost Saving



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).

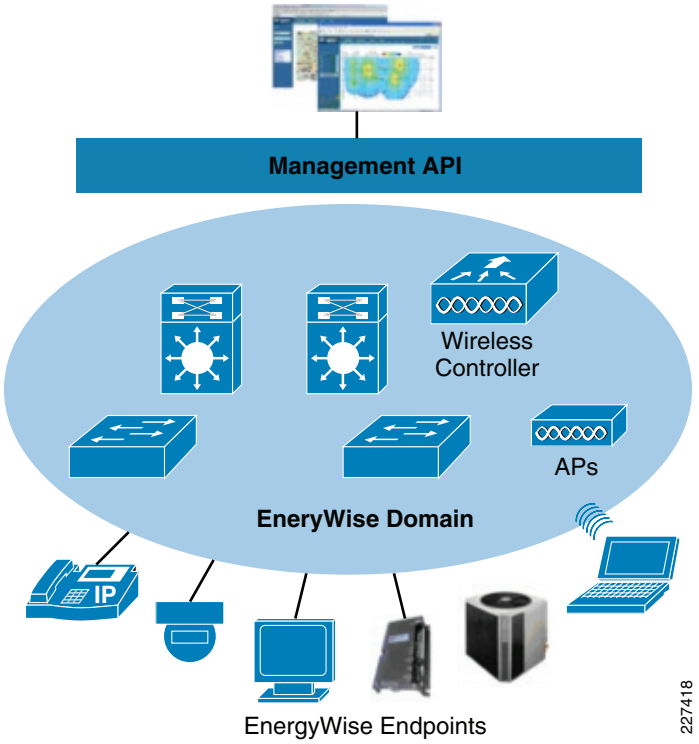
Figure 1-10 Cisco EnergyWise Optimized Power Delivery and Verification



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.

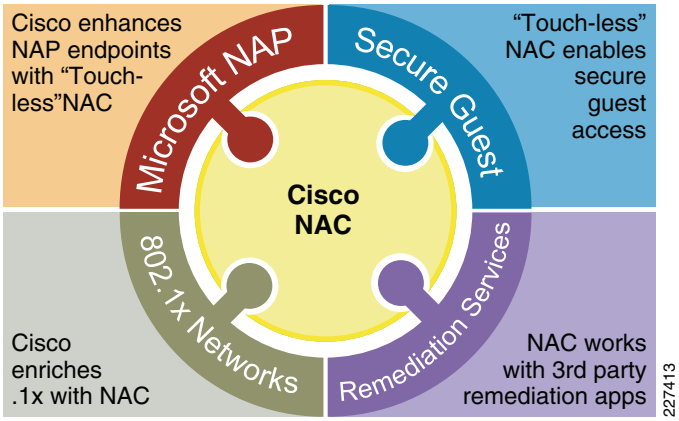
Network Admission Control for Guests and Students

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.

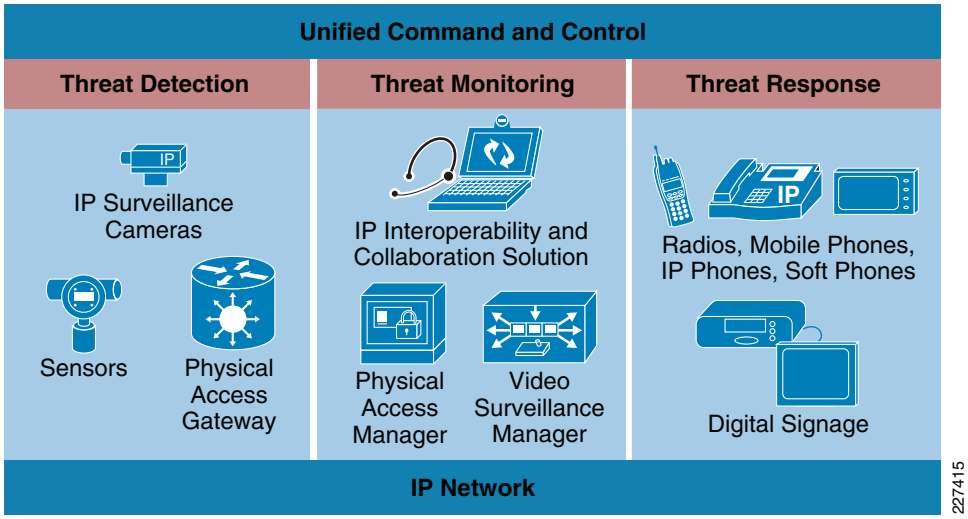
Cisco enables customers to build cost-effective, modular physical security solutions that are both best in class and interoperable. Cisco physical security products support the company's vision of a single unified security product suite that enables integration with all security operations within the 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

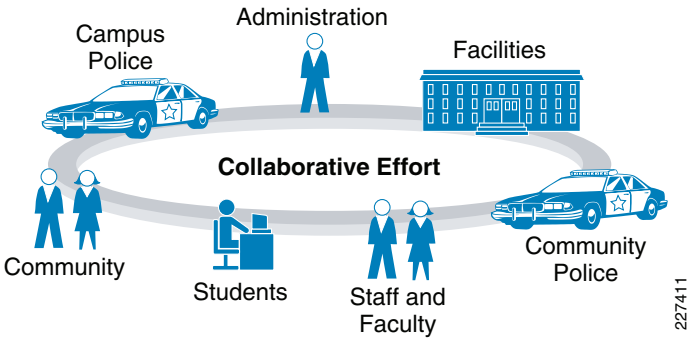
IPICS for Emergency Collaboration

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