CHAPTER 2

Service Ready Architecture for Schools—A Framework for Education

The drivers, key initiatives and requirements of the education environment are evolving beyond the traditional enterprise network. The next generation network architecture for school environments must be built on a technical foundation that takes into consideration the current economic environment as well as other business factors impacting the education market as a whole. The fundamentals of this next generation network must:

- Allow many services to operate seamlessly over a common infrastructure.
- Embed service recognition, awareness, and differentiation into all components.
- Support different voice, video, and data services while ensuring availability, scalability, and security.
- Adapt to network technical innovations that allow for better resiliency and the implementation of new network services.
- Integrate these new services and technical innovations with existing network equipment, protocols, and methods of communication.

The Service Ready Architecture for Schools is a well-designed and validated network architecture that is flexible, adaptive, and cost effective to support a wide range of educational services. This architecture provides the ability to deliver all of the services required of an enhanced learning environment, as well as the ability to collaborate with other schools, district headquarters, and entities beyond the district.

At the heart of the architecture is a robust routing and switching network. Operating on top of this network are all the services used within the school district, such as safety and security systems, voice communications, video surveillance, etc. The architecture has been designed around both school operations and technical considerations.

Architectural Design Considerations

This architecture utilizes key technologies that address the safety and security, connected real estate, and multi-service requirements of the modern educational network. The architecture is constructed in a manor that allows these technologies to work seamlessly together.

- High availability—The high availability technologies used in the Service Ready Architecture for Schools 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 re-learn (reconverge) the network. The use of this technology allows critical services such as voice and video communications to remain unaffected by network outages.

- Single-fabric multi-service—This technology gives the network administrator the ability to have many different services or networks share the same infrastructure, yet maintain logically separate networks. As multiple services operate over a single infrastructure, it becomes important to manage traffic based on the service being utilized. In the education environment this is particularly important as schools struggle with allowing student access to the same network used for grading systems, safety and security, and phone conversations.
- 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 teacher's use of the network to enter grades 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 decide which traffic is most important. The ability to understand, mark, shape, and limit traffic is embedded into the Service Ready Architecture for Schools.
- Access layer flexibility—Employing a hybrid access layer design allows the network administrator to leverage an existing Layer 2 network while giving them the flexibility to implement a routed access layer. Moving the Layer 2/Layer 3 demarcation point to the access switch allows the network administrator to prevent loops without requiring multiple complex Layer 2 technologies, such as spanning tree protocol. Additionally, it provides high availability and eases network troubleshooting and management by leveraging well known Layer-3 troubleshooting tools and technologies.

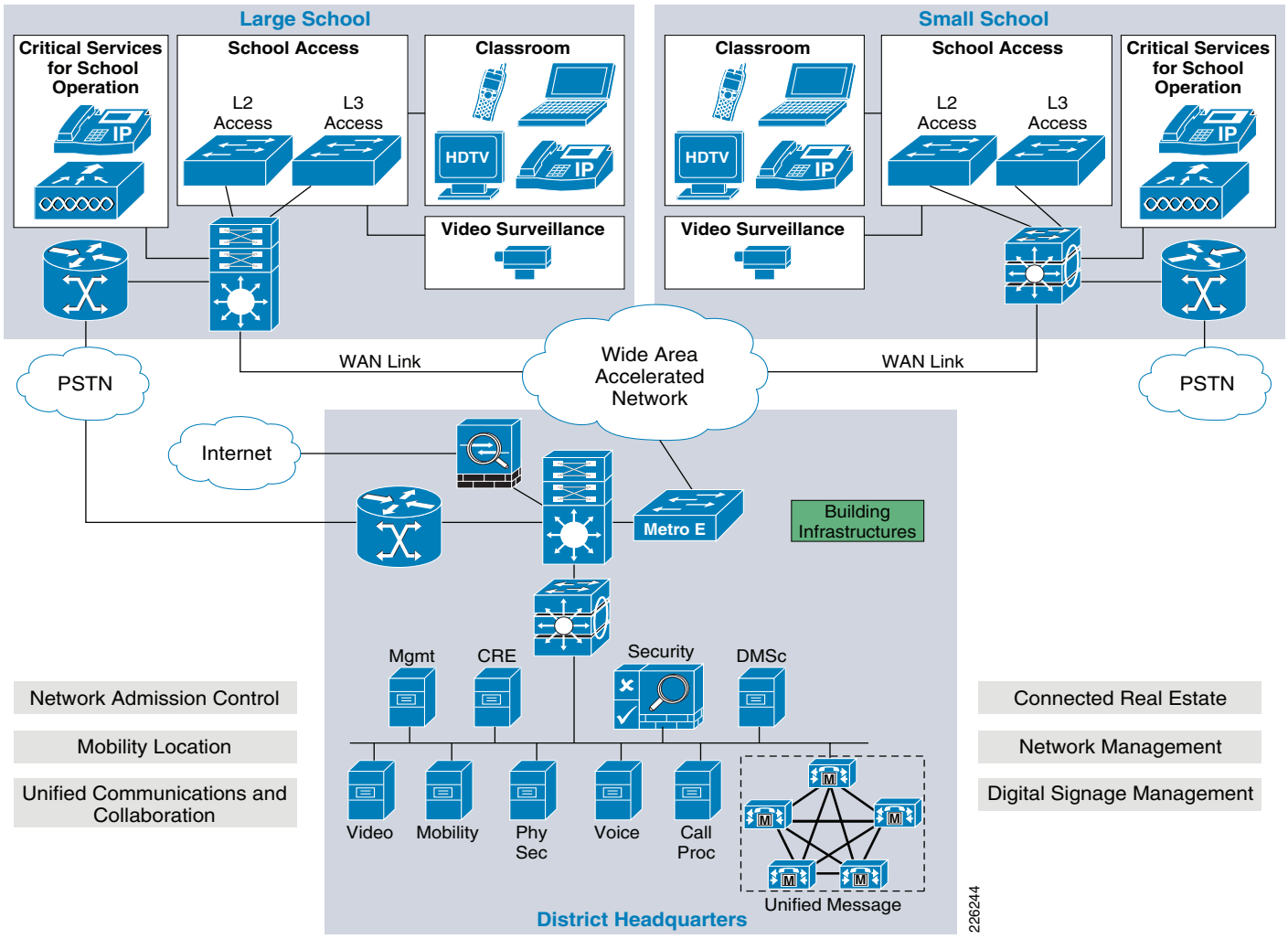
It is challenging to design architectures for the education environment that include technical innovations and services needed to support the classroom of the future and also create a safe and secure learning environment.

Cisco is committed to making this next generation architecture a reality by providing proven, validated network designs to ease the deployment of these new services. With each design, a deployment model is adopted and guidance provided on how to deploy services and technical innovations that meet the business and technical requirements of the education environment.

Overall Design

An architectural model for the school network is shown in Figure 2-1.

Figure 2-1 Service Ready Architecture for Schools



Cisco's Service Ready Architecture for Schools adopts a mission-critical services model in which services (safety and security, Unified Communications, and mobility) are deployed and managed at the district headquarters, allowing each school to reduce the need for separate services to be operated and maintained by school personnel.

Because many of the services are centrally located within the district office, rather than within each school itself, high network availability must be maintained. However the architecture also uses resilient application service features to maintain mission-critical services within the school in the event of a network failure.

This service model of the architecture allows school districts to maintain a good balance of controlling costs, pooling technical talent, and managing network services to offer a highly resilient, scalable, secure, and flexible network for the 21st century school.

Service Ready Architecture for Schools—Foundational Technologies

The Service Ready Architecture for Schools is the underlying service delivery framework from which all services and technologies flow for the school and district environments. This foundation must have simplified configurations and operations to ease the technical expertise required to support the environment, thus lowering the need for network experts. There is also a need for multiple core/distribution options to scale to the size, bandwidth, and requirements of the school's network to adapt to different size schools and school districts. The technology choices to scale this design and meet future needs include:

- High availability—The network must continue operations in the event of a network or service failure.
- Redundancy—All critical school services reside within the school to ensure they are not interrupted in the event of a wide area network outage, but the network should be flexible so as to allow non-critical services to be located in the district office to leverage economies of scale and lower total overall cost.
- Quality of Service (QoS)—The network must ensure proper prioritization of real-time traffic to enable a media rich network environment supporting voice, video, and data applications.

High Availability

The long-term capability of the network does not require constant hardware or software upgrades. New features and services can be added via in-service software upgrades. The network is highly available through redundancy and modularity and capable of providing an increased level of service not currently realized. Features are upgraded instantly and seamlessly over the network. Cisco can provide nonstop communications with resiliency and redundancy throughout all the layers of the network.

Many elements must be correctly designed and implemented to achieve such a high standard.

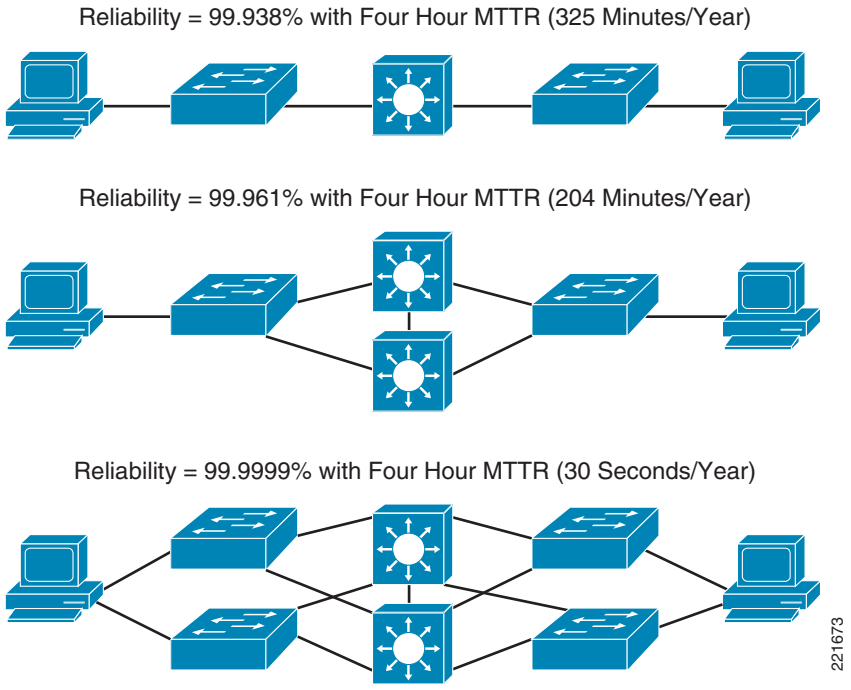
- Network operations and configuration management:
  - Management tools—Simplify provisioning, configuration management, troubleshooting
  - Management processes—Consistency of processes, minimize service times, etc.
- Network design and software features:
  - Redundancy—Paths, devices, servers, power, system components, locations, etc.
  - Resilience—Ability to function when the network is in a degraded state from an attack, misconfiguration, maintenance window, etc.
  - Prioritization and congestion management of traffic (QoS)
  - Security—Harden infrastructure, protect applications and data
- Hardware and software reliability—Servers, network devices, end-user systems
- Circuit reliability—WAN and LAN circuits
- Data center and services edge—Real-time data recovery and data archival capability

For more information, refer to the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html.

Redundancy

- Path redundancy—End-to-end redundant paths are required (see Figure 2-2) to achieve maximum redundancy. However at the access layer redundant paths to client end systems are typically uncommon. Redundant connections are critical in the data center or services edge where the application servers are located.

Figure 2-2 Second Network Shows End-to-End Redundant Paths



- Device redundancy—Redundant devices are usually preferred over redundant components within a single device. While redundant components within a single device are valuable, the best availability is usually achieved with completely separate devices (and paths).
- Power redundancy—Power diversity is another area that must be addressed because redundant devices attached to a single power source are vulnerable to simultaneous failure. For example, redundant core switches should have at least two unique power sources. Otherwise, a single power failure brings down both core switches. Alternatively, backup power could be implemented. These types of mundane issues are very important when creating a highly-available system.
- Network design and software features—In a hierarchical network design, the core and distribution layers can re-converge in less than one 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 re-convergence are examples of access layer problems that reduce end-to-end availability. Spanning Tree typically takes up to one 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.
- Access-layer design improvements—Currently, there are three different ways to design the access-layer control plane. Although all three of them use the same physical layout, they differ in performance and availability:
  - Traditional multi-tier access layer

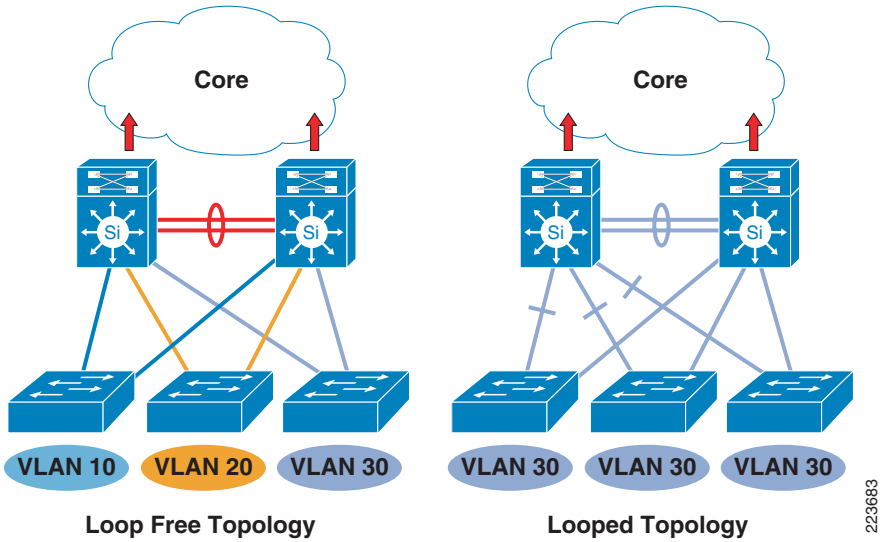
This is the traditional design where all access switches run in Layer 2, while distribution switches run in Layer 2 mode when facing the access layer and in Layer 3 mode when facing the core. Cross-connects between distribution switches are usually Layer 2 links. When not optimized, this model is dependent on spanning tree, with all its inherent limitations, to detect and recover from network failures. As mentioned, load balancing of redundant uplinks is not possible because spanning tree usually blocks one uplink. HSRP, VRRP, or GLBP must be used to provide First Hop Routing Protocol redundancy.

While noting the deficiencies of 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 2-3.

The best practice design offers several benefits. First, a loop-free topology is created. This means spanning tree does not impact re-convergence 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 2-3 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.

- Routed access layer

  This design improvement, as the name implies, 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.
  - Re-convergence times for the end-to-end network can be reduced to one second or less.
  - Re-convergence times become more predictable with the elimination of spanning-tree.
  - Redundant uplinks can be fully utilized.
  - HSRP/VRRP is no longer needed to provide host redundancy. 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 be standardized across schools.

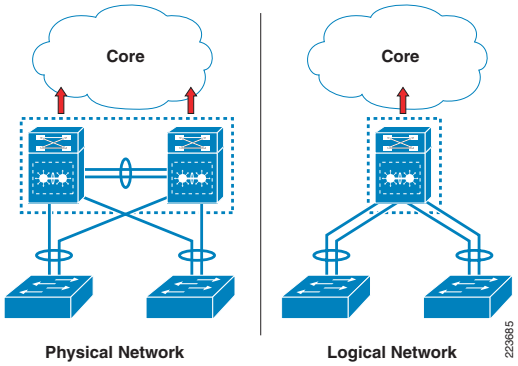
A drawback to the routed access model is the requirement to have separate IP subnets and VLANs on every access switch. This is in contrast to the traditional multi-tier model where a user VLAN can span several switches. However the convergence times of the routed access layer are much less than that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

For more information, refer to the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html.

- Virtual switch technology

This is a new service enabled by Cisco's Virtual Switching Systems (VSS) technology on the 6500 series and stackwise technology on the 3700 series switches. These features allow two or more distribution switches to be combined into a single virtual switch from a management and data forwarding perspective. Figure 2-4 highlights this technology.

Figure 2-4 Cisco's Virtual Switching Systems



VSS provides several compelling benefits over the traditional multi-tier design and the routed access design:

- Each access switch with redundant uplinks to two distribution switches now appears to be connected to a single switch via a two-port Etherchannel.
- Both links are now forwarding as spanning tree loops have been removed.
- Link failover times are below one second, consistent with Etherchannel capabilities.
- HSRP/VRRP are no longer needed to provide default gateway functionality.
- Unlike the multi-tier or routed access designs, there is no requirement for per-switch VLANs and IP subnets. This is a significant advantage and means the benefits of VSS technology can be gained without a major network reconfiguration.

Quality-of-Service (QoS)

There is some debate in the networking industry about the need to deploy QoS in enterprise architectures because of the ample amounts of bandwidth that make congestion rare. 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. Reasons why QoS is important in the campus portion of the network include:

- 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 ensure priority traffic is transmitted.
- Prioritized traffic, such as 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.

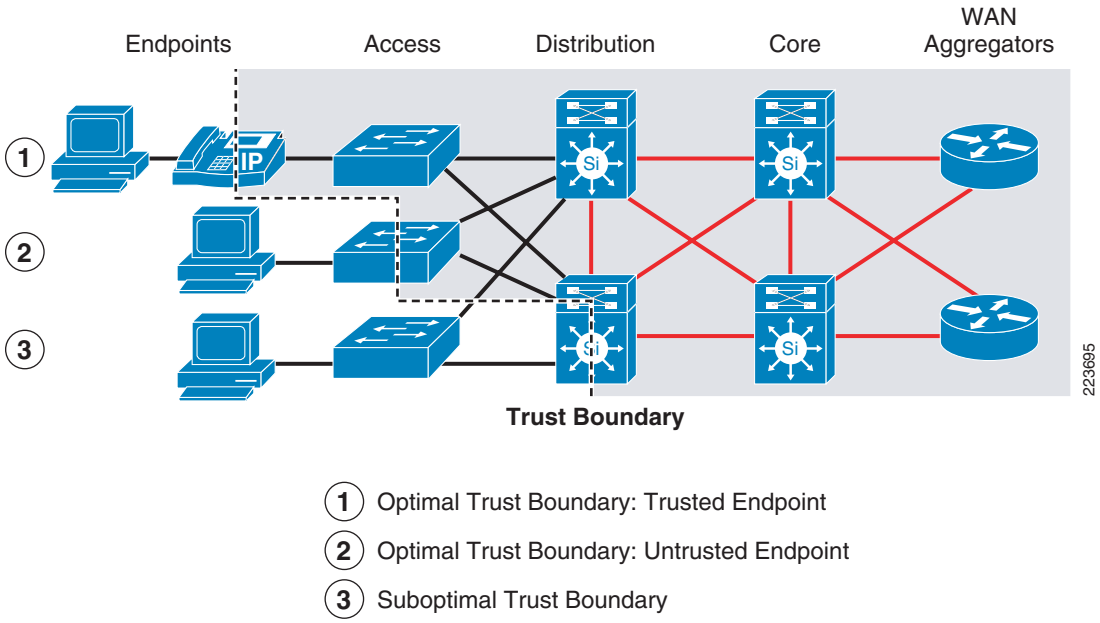
QoS Deployment Guidelines

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 CPUs of networking devices. High-speed networks require hardware-based QoS functions.

Figure 2-5 summarizes key QoS functions and where they should be performed.

Figure 2-5 QoS Functions



For more information, refer to the following:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

Service Ready Architecture for Schools—Key Services

The adoption of IP technology has led to a change in the learning environment. No longer are networks used solely to provide data communication between computers. IP technology has extended beyond the data network and is now used extensively for voice and video communication as well. Services that are a part of the Service Ready Architecture for Schools are shown in Figure 2-6.

Figure 2-6 Services in the Service Ready Architecture for Schools

Each of these services overlay the IP network and foundational technologies described earlier. While the services shown in Figure 2-6 are just a sample of the myriad of services available, they can be summarized into five key services:

- Unified Communications
- Digital Media Systems
- Mobility
- Security

Unified Communications

Cisco Unified Communications provide many solutions for schools 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 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 redundancy keeps service reliable. Cisco also offers several unified communications platforms for small districts. 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 and 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, 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—Schools may operate in unique educational environments that require specialized applications. To meet these needs, Cisco provides a versatile service creation platform, enabling schools 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.

For more information, refer to the following URL:
http://www.cisco.com/en/US/netsol/ns818/networking_solutions_program_home.html

IP Video Surveillance

Video surveillance systems have proven their value in a wide range of applications. In educational environments, video documentation of critical incidents enhances student safety and better protects valuable assets. However, traditional analog CCTV surveillance systems have many limitations—they are unable to store recorded video in local and remote locations or provide video access to mobile or

remote users. Having recognized the cost savings, productivity improvements, and enhanced communications provided by IP networks, many administrators would like to apply these technology benefits to video surveillance systems.

Network-centric video surveillance components include:

- Cisco Video Surveillance Manager enables education administrators and security personnel to view, manage, and record video locally and remotely using the IP network and a standard Internet browser. Video can be securely accessed anywhere, at any time, enabling faster response, investigation, and resolution of incidents. Video can be recorded and stored locally and off-campus, allowing it to be managed and aggregated with video from multiple locations. VSM interoperates with a wide range of third-party vendor devices and applications such as video analytics, providing a solution that is cost-effective to deploy, fits budgets, and enables new capabilities. As a result, student safety can be enhanced and valuable assets can be better protected through the video documentation of critical incidents.
- Cisco Video Surveillance Media Server—Media Server is a highly scalable and reliable video management platform that manages, replicates, distributes, and archives video streams.
- Cisco Video Surveillance Operations Manager—This Web-based user interface authenticates and manages access to video feeds. It is a centralized administration tool for the management of Media Server hosts, Virtual Matrix hosts, cameras, encoders, and viewers.
- Cisco Video Surveillance Media Virtual Matrix—Virtual Matrix monitors video feeds in command center and other 24-hour monitoring environments. It allows operators to control the video being displayed on multiple local and remote digital monitors.

For more information, refer to the following URL:
http://www.cisco.com/en/US/netsol/ns929/networking_solutions_sub_program_home.html.

Digital Media Systems

The Cisco Digital Media System is a comprehensive suite of digital signage, desktop video, and enterprise TV applications that you can manage centrally:

- Cisco digital signage provides scalable centralized management and publishing of compelling digital media to networked, on-premise digital signage displays. It enables the dissemination of district news and emergency Information to large screens connected to the school's existing network. You can deliver the same content to all signs in the district, such as reminders of testing dates, or deliver different content to different schools. Within the same school, you might display the cafeteria menu on one digital sign and information about an upcoming bond election on signs where parents pick up their children.
- Cisco desktop video gives students access to high-quality and compelling videos on demand (VoDs) and live Webcasts at their desktops. Digital Media can be browsed, searched, and viewed over the network through a unique, easy-to-use Cisco video portal experience—anywhere, anytime.
- Cisco enterprise TV is an interactive application that enables schools to deliver on-demand video and broadcast live TV channels over an IP network to digital displays. On-screen menus and program guides give users access to enterprise TV content and organizations can customize lineups and create their own content libraries. Users can navigate through channel menus and select from on-demand content with a remote control or other remote devices.

Components of Cisco's digital media system include:

- Cisco Digital Media Manager is the central management application for all Cisco Digital Media System products. It is used to manage, schedule, and publish compelling digital media for digital signage, enterprise TV, and desktop video. As an integrated part of the Cisco Digital Media System, this Web-based media management application enables content owners to easily upload, catalogue, edit, package, and publish digital media content for live or on-demand playback.
- Cisco Video Portal allows users to easily browse, search, and view digital media interactively on the desktop. It provides secure login, customizable playlists, search, advanced player controls, full-screen playback, slide synchronization, viewer questions support, and a secure usage-reporting tool. It supports established video formats such as Windows Media, Flash, and MPEG/H.264.
- Cisco Digital Media Players are highly reliable, IP-based hardware endpoints that enable digital signage and Enterprise TV through the ability to play high-definition live and on-demand video, motion graphics, Web, and dynamic content on digital displays. The Digital Media Player hardware options include support for standard-definition and high-definition MPEG-2 and MPEG-4/H.264, Flash, RSS, and other Web formats and dynamic data.
- Cisco LCD Professional Series Displays are an integral part of the Digital Media System (DMS) suite of products and are used to display information. Cisco LCD displays are available in different sizes and models and offer full 1080p resolution.

For more information, refer to the following URL:

http://www.cisco.com/en/US/netsol/ns928/networking_solutions_sub_program_home.html

Mobility

Cisco Mobility and Wireless Solutions for Schools give students and staff the freedom to be anywhere on campus and still perform all the tasks they would normally do on a classroom'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, teachers, parents, and administrators. Mobility products include:

- 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 system-wide wireless LAN (WLAN) functions, such as:
  - Enhanced security with WLAN policy monitoring and intrusion detection
  - Intelligent radio frequency (RF) management
  - Centralized management
  - 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:

- High-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.
- Cisco Mobility Services Engine is a solution that creates an open platform for the development and optimization of mobile applications. Designed with extensibility in mind, the platform supports a suite of software that is designed to create and optimize the performance of mobility applications by offering a standardized, open method for bridging network and application intelligence. The Mobility Services Engine allows schools to simplify the deployment of mobility applications across the district and introduces a structured way for partners to develop industry-specific mobility applications.

For more information, refer to the following URL:
http://www.cisco.com/en/US/netsol/ns820/networking_solutions_program_home.html

Security

Cisco security solutions combine multiple security technologies along with embedded security in Cisco routing and switching platforms to protect school network infrastructures. Some of these technologies include:

- Firewall solutions for network security
- A reliable firewall is the hallmark of a secure network. Networks support sensitive, crucial applications and processes and provide a common infrastructure for converged data, voice, and video services; firewall security is a primary concern. Instead of providing only point products that set a base level of security, Cisco embeds firewall security throughout the network and integrates security services in all of its products. Firewall security becomes a transparent, scalable, and manageable aspect of the business infrastructure.
- Cisco NAC Appliance is an easily deployed Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network.
- Cisco Secure ACS is a highly scalable, high-performance access policy system that centralizes authentication, user access, and administrator access policy and reduces the administrative and management burden. Cisco Secure ACS is a central point for administering security policy for users and devices accessing the network. Cisco Secure ACS supports multiple and concurrent access scenarios including:
- Device administration—Cisco Secure ACS authenticates network administrators, authorizes commands, and provides an audit trail.

- Remote access—Cisco Secure ACS works with VPN and other remote network access devices to enforce access policies.
- Wireless—Cisco Secure ACS authenticates and authorizes wireless users and hosts and enforces wireless-specific policies.
- 802.1x LAN—Cisco Secure ACS supports dynamic provisioning of VLANs and access control lists (ACLs) on a per user basis and 802.1x with port-based security.
- Network admission control—Cisco Secure ACS communicates with posture and audit servers to enforce admission control policies.

For more information, refer to the following URL:
http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html

Conclusion

The Cisco Service Ready Architecture for Schools is a network roadmap for school districts to utilize to enable 21st century education for students and teachers. It is built by combining an understanding of the current and future school district network needs with the best technology available, while considering the technical and financial constraints faced by school districts.

To learn more about the Cisco Service Ready Architecture for Schools, refer to the following URL:

http://www.cisco.com/go/education