Cisco Public Sector Blueprints

Architectural Framework for K-12 Education

Version 1.0
December 19, 2008

U.S. Public Sector - Strategic Programs & Solutions

The information contained in this document is proprietary and confidential to Cisco Systems, Inc. (Cisco). The document is furnished in confidence to the party requesting this information with the understanding that it will not, without the express written permission of Cisco, be used or disclosed for other than evaluation purposes.

Legal Disclaimer

The information contained in this Architectural Framework document is proprietary and confidential to Cisco Systems, Inc. (Cisco). The Architectural Framework document is furnished in confidence to the party requesting this Architectural Framework document with the understanding that it will not, without the express written permission of Cisco, be used or disclosed for other than evaluation purposes.

This Architectural Framework document is not and should not be construed as an offer to contract. Some information contained in this Architectural Framework document may reference future technology under development. All such information is subject to change.

It should be noted that, in preparing this Architectural Framework document, Cisco has made certain assumptions. Except as expressly stated in Architectural Framework document or as otherwise expressly agreed upon in writing by the parties, any descriptions, documentation, or references to Third-Party Products, to the extent they are provided in this Architectural Framework document, shall be for informational purposes only.

Trademarks

Every effort has been made to identify trademark information in the accompanying text. However, this information may unintentionally have been omitted in referencing particular products. Product names that are not so noted may also be trademarks of their respective manufacturers.

Cisco is a registered trademark of Cisco Systems, Inc.

Cisco Systems is a registered trademark of Cisco Systems, Inc.

The Cisco logo is a registered trademark of Cisco Systems, Inc.

Cisco IOS is a registered trademark of Cisco Systems, Inc.

IOS is a registered trademark of Cisco Systems, Inc.

WebEx is a registered trademark of Cisco Systems, Inc.

Table of Contents

Introduction

The purpose of this architectural framework document is to provide a point of reference for Cisco Public Sector Account Teams and Solutions Business Development teams that discusses the technical considerations that should be addressed when approaching the U.S. K-12 Education environment. This architectural framework will focus solely on the U.S. K-12 environment and is one of many reference architectures produced by the U.S. Public Sector Strategic Programs and Solutions Team.

K-12 Education in the United States

The U.S. K-12 Education environment is undergoing a significant transformation today where technological innovation is not only employed to augment the learning process, but also to optimize school operations by driving energy and building efficiencies, heightening the awareness of, and responsiveness to, safety and security concerns that affect our schools and their respective districts.

With 97,000 public schools spread across 18,000 districts, with an additional 35,000 private schools, educating a combined 56,000,000+ students nationwide, the U.S. K-12 Education environment is extremely vast and must be able to adapt with agility to maintain educational excellence on a global scale, keeping pace with the next-generation education environment. Technology can provide a powerful platform for the educational needs of the 21st century.

Major Trends in Schools

- ***Student performance and assessment remain top of mind***—Schools are being held accountable for the success and failure of students. The No Child Left Behind (NCLB) and state mandates continue to place more pressure on schools to demonstrate how children are progressing in their education.
- ***Teacher attraction/retention and training***—Schools are struggling to attract and retain teachers. Over one-third of new teachers who enter the profession leave within the first 2 years, and over 40 percent of today's teachers will retire in the next 10 years. Professional development requirements are increasing, as today's teachers need to be certified and have high proficiency in their subject matter.
- ***Teaching 21st Century Skills***—Schools are being challenged to teach children skills that employers in today's global economy need, such as critical thinking, problem solving, and technology skills, which students need to succeed in the world today.
- ***School Safety and Security*** – School boards are enhancing security to help them cope with school violence, vandalism, potential terrorist attacks, and natural disasters. Schools

must ensure that confidential student data is not compromised and that students are safe from inappropriate content and predators while online.

- ***Transparent and effective communication***—Schools are striving to develop better and more open communications between teachers, administrators, students, and parents. Communication is seen as a key component in developing and managing student performance, since bringing the community and schools together creates a more open and positive learning environment. Historically, the line of communication between parents and teachers was only through the students. Technology provides a platform to allow direct links between all the parties involved in a student's education.
- ***School funding***—Schools are constantly facing budget issues. Even though some states in the U.S. have increased funding, many schools are still struggling financially, and K-12 technology funding continues to fluctuate. The Federal Enhancing Education through Technology program funding for 2007, for example, is only about one-half of the $500 million budgeted in 2005, and the E-Rate application process continues to be increasingly complex and time consuming. With the federal government, on average, providing only 6 percent of K-12's technology funding needs, schools are struggling to work better with state and local governments to secure additional funding. The bottom line is that schools are challenged to increase productivity while lowering operating expenses.

Cisco's U.S. K-12 Vision

Drivers and Objectives

In forming an architectural framework for U.S. K-12 Education, three key drivers are at the forefront of learning innovation.

- **Academic Excellence:** Student performance and assessment remain top of mind. Schools are being held accountable for the success and failure of students. The NCLB and state mandates continue to drive schools to demonstrate that their students are advancing in their level of education.
  Objective: *Leverage Cisco's innovation and prowess in networking, collaboration and technology solutions to remove barriers to learning and accessing information. Enable schools to communicate and collaborate throughout the district and beyond, to reach other higher education and research facilities resources state-wide, nationwide and globally.*
- **Administrative Efficiency:** With school budgets and funding sources tightly monitored and regulated in the current economic climate, schools strive to improve operational efficiencies. When schools streamline operations and processes, they become more efficient, and this supports them in their transformational initiatives.

Objective: *Provide schools the technological foundation and solutions to improve communications, automate routine tasks, streamline management and operations, increase productivity while reducing costs, provide better responsiveness with fewer resources, and enable advanced mobility.*

- **School Safety and Security:** Student safety is absolutely top of mind for schools. The top three threats within the U.S. Public Sector are shootings, theft, and vandalism. The preservation of life and protecting the welfare of our students is of utmost concern. ***Objective:*** *Take what we've learned from creating the Cisco Open Platform for Safety and Security (COPSS) to ensure that the platform and networking is in place to provide the necessary technology and solutions to allow schools to reach out immediately in emergency-response situations, provide critical information to everyone at once, and to proactively reduce and thwart threats, before they can evolve into crisis situations.*

The Future of Education

The ultimate end result of implementing the K-12 Architectural Framework is to truly transform the current education environment to one that promotes learning anywhere, anytime, regardless of the medium. Leveraging technology to eliminate barriers to accessibility is absolutely top of mind to educators and school district staff. Making information easy to access enables students to learn at their own pace and not be constrained to a single method of information delivery. Mechanisms that increase student performance can be realized through technology to assist in the development of 21st century skills. Some of the key initiatives to consider are:

- ***Smart and Flexible Learning Environments***: The very classrooms where teaching and learning take place are transforming. Dynamic classrooms, where the physical format of the room can be changed on-the-fly, are being seen in more schools to facilitate the use of advanced technologies that allow classrooms to be more connected to resources and the district network.
- ***Technology-Enabled Learning***: Information is being delivered in multiple formats, often combining methods of delivery to optimize the learning experience. More and more user-created content is coming to the forefront in the education community. Students learn and share via video, photo-sharing, blogs, wikis, instant messaging, etc. Additionally, the learning paradigm is shifting from static consumer-only to dynamic interactive/real-time consumers and producers.
- ***Social Networking and On-Line Learning***: Students are interfacing with each other and their educators more than ever. Another interesting trend is that students are publicly publishing their work more today, which drives a higher expectation for quality in the work they produce.

- ***Convergence of Information and Communications***: Web 2.0 initiatives continue to drive technology practices in the education community. Unified Communications is becoming more prevalent in school districts and leverages the benefits of an IP-based platform to marry data-rich information with communications facilitating a higher level of responsiveness and engagement with the extended community (the district, other schools, students' parents). This drive toward convergence has also enhanced the safety and security practices in schools where informed emergency response and threat avoidance are top of mind.
- ***Learning Communities***: Collaborative environments for both students and teachers are on the rise. Integrating technologies further enhances the experience by providing such utilities as interactive-video, on-demand video feeds, voice and Web collaboration, video to mobile devices, and TelePresence.
- ***1-to-1 Learning***: Providing teachers and students an environment where everyone has access to a mobile computer, as well as digital content, educational software, and digital authoring tools.
- ***Connected Real Estate***: Intelligent and energy efficient buildings are high on the priority list for school districts as energy costs have risen and administrative budgets have been reduced. Converging disparate building networks into a common IP backbone marries energy efficiency, technology infrastructure, and Green initiatives, virtualizing the infrastructure while reducing the size and cost of the physical cable plant. Connected Real Estate is also a key element in promoting safety and security. Policing building access or using RFID tagging for the protection of assets is quickly becoming a popular practice, as is the incorporation of IP video surveillance systems and emergency response technologies that are integrated to the entire district's network, as well as the public safety community.
- ***Mobility***: One of the largest movements in the education community is the pursuit of mobility. More education environments are moving toward wireless networks as the network of choice. It allows freedom of movement for students and educators, and also enhances safety and security by further augmenting the ability to reach individuals quickly and respond immediately to emergency situations. Furthermore, the use of laptop computers and mobile devices only seems to increase as time goes on. Integrate the preferred learning technologies with mobile platforms and we can realize learning anywhere, anytime, any place.

Technical Overview

Fundamental Concepts and Services

The reference architecture for the K-12 Framework is predicated on enabling 21st century learning through technology insertion in the classroom. The “classroom of the future” is service-enabled to enhance the learning environment by facilitating collaboration with other schools in the district, and even beyond the district – often statewide, and even nationally.

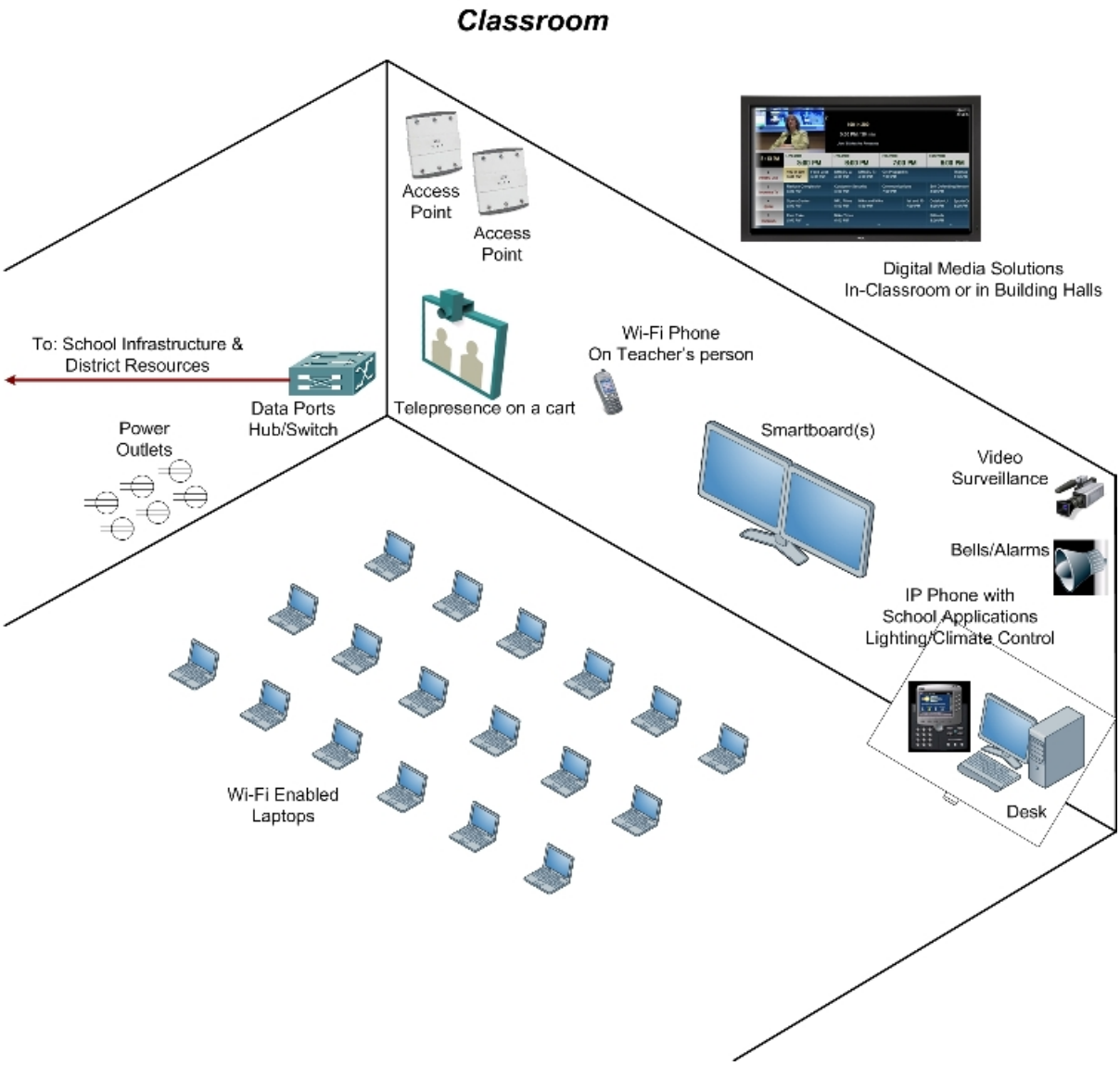
For example, the classroom becomes a learning environment where new tools and technologies will be available to the educator, as well as the students. Wireless laptops computers may be available to every student, connecting to the school network and ultimately accessing the Internet. Portable TelePresence units can be moved from classroom to classroom on an as-needed basis to connect to other schools, or guest speakers from higher education institutions that have, or have access to, TelePresence systems.

From a building standpoint, digital building systems for energy efficiency provide environmental controls at the teacher’s fingertips via integrated XML applications that are driven to the IP phone in the classroom. Climate and lighting controls are available, as well as intelligent building solutions that can reduce power consumption by deactivating areas of the school that are not in use, or powering off devices after school hours.

Physical Security can also be converged onto a common IP backbone within the school and throughout the school district. IP video surveillance cameras and line-powered bells/alarms can be directly integrated with the network. Video surveillance and analytics can be monitored and stored both locally at the school and centrally at the district for enhanced physical security. Bells and alarms are integrated with emergency response applications, can be delivered through the communications infrastructure and link back to the district, as well as the public safety community. Additionally, Digital Signage provides real-time video awareness of emergency alerts and messaging, whether in the classroom or throughout the halls of the school.

School applications securely converge data-rich information about students with the communications system. Access to this information allows such services as taking attendance and sending outbound notification to parents reporting absences via automated messages or voicemail. Student records can be securely accessed via the IP phone or a wireless handheld devices by the school nurse in the event of a medical incident, and announcements and alerts can be delivered to a specific classroom.

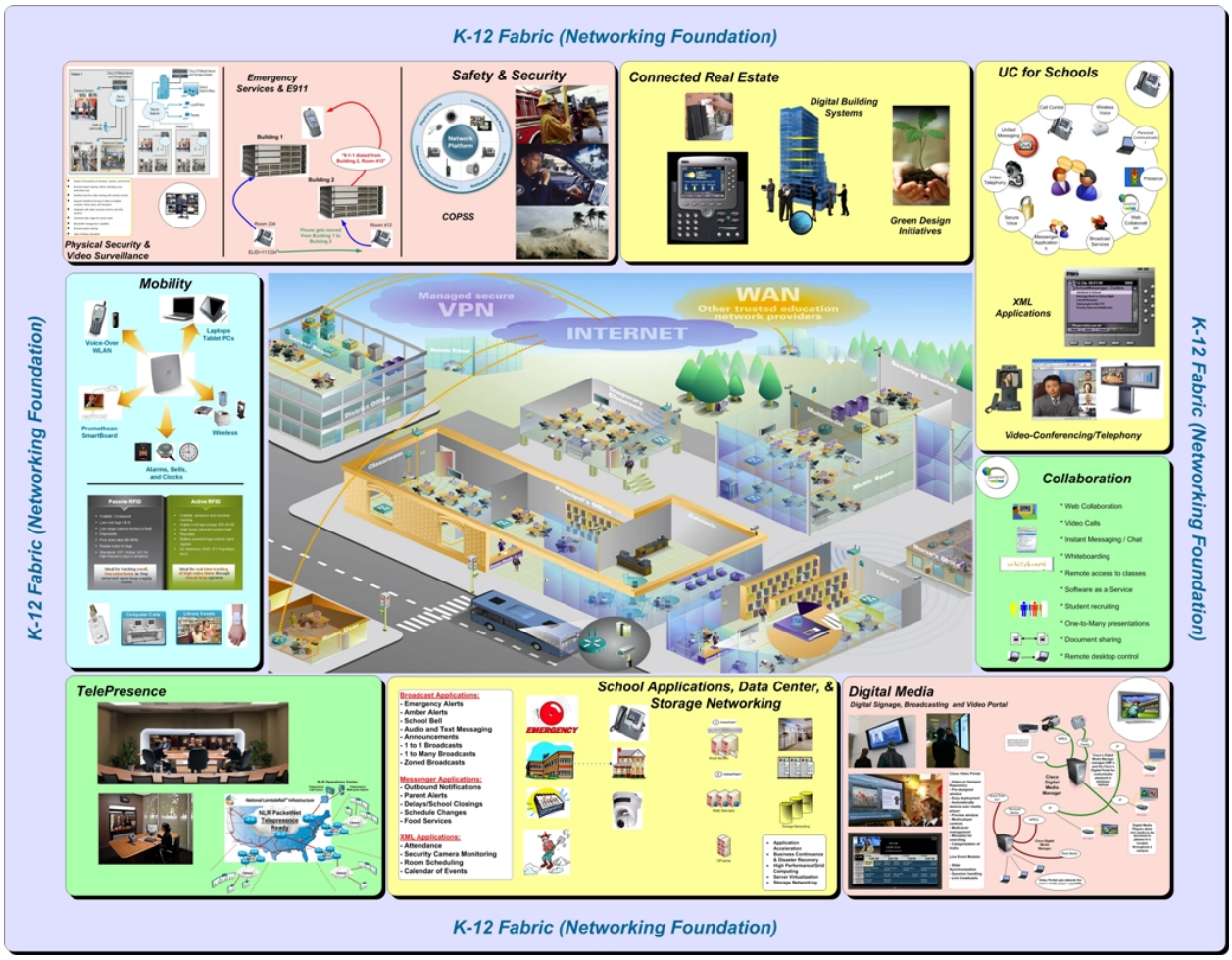
Mobile communications, in the form of a Wi-Fi IP phone, can be provided for teachers so they can move freely throughout the school, and even throughout the entire district, yet be reached immediately. This also allows teachers immediate access to communications resources in the event of an emergency, further augmenting the safety and security practices at the school.



These are just some of the possibilities that can be achieved with the K-12 Architectural Framework, and this only addresses the classroom so far. The underlying infrastructure that integrates all of the elements of the district is the Service Framework, or K-12 Fabric, that delivers these enhanced services, and can also allow collaboration well beyond the district.

Service Framework – The K-12 Fabric

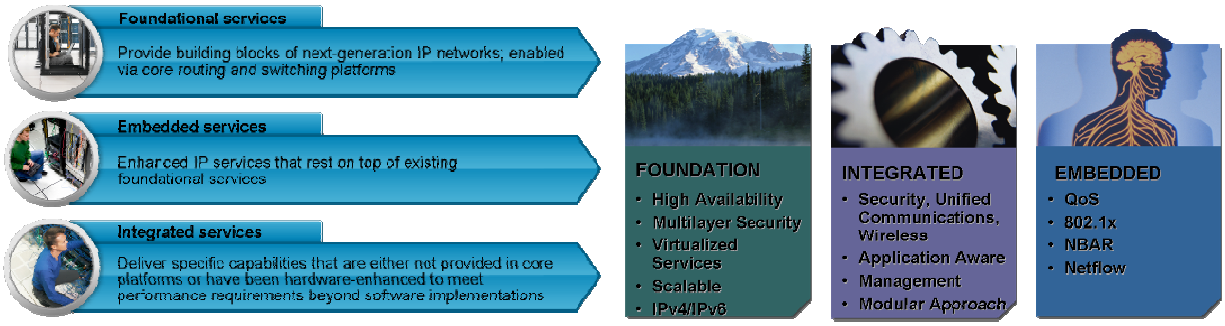
The K-12 Service Framework is designed to address the fundamental building blocks of the 21st century school environment. The foundation of the K-12 Service Framework lies in the K-12 Fabric. This Fabric is the networking foundation developed as a result of Cisco's 20+ year track record as the global leader in communications technology and innovation, allowing schools to leverage the network as the platform for 21st century education. This foundational approach creates an infrastructure that transforms the network from just simple connectivity and bandwidth to a platform for delivering differentiated services that extracts the most efficiency from the foundation, and optimizes the solutions available to schools, truly enabling the network to be a solutions delivery platform.



The fundamental building blocks are represented as the technology services that define the core and advanced technologies which enable schools to transform the way they educate and operate. These key services are represented in the blueprint diagram above as:

- Safety and Security for Schools
- Connected Real Estate
- Unified Communications for Schools
- School Collaboration Services
- Digital Media Solutions
- TelePresence
- Mobility
- School Applications & Data Center

This K-12 Fabric leverages the synergistic capabilities of proven interoperable technologies enabled through service tiers which are pervasive throughout the network infrastructure providing mechanisms for delivering services. Inter-related services build off of one another to form specific school/district offerings. Service tiers provide a methodology for categorizing and differentiating services to bring solutions enablement to schools and districts.



In designing any K-12 environment, these service delivery considerations must be addressed to implement a foundation that is:

- **Number One – Resilient!** The network as a platform has taken on a new role and is now considered critical infrastructure like a utility and such must be highly available and

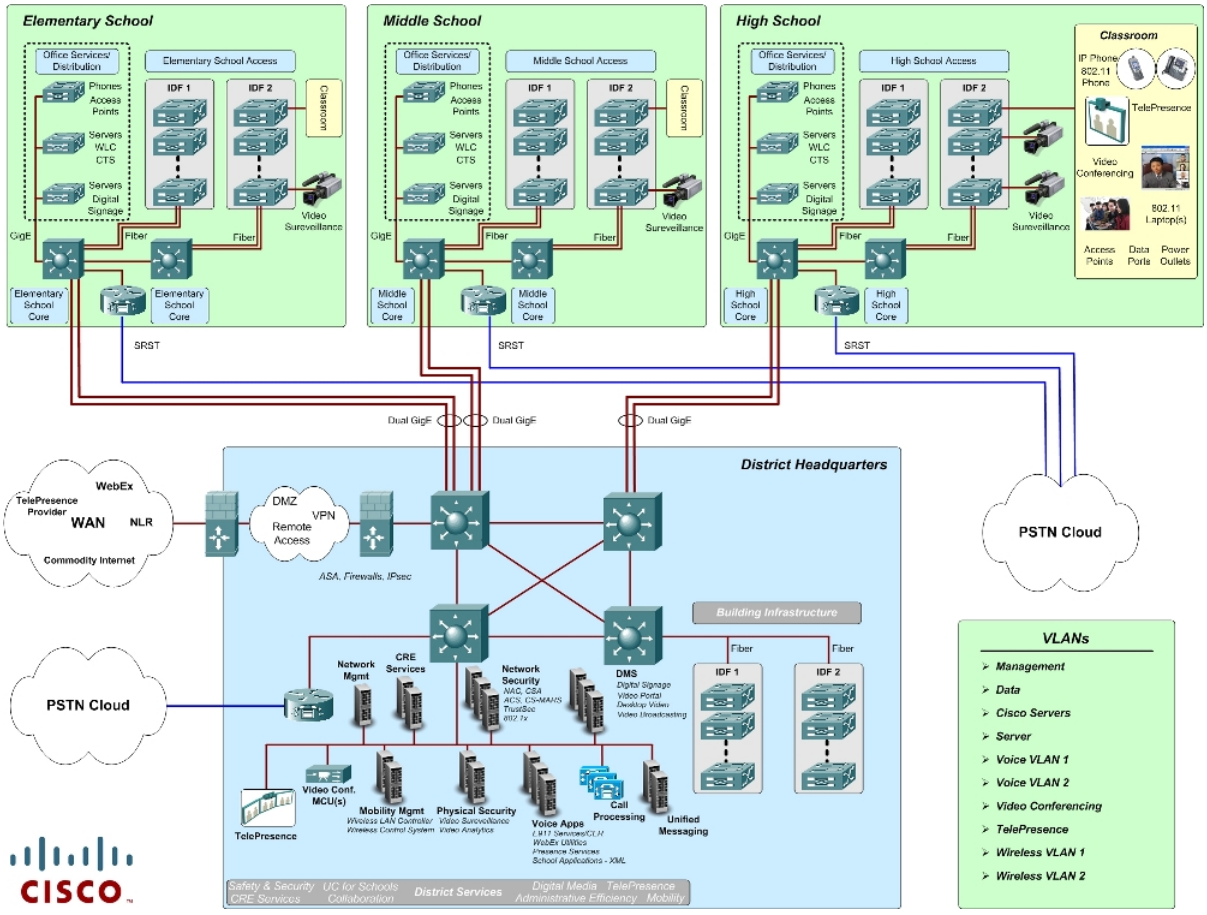
scalable. Classic perimeter security is no longer sufficient as users become more mobile, security must be pervasive across all levels of the architecture. It is not just a matter of protecting the perimeter and access, but protecting all elements of the network.

- **Integration:** Services and enabled solutions are integrated into the network foundation as integral parts and offerings available to schools and districts. For instance, security, unified communication and collaboration, mobility, etc., are all critical parts of the network. The network is aware of these services and solutions – if the network is aware and understands what function a service or solution is performing, then the network can make an informed decision about how to direct that information across the school/district infrastructure. This also provides the ability to help the solutions deliver their services better.
- **The Network Must Be Adaptive:** The network should have the ability to provision, optimize, analyze and defend itself. These critical capabilities are ***embedded*** in the network. The more intelligent the network, the more self-governing the network; thus, the lower its operational costs and the higher its capability and adaptability.

Reference Architecture for K-12 Education

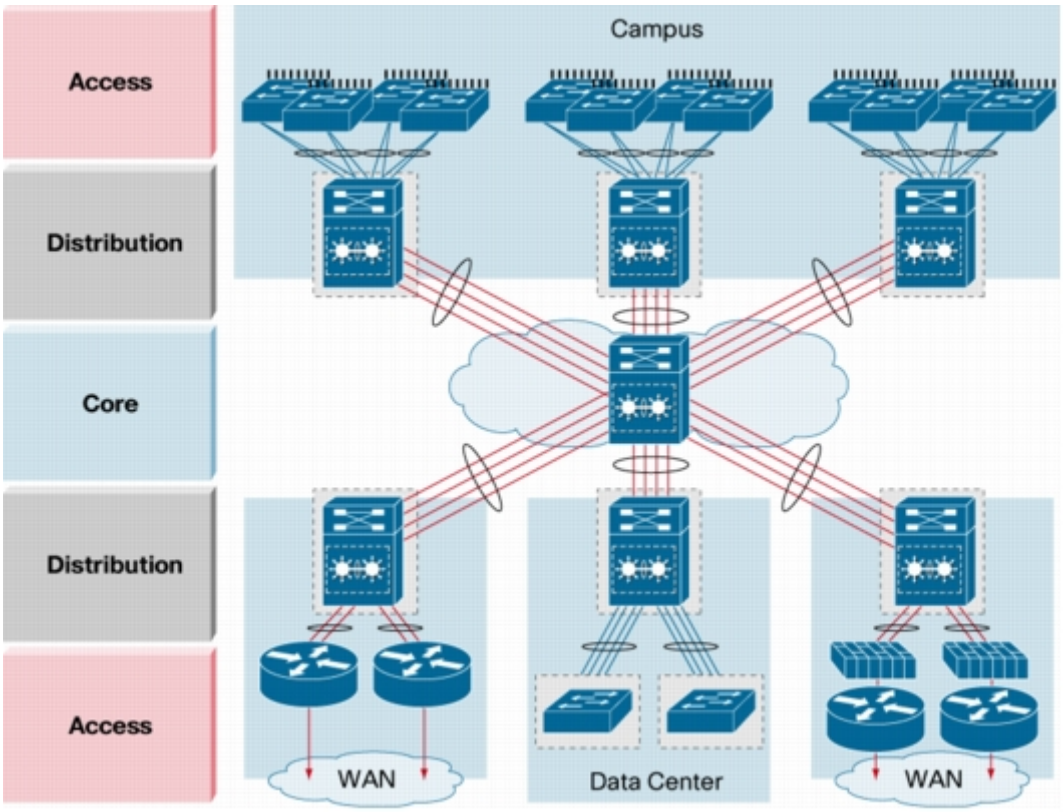
The K-12 Reference Architecture is an example of how the K-12 Fabric can be leveraged to set the underlying enterprise architecture used by schools to communicate and collaborate. This reference architecture will provide the foundation to deliver enhanced services and solutions that will optimize school operations, yet allow schools to adapt and respond to the changing needs of students and educators.

The following figure is a notional architecture for a school district and its schools, based on the concepts and methodologies of the K-12 Fabric. This diagram depicts a Metropolitan Area Network (MAN), which is a campus network for the school district, linking the District Headquarters and associated schools via Gigabit Ethernet (GigE) connections over optical fiber.



This topology, by design, follows enterprise architecture best practices with a well defined hierarchical Core, Distribution, and Access layer to further enhance the concepts and methodologies brought forth by the design guidelines of the K-12 Fabric.

The advantage of this hierarchical design is that it allows one to build a modular, deterministic, and scalable foundation. By utilizing this layered hierarchy, the complex collection of services and protocols in the Reference Architecture are pervasive, and can be tied to authentication methods to deliver services only to the users who require them.



Core Layer: This layer is literally the backbone of the network architecture and is responsible for delivering services quickly and reliably. The core must be highly available and survivable to provide interconnectivity between distribution points or layers.

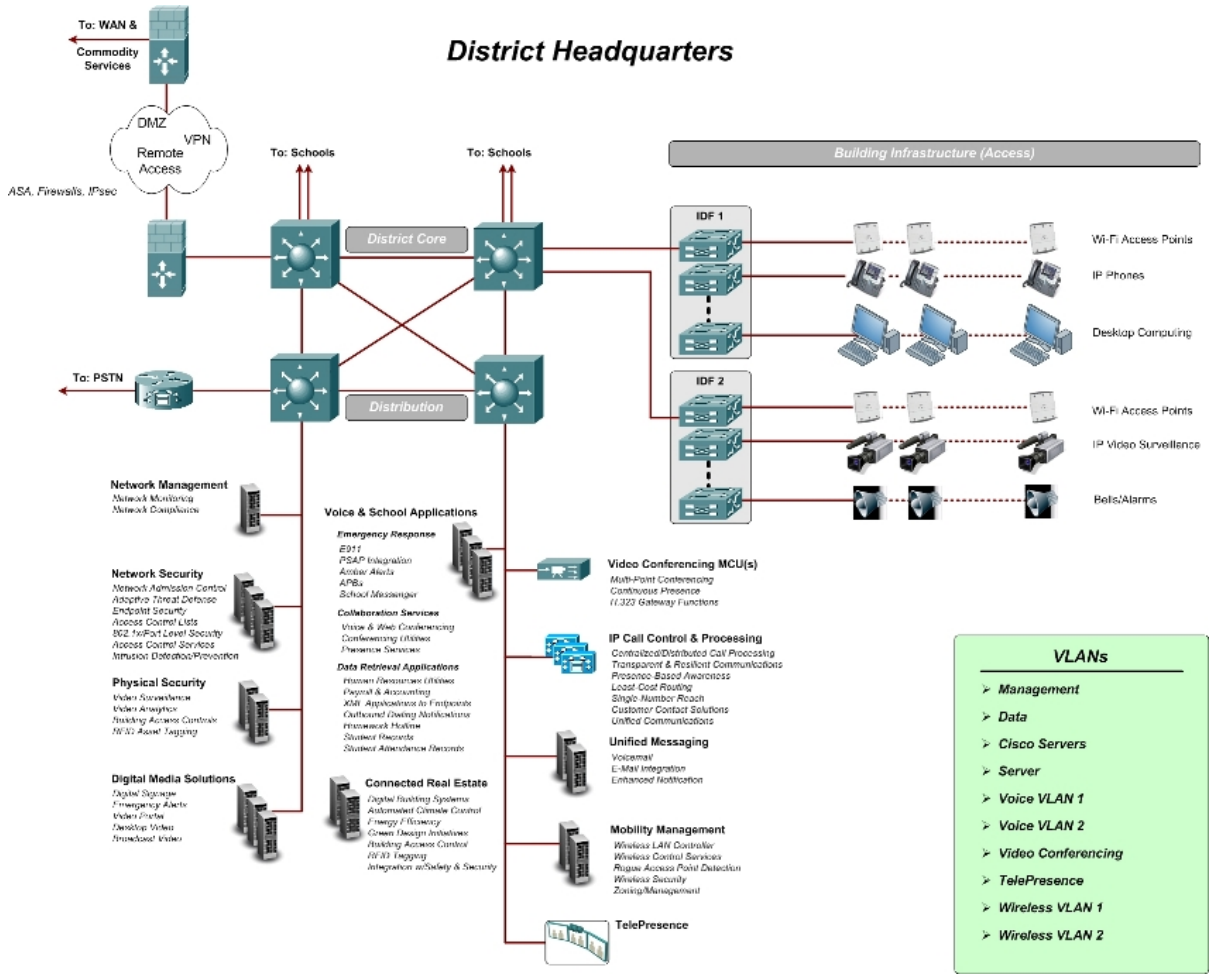
Distribution Layer: Sometimes referred to as the Workgroup Layer, this is the communication point between the Access Layer and the Core Layer. The Distribution Layer provides routing, filtering, and the implementation of policies to determine the fastest way that network service

requests are to be handled. This layer can be used to host regionally based or distributed network resources.

Access Layer: This layer is located at the periphery of the network and controls end-user and workgroup access to network resources. The origin and destination of most network communications is supported here.

Additionally, the hierarchical networking model allows for easier growth of the network due to its modular topology; creates smaller fault domains though clear demarcation and isolation; promotes load-balancing and redundancy; incorporates a balance of both Layer 2 and Layer 3 technologies, garnering the strengths of both; and takes advantage of Layer 3 routing for, faster convergence, scalability, and control.

Looking at a portion of the K-12 environment, such as that of the District Headquarters shown below, one can visualize the hierarchical networking layers on a smaller scale.

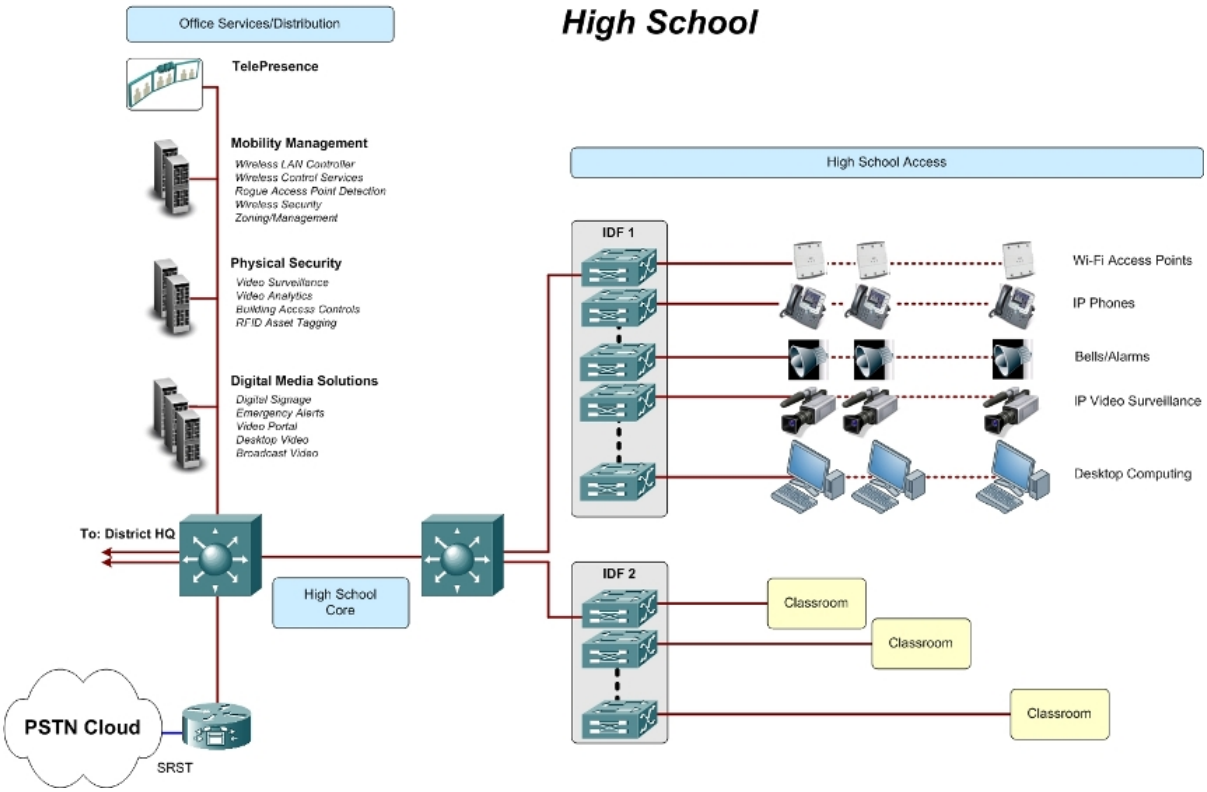


District Core: Provides the backbone for the entire school district and delivers fault-tolerant high-speed services throughout the district.

Distribution: This is the major communication point between the schools and District Services – which map directly to the technology services defined earlier for the K-12 Reference Architecture. Within the district, this is where policies are created and managed to facilitate the distribution of services to the schools, and ensure the most efficient transport path to maintain high availability and resilience in the entire district. This is also where security policies are enforced, and where transport paths are optimized, based on the type of service requested.

Building Infrastructure (Access): In a school environment, the Access Layer is where devices and peripherals connect to the network infrastructure. For example, in-building wireless access, video surveillance cameras, line-powered bells and alarms, desktop computing, servers, IP phones, and digital building controls. Within the district's schools, the Access Layer is where the actual classrooms attach to the network to gain connectivity to the district's technology services.

A similar hierarchy can be seen in the individual schools. For example, the High School diagram that follows shows a very similar layered network topology, yet may incorporate some services at the school to provide a level of autonomy, service distribution, and localized management.



Design Considerations

The common thread is that regardless of location in the district, the fundamental networking architecture can support the services required, whether they are at the district headquarters, a high school/middle school/elementary school office, or right in a classroom where a class is being taught. Some of these key considerations are:

- ***Latency and Bandwidth***: Gigabit Ethernet access where possible, speed of access is a high priority.
- ***High Availability***: Implement a strategy for sub-second convergence. Need to account for protection at the access layer. Implement a strategy that leverages centralized (district) and localized (school) services as backups for each other. Have a survival strategy. A school needs to be able to function on its own, should its connection to the district be severed.
- ***Quality of Service***: Essential for collaboration services such as Unified Communications, Video-Conferencing, TelePresence, and Digital Media.
- ***Mobility***: Implement high-speed wireless LANs to provide mobile access to voice services, voice applications, and multi-media services.
- ***Identity and Confidentiality***: Authentication and authorization of endpoints and end users on the network. Enforce encryption policies, leverage network admission control and endpoint security strategies to mitigate risks and neutralize threats.

These and other considerations will be detailed in the next section of this document which addresses the individual technology services that define the K-12 Reference Architecture.

Technology Services

As highlighted earlier, the K-12 Reference Architecture addresses the fundamental building blocks of the 21st century school environment, represented as technology services that define the core and advanced technologies utilized by schools. The key services addressed in this blueprint are:

- ***The K-12 Fabric***
- ***Safety and Security for Schools***
- ***Connected Real Estate***
- ***Unified Communications for Schools***
- ***Mobility***

The following technology services will be detailed in a future release of this blueprint document:

- ***School Collaboration Services***
- ***Digital Media Solutions***
- ***TelePresence***
- ***School Applications & Data Center***

The K-12 Fabric

The foundation of the K-12 Reference Architecture lies in the K-12 Fabric which forms the underlying service delivery framework. As mentioned earlier, this is the enterprise architecture through which all services and technologies must flow for the K-12 school and district environments.

Critical Technologies

Stacking Switches in Wiring Closet

Stacked fixed-configuration switch solutions make sense in the wiring closet when a modular switch is overkill, when port density may change up or down over time without a concern about reconfiguration downtime, or when flexibility in adding new fixed-configuration switches in a phased approach is desired.

Stacked switches in the wiring closet are not well suited to high demands for system uptime, when use of existing power supplies is desired, or when management of a single switch versus multiple switches reduces the number of devices to configure.

However, Cisco Systems has several stacking solutions for the wiring closet that allow the switches to be managed as one switch, and share one or more uplinks to the Distribution Layer in the building.

The Cisco Stacking Solutions are:

- Catalyst 2975GS (Single IP address for stack management, two Stackports per switch), up to nine per stack
- Catalyst 3750E Series (Single IP address for stack management, two Stackwise Plus™ ports per switch), up to nine per stack
- Catalyst 3750 and 3750G Series (Single IP address for stack management, two Stackwise ports per switch), up to nine per stack

Quality of Service Enablement

Voice, video, and other real-time classes of IP network services have strict requirements concerning packet loss, delay, and the variations in delay (also known as jitter). To meet these requirements, the K-12 Fabric incorporates Quality of Service (QoS) features throughout its infrastructure to allow for the proper prioritization of real-time traffic.

The QoS components for the K-12 Reference Architecture are provided through the rich IP traffic management, queuing, and shaping capabilities of the K-12 Fabric. Key elements that enable QoS are:

- Traffic Marking
- Enhanced Queuing Services

- Link Fragmentation and Interleave (LFI)
- Compressed RTP (cRTP)
- Low-Latency Queuing (LLQ)
- Link Efficiency
- Traffic Shaping
- Call Admission Control (CAC) – bandwidth allocation

Embedded Event Management

Network-Based Traffic Flow Statistics Gathering

DHCP Snooping

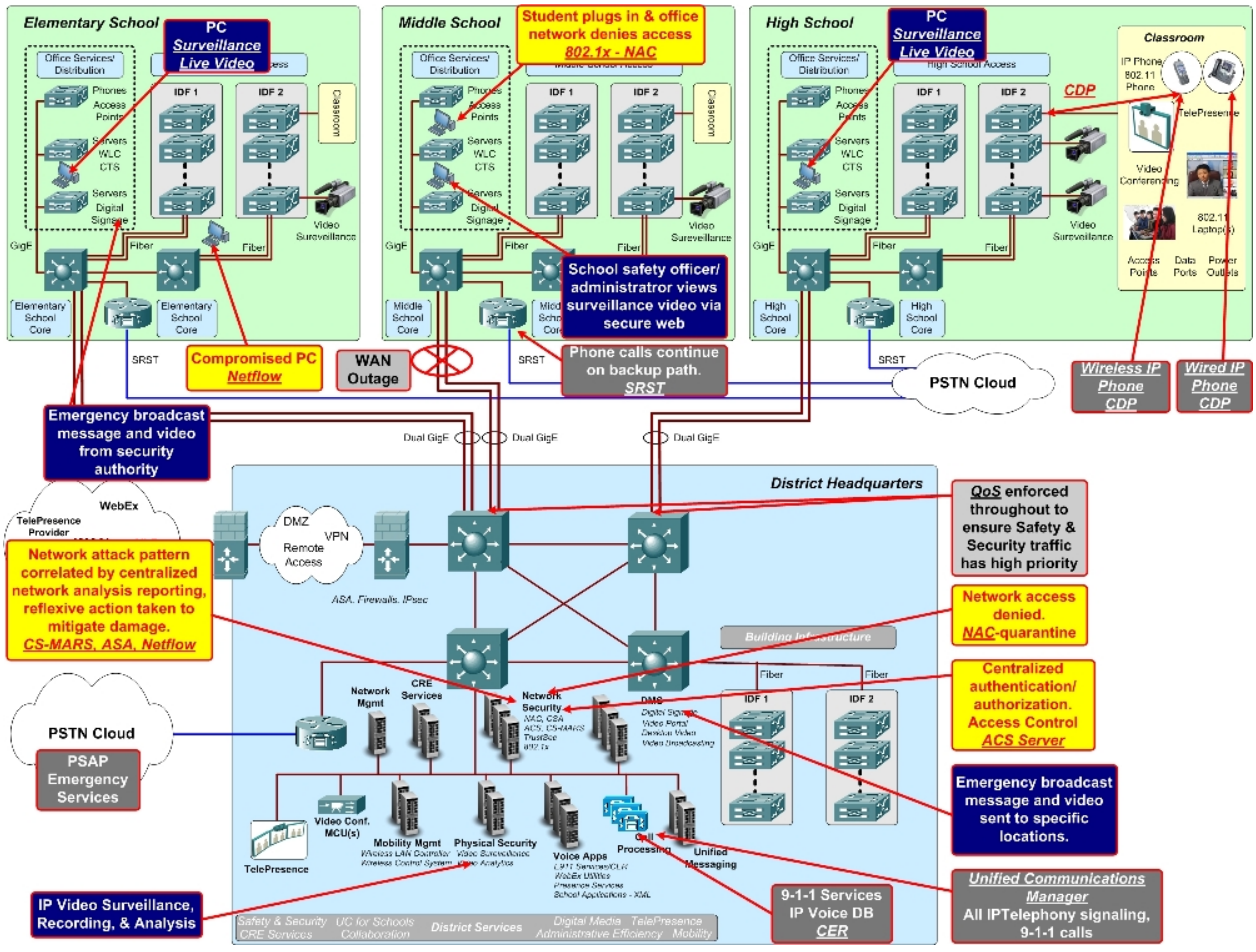
Cisco LAN Management Solution (LMS)

Authentication and Identity services

Safety and Security for Schools

A safe school employs the right tools to ensure the safety of the students, staff and faculty and responds immediately and effectively in the case of an incident. A safe school is a key differentiator for student and faculty recruitment, and is an integral part of the community which welcomes local citizens and contributes positively to the locality in which it resides.

Whether it is network security, video surveillance, video analytics, E911 services, unified communications applications, or a combination of these services, it is the convergence of these solutions that works for the greater good. It is not about the unification of security into one environment, but the collaboration between environments that promotes the success of safety and security solutions. The following diagram illustrates how key technologies for school safety and security are deployed and are utilized in the K-12 Reference Architecture.



Critical Technologies

Identity Management

As the number of network devices has increased in schools, the use of identity management techniques has become more common. There is now a desire to provide a mechanism to associate identities with the port of access to the LAN to establish authorized access. The IEEE 802.1x standard ties the Extensible Authentication Protocol (EAP) to both the wired and wireless LAN media and supports multiple authentication methods. 802.1x defines a generic framework that is able to use different authentication mechanisms without implementing these mechanisms outside the backend authentication infrastructure and client devices. 802.1x specifies a protocol framework between devices desiring access to a LAN (supplicants) and devices providing access to a LAN (authenticators).

Network Admission Control

Within the district and school environment, the protection of sensitive student and staff information is a top priority. Network admission control provides registration and enforcement utilities that allow a school or district's network administrators to authenticate, authorize, evaluate, and remediate users and their machines in a controlled environment prior to granting access to the network and internal resources, whether through wired or wireless access. Being able to deploy network admission control in out-of-band or in-band topologies allows flexibility in implementation, as well as the ability to address wireless and VPN access. Some of the key benefits of deploying a network admission control solution are:

- Multiple user groups can be addressed by defining roles and correlating them to areas of the network that they can access.
- Full network admission control features available for wireless networks and those users entering via VPN connections.
- Guest access, which provides control of how much they can access.
- Security and encryption for staff, can be specific areas only.
- CSSC as a client, free unlimited license supplicant for wired, encryption over wireless is licensed.
- Automatic security policy updates can be enforced throughout the district.
- Authentication and authorization with single-sign-on.

Centralized Access Control

Even with a relatively limited number of devices on the network to manage, maintaining robust access security on those devices over time is a challenge. Add various user groups, including teachers and hundreds or thousands of students, administrators, and guests, and the security challenge grows exponentially.

A centralized Access Control System from Cisco receives the requests from devices throughout the network, then goes to check credentials, clearances, authorizations, and posture. That means ACS has to interact with various external user databases (Microsoft AD or LDAP) and engines to come up with the right decision. ACS then registers the request and action taken and enforces it on the network device – allowing the right access to the right user. ACS is able to act on both user access policy and device administration policy.

Cisco Secure ACS supports both key device protocols required for identity and access control – RADIUS and TACACS+. This allows you to centralize access control in a single system. It has the interfaces to interoperate with existing identity and policy databases and systems to make multi-dimensional access policy decisions. It is not just a single server, it is a system that can be deployed and distributed as needed to meet availability, performance, and resiliency requirements. ACS provides the management tools and interfaces to manage deployments supporting large numbers of users and network devices, supporting large school districts and small. ACS reporting, alerting, and troubleshooting capabilities provide maximum visibility into authentication and authorization activities across the network.

The key products that create Centralized Access Control Services for schools:

- ACS and ACS SE, Multi-purpose ACS for Larger Districts (802.1x support, including EAP-TLS, Protected EAP (PEAP), and EAP-FAST
- ACS Express, Easy and Effective for Medium and Smaller Districts (up to 50 devices, 350 users)
- ACS View, Enhanced Reporting Engine

Web & E-Mail Content Filtering

IronPort solutions for web and e-mail filtering

Secure Remote Access by School Staff

- SSL-VPN teleworker access
- Web VPN/Client features, Cisco Integrated Security Features (CISF) integration (home drive)
- ASA (Web VPN), ACE Appliance (SSL offload, load-balancing)
- Can be Service Control Engine or NM-APA. Can detect encrypted p-to-p
- NBAR

Teacher, Lab, and Student Computer Security Agents

- Integration points – forcing connectivity to trusted wireless networks. Avoid client mis-association, unfiltered content.
- Host correlation, watch-list. Watch for attacks to multiple hosts, Network IPS can block access to host, signature-level tie-in.

Video Surveillance Cameras using IP, Unified Network Infrastructure

Districts and schools can leverage centralized digital network storage for the captured video, to review and analyze as required.

Wireless IP Video Surveillance

For areas of school facilities that are difficult or expensive to reach with network cabling, wireless IP-based surveillance cameras allow you to place cameras exactly where you need them. The wireless IP video cameras utilize the same mobile network infrastructure, which reduces expensive separate cabling and management.

Secure camera access to the wireless infrastructure is provided by mobility features such as WPA/WPA2-PSK, WPA/WPA2-Enterprise, and 802.1x. Network management security is important as well, utilizing HTTPS, IP Address Filtering, and User Access Rights to the cameras.

Outdoor Wireless Coverage & Local Law Enforcement Surveillance

One of many partnerships that schools create is with local law enforcement. One of the ways that mobile technologies can be utilized is with law enforcement vehicles that patrol near the school and respond in case of emergency. Using secure wireless video transmission with outdoor wireless coverage, schools today are delivering live IP-based video surveillance to mobile local law enforcement agency vehicles that can be several hundred feet away from the school. The enablement of outdoor mobile wireless services, along with mobile security features makes this possible in a secure manner.

Activation of Remote Video Cameras of IP Phones During Emergency

- Centralized activation and recording of specific events in real-time
- Remote phone off-hook capability to listen-in to specific locations, such as classrooms

Continuity of IP Voice Services

- Survivable remote site telephony (SRST)

Port Security – Cisco Integrated Security Features

The network switches that handle user access to the network, as well as wireless user access, are the source locations for attacks on the internal network. They are also the best place to protect the network. Specific features in the wireless network hardware and software can help prevent these types of common attacks:

- MAC flooding attacks
- DHCP rogue server attacks
- DHCP exhaustion attacks
- ARP spoofing attacks
- IP spoofing attacks

The Cisco Integrated Security Features (CISF), in conjunction with the Wireless LAN Controller, enables these preventative measures. Features such as Port Security, DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard are utilized at the network edge, to stop these attacks closest to the source.

Centralized Database Collection of Intelligent Device Events

Districts and schools can take advantage of information and event management appliances such as the Cisco Security Monitoring, Analysis, and Response System (CS-MARS). MARS provides real-time event collection, aggregation, and correlation to identify, manage, and counter security threats:

- Detects misbehaving network devices (Netflow)
- Sends signature control information dynamically to network elements
- Can send signature control information to wireless LAN controllers
- Collect Intrusion Prevention System (IPS) information
- Events from devices other than network components (SNMP traps, syslog)

MARS provides a powerful correlation engine that allows a district's network administrator to build rules and construct reports based on context correlation, then visualizing incidents while mitigating threats.

Connected Real Estate

Power Usage Monitor in Hardware

On a per-port and per-device basis, this is the ability to monitor Power over Ethernet usage by client devices, then to aggregate together for query by remote power management applications. Building Field Controllers can report information through the converged network, as well as receive secure instructions for operational changes.

With further enhancements, time-based power management is possible. Through per-port power conserving features in hardware, devices may be controlled automatically to conserve power during off-hours. The PoE MIB would be used to collect and interpret data from the access layer switches.

Smart Building Access

Provides schools with intelligence regarding who is entering school facilities and when. Additionally, smart building access can allow or limit access to parts of the district based of time of day, day of week, or close areas off when needed.

RFID Tracking and Reporting

RFID tags can be applied to high-cost school and district assets to deter theft, easily identify location of assets, and prevent misplacement. RFID tagging can also be used to monitor student and teacher movement through school and district facilities.

Intelligent Environmental Controls

Driving Green initiatives, intelligent climate and lighting controls enable districts and schools to optimize their use of energy and dramatically reduce energy consumption. Intelligent controls can reduce or power down environmental controls when building are not occupied.

Digital Building Systems

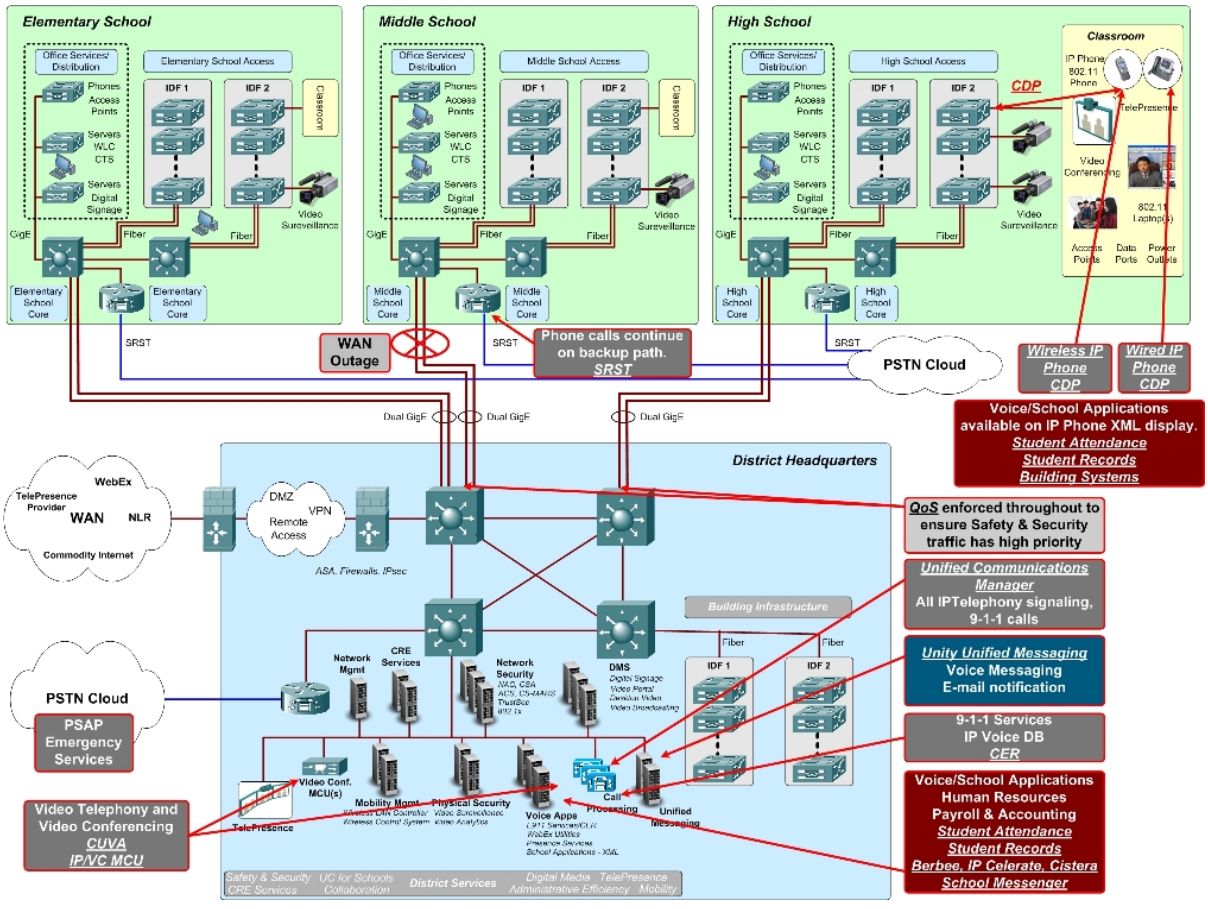
Merging building and IT systems over IP brings forth efficiencies and benefits that fully leverage the capabilities of network convergence:

- Optimized remote control, monitoring, and reporting of building systems, including centralized management of a distributed district infrastructure.
- Intelligent HVAC and lighting systems, resulting in reduced energy consumption costs.
- Improved safety and security – leveraging RFID tracking, IP video surveillance, intelligent building access, and integration to network security systems and notification services.
- Single cable plant deployment – compelling reductions in infrastructure cabling costs.

Unified Communications for Schools

Unified Communications is the delivery of fully integrated communications, by enabling data, voice, and video to be transmitted over a single network infrastructure using standards-based IP. Leveraging the K-12 Fabric and Reference Architecture, Cisco Unified Communications delivers innovative and integrated solutions that ensure that the district is communicating in the most effective and efficient manner possible. These IP-based communication services improve district-wide communications, safety, and productivity, while offering significant cost savings to optimize operational efficiency.

The illustration below depicts how Unified Communications services would be implemented in a school and district environment.



Critical Technologies

Quality of Service Enablement

Voice, video, and other real-time classes of IP network traffic have strict requirements concerning packet loss, delay, and the variations in delay (also known as jitter). To meet these requirements, the K-12 Fabric incorporates QoS features throughout its infrastructure to allow for the proper prioritization of real-time traffic, such as traffic classification, queuing, traffic shaping, compressed Real-Time Protocol (cRTP), and TCP header compression.

Intelligent Recognition and Management of End Device

As the variety of Power over Ethernet devices and capabilities increase over time (IP Phones, Access Points, Building Operations), the ability of the network to understand what is physically connected to the Ethernet ports becomes even more critical. Different devices draw different amounts of power, have different traffic profiles, and may have different VLANs associated to multiple functions.

The network hardware should be able to communicate with these devices, recognize them, and make the appropriate network modifications automatically to support the end-user.

Cisco Systems has implemented several enabling hardware and software technologies throughout the network that support seamless Unified Communications. Below are six key technologies. Upon connection of an Ethernet device in the school building, the Ethernet switch will automatically sense what kind of device it is, and apply the following functions automatically:

- Power – determine what kind of power the device needs, including PoE pre-standard or IEEE 802.3af, apply the power properly, then monitor power usage while connected and report power consumption to management tools.
- VLAN Association – determine what type of device is connected, then apply the proper VLAN policy to the device
- QoS enablement – enable QoS on the port to properly match the traffic profile of the device
- Trust Boundary – determine trust level for the device based upon the trust policies in force across the network, and put into effect immediately
- E911 Location detection – provide CDP information to the device, which allows it to register location to E911 location services (CER) on the network
- Auto Smartport (Target C1Q09, IP Base) – use custom macros to automate handling of device enablement

Enhanced 911 Location Service

As IP telephony devices relocate, it is critical that location information is tracked. This is done through correlation of device switch port location to a centralized database, which then when a 911 call is placed, sends the proper location information to the Emergency Services PSAP.

A key technology that enables this service is Cisco Discovery Protocol, or CDP. It is offered on Cisco routers, switches, access points, and other networking elements to communicate automatically with IP-enabled voice devices. This is a very important service to facilitate E911 location information.

Cisco Emergency Responder stores the database information about the network locations within your schools, and then automatically updates centralized device location information automatically. Backup CER servers are available.

Once CDP is enabled in your network, along with Cisco Emergency Responder, IP voice devices, including WiFI phones, can move from one school to another and update E911 location information automatically, without network administrator manual updates.

The features and products are:

- Cisco Emergency Responder Server
- Cisco Discovery Protocol (built into Cisco router, switch, endpoint software)

Unified Messaging

Receive voicemail, e-mail, and faxes in one inbox, and provide messaging capabilities that take advantage of text-to-speech functionality to provide access to messages via multiple methods. Unified messaging also provides mechanisms for a school and/or district to leverage its directory infrastructure to deliver messaging capabilities across the entire district.

UC Integrated Applications – Improving Productivity, Responsiveness, and Reducing Costs

Leverage the flexibility provided my XML applications that use the IP phone as a delivery endpoint:

- Student Attendance – take attendance, record absences, and send messages to the student's parents via Unified Messaging across the K-12 Fabric infrastructure.
- Real-time look-up of student records for medical information, data, and parent contact information.
- A single interface to reach emergency services – school or district-wide emergency messages, US Amber Alerts, weather/natural disasters notification, photo notification of on-site visitors, etc.

Remote Site Survivability

In a school district environment, survivable remote site telephony (SRST) allows the use of a centralized call-processing model, yet provisions for backup communications paths should there be a network failure across the WAN or MAN. Upon a WAN/MAN failure, the school IP Phones or gateway register to the SRST enable router which then provides telephony services for locally connected phones and PSTN voice modules.

- All Cisco IP Phones are supported.
- VG224, VG248, or ATA 180 Series can be used for analog devices.
- Flexibility of PSTN trunk choice – FXO, DID, T1/E1, BRI & PRI.

Wi-Fi & Dual-mode Telephony

Voice mobility brings down the communications barriers in schools and districts by allowing personnel to be reached virtually anywhere in the district, at virtually any time during operational hours. Wi-Fi enabled phones not only provide mobility in schools, but can be used within the entire district, leveraging the K-12 Fabric for a district or state-wide system to truly stay connected.

Additionally, dual-mode telephony allows the use of certain cellular devices in the district infrastructure, as Wi-Fi enabled phones, dramatically reducing communications costs for cellular air time and roaming fees. Again, leveraging the K-12 Fabric and district unified communications platform access to the IP Telephony infrastructure is provided via many endpoint options, increasing productivity and responsiveness.

Mobility

802.11n Wireless Capabilities

- Provides increased wireless capacity for high bandwidth applications, such as network video, 1-to-1 learning, and environments with network-based storage.
- Simultaneous support of a/b/g devices
- Gigabit Ethernet uplinks support
- PoE

Wireless IP Phones using School Wireless Infrastructure

- Key staff, such as support personnel, administrators, can carry wireless phones that share features with the wired IP phone system.
- Wireless IP phone capabilities are available district-wide.
- Reduces the need and use of cellular phones, which may have poor coverage and/or high usage costs.

WiFi Interference Monitoring and Rogue Detection

To reduce support time for the wireless infrastructure across multiple buildings, utilize access points to search the network for interfering rogue access points. These can come from a variety of sources, including neighboring facilities, homes, students, or staff-installed portable access points. When rogue wireless devices are detected, take network-based remote action to preserve the school's wireless network integrity.

- Live graphical map of building blueprints, identifying the location of rogue devices in the entire wireless environment.
- Enables RFID tracking and support.
- Combines with outdoor wireless coverage for asset tracking, sports facilities applications, wireless security systems, utility management

Centralized Wireless Access Point Configuration and Management

- WLAN Controller
- High availability features for redundancy and reliability

Closing Remarks – Moving Forward with the Blueprint

In closing, we envision this document to help form a methodology for developing the best practices required to ensure success in implementing the technology initiatives for 21st century learning. It highlights the key technologies and services that are most applicable to the K-12 environment and is designed to serve as a staging ground for developing specific architectures and solutions for Cisco's K-12 customer-base.

In addition to this document, future blueprints and reference architectures will be developed to address the technology services in more depth, to help optimize designs and configurations for our K-12 customers.