Cisco Notifi-Ed Solution for School Safety and Security Application Deployment Guide

Cisco Validated Design

May 15, 2009

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

About the Guide

This application deployment guide describes the benefits and features of the Cisco Notifi-Ed solution and details on how to implement the solution in a typical school district architecture. It explains the network architecture that was built in the lab to represent a typical school district and the testing performed to validate how the Cisco Notifi-Ed solution should be deployed on top of that network architecture.

Target Audience

The target users for this application deployment guide are school districts that want to use the Cisco Unified Communications for mission-critical services beyond basic IP telephony and sales engineers who are helping them plan and deploy these communications technologies and services. Some of these education accounts may also be focused specifically on improving safety and security for their staff and students by expediting communications through the school district and the parent community and minimizing response time during emergencies. It is assumed that the administrators of the Notifi-Ed solution have experience with installing the Cisco Unified Communications Manager and Cisco IP phones as well as basic configuration of Cisco routers and switches.

Other users of this guide include the following:

- Grant writers for schools
- Education customers with technical networking/telephony experience
- Channel partners and system integrators
- Superintendents and assistant superintendents of school districts, including assistant superintendent of administration, assistant superintendent of curriculum, and assistant superintendent of human resources

About the Authors

Karen Chan, Vertical Solutions Architect, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

Karen is an Education architect within the Industry Solutions Engineering group at Cisco. As a member of the Industry Solutions Engineering team, she has also worked as a Technical Marketing Engineer in Retail on the PCI for Retail solution as well as in Financial Services on the Digital Image Management solution. Prior to Cisco, Karen spent 11 years in software development and test.

Jenny Cai, Vertical Solutions Architect, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

Jenny currently works with the Industry Solutions Engineering team and is responsible for developing and validating education solutions. Since joining the team, she also worked on validating solutions for the Financial Services vertical. Prior to this group, Jenny worked on the Cisco 7600 series router.

Prior to Cisco, Jenny worked on a fault-tolerant server for the Financial Services industry while at Stratus Computer, and a continuous-feed printer for the oil industry while at Atlantek.

Solution Overview

Executive Summary

Schools today are expected to provide the highest level of safety and security to their student population as the community has become accustomed to hearing about violence and threats on school grounds—ranging from bomb threats to student shootings. Parents demand that school districts be prepared to respond effectively to such critical emergencies; therefore, it is ever more important for school districts to optimize their communication technologies in preparation for such disasters. As school districts plan to discontinue their legacy analog telephony systems and migrate to IP telephony, they are already looking ahead at what additional applications and network configurations they must add to their network to end up with a communications platform that is scalable, highly-available, automatable, and supports functions including voicemail, paging, bells/alarms, and announcement broadcasting. Whether it is to install IP telephony for the first time on their network or whether it is to evaluate the benefit of an upgrade to their existing system, school districts are first evaluating whether they can leverage their IP telephony network to deliver critical services to faculty and students before making major investments.

The Cisco Notifi-Ed solution for School Safety and Security is a Cisco Validated Design (CVD) that provides school districts with an integrated communications system for rapid mass and audience-specific message broadcasting. The solution demonstrates how the Cisco Unified Communications can be used by Reliance Communication's SchoolMessenger system and Singlewire's InformaCast product to deliver rapid communications to school administrators, teachers, students, and parents through audio, Register for Text Messages (SMS) text, and email and to receive and log acknowledgements from message

recipients, a critical function in emergency situations where school districts must be sure that parents have received announcements about the well-being of their children. The Cisco Notifi-Ed can be used to send emergency communication as well as daily operational announcements to the broader community that consists of parents, school district administrators, school faculty, students, and law enforcement.

The following are examples of how the Cisco Notifi-Ed solution can be used in non-emergency and emergency situations to give timely notification to teachers, students, and parents.

- There is a snow storm and school is cancelled. A recorded phone message and/or SMS is sent to every parent and/or student advising them about the school cancellation. An audible alert is also sent to every IP phone and IP speaker in the school in case students/staff have already arrived, or did not get the message.
- The principal receives an anonymous phone call with a bomb threat. He sends an audible message and text to every IP phone and every IP speaker in the school, advising everyone to initiate the evacuation plan immediately and that it is a real event and not a drill. Simultaneously, he sends recorded phone messages to all parents asking them to pick up their children immediately due to the bomb threat.

Target Market

The U.S. School 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 and heighten 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 nation-wide, the U.S. School 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.

In addition, given the opportunity to request one-time grants through newer programs such as economic stimulus funding and more traditional programs such as Erate, schools must be able to invest the one-time grants in technologies that will not require them to hire additional headcount for ongoing system maintenance. They must invest in technologies that are easy to deploy, manage, and scale.

Schools require a quick way to notify part or all of its parents and employees by telephone, and/or email, and/ or SMS, and/or in-school paging, in the event of an emergency and to place routine calls concerning local school meetings, attendance, and other announcements concerning school operations.

By partnering with SchoolMessenger and Singlewire, IT departments garner buying and funding dollars from other functions including:

- *Superintendent*—Needs to call parents for PR purposes, concerned about district image and compliance with federal requirements
- *Multiple Assistant Superintendents (Student Services, Safety, Facilities, MTO, Purchasing)*—Needs to call parents about absences, truancy, and emergency preparedness. Needs to streamline communication systems and achieve efficiencies/cost savings
- *Food Services/Child Nutrition Director*—Needs to call parents about low lunch balances, send reminders about free, and reduced lunch apps
- *Transportation Director*—Needs to call parents and staff for route changes, schedules, etc.
- *Public Relations*—Responsible for outreach and communication programs

These additional decision-makers, combined with increased cost savings for district's outreach programs helps IT departments secure the support they need to adopt new information technologies and deploy IP Telephony in the classroom for teachers.

Solution Description

Every day, the administrators and teachers of school districts strive to provide the best education possible to all students, in the safest environment possible. Unfortunately, many of the communication tools they use today hinder their productivity. Traditionally, school district's communications consist of inefficient paper-based practices, outdated phone systems—such as older PBX (private branch exchange), centrex, or key systems with limited features—site-based paging and auto-dial configurations, and analog speaker systems, all running on a network that does not support additional technologies like video surveillance and digital signage.

These discrete and outdated systems make it difficult for administrators, teachers, and staff to be productive and work efficiently. They may spend excessive time driving between locations, lose paperwork, and have to engage in sessions of phone tag—all of which can lead to frustration and job dissatisfaction. Plus, these outdated systems cost a significant amount of money to operate because they often require separate personnel to supervise and maintain. Worse yet, they might also have a more serious effect like delaying the response to an emergency situation and the broadcasting of information to the parent community.

The Cisco Notifi-Ed solution is designed to improve communications for school districts. By using the Cisco Unified Communications infrastructure and proven network designs, along with leading industry applications from partners Singlewire and SchoolMessenger, the Notifi-Ed solution provides a dynamic collaboration platform for safety and security as well as administrative efficiency, effective teaching, and next-generation learning.

Cisco Unified Communications Manager and IP Phones

The Cisco Unified Communications is a powerful, IP-based communications system that uses your existing data network to provide new, advanced communication services, such as voice, video, and web collaboration to help ensure that your district is communicating in the most effective and efficient manner possible. IP-based communication services improve district wide communications, safety, and productivity, all while offering significant cost savings.

The Cisco Unified IP phones are not like regular phones. They provide better communications, make schools and districts safer, and improve the business of education. They can be installed either with wired or wireless in classrooms, offices, and common areas. With IP phones, it is easy to:

- Improve communication with parents, who can leave voicemail for teachers and have more frequent conversations to discuss grades, attendance, behavior, and other student-related issues. Teachers and staff can automatically send parents voice and text messages with advanced outbound-calling services
- Enhance connections between district staff members, who can converse privately and access resources with the touch of a button. Plus, district staff members can easily see if a person is available and if they would like to be contacted via phone, email, or chat.
- Receive voicemail, E-mail, and faxes all from one inbox and providing advanced messaging capabilities where E-mails can be heard as voicemails or voicemails can be read as E-mails.
- Provide district-wide intercom paging, allowing classes to hear school announcements over IP-phone speakers and external loudspeakers.

- Enable district-wide broadcast messaging that allows office staff to record a message once and send it to multiple voicemail boxes and/or directly to phone displays.
- Deliver mobility with wireless IP phones and follow-me capabilities for administrators who need to stay connected and have access to vital information when they’re in locations outside the office.
- Give access to online directories so that teachers and district staff can easily contact people and get the services they need.
- Set up homework hotlines for students and parents to call and get details about assignments.

With a Cisco Unified IP phone in every classroom, it is easy for a teacher to get help if a problem occurs. There's no need to leave students unattended in order to contact another teacher or the office. Instead, teachers can simply place a call using their IP phones. In the event of an emergency, each teacher can access first responders with the touch of a button The support of wireless as well as wired IP phones allows mobility through the school grounds- particular useful in schools where security personnel roam the halls or where teachers move from classroom to classroom. With wireless IP phones, they can be certain to receive emergency notification wherever they might be and will be able to respond immediately by triggering a SchoolMessenger or InformaCast message broadcast.

The Notifi-Ed solution enhances safety by enabling staff to:

- Press a single button to reach emergency services.
- Deliver district wide emergency messages to parents and classrooms within minutes of a situation.
- Connect to the U.S.-based Amber Alert system and obtain notification of missing children in their state.
- Provide weather alerts, and other notifications to each Cisco Unified IP phone.
- Send photos of on-campus visitors to teachers.

Table 1 highlights the main features and benefits of the Notifi-Ed solution as well as the features and benefits of the partner applications Singlewire InformaCast and SchoolMessenger that are used in the solution.

Table 1 How Cisco Notifi-Ed Solutions Address Customer's Primary Challenges

Challenge	How Cisco Notifi-Ed Solutions Help
School safety and security	• Enables real-time communication between safety and security systems, networked data, and first responders • Helps maintain and disclose information about crime on or around campus
Antiquated infrastructure	• Replaces outdated equipment and integrates existing technology where possible • Offers flexible financing through Cisco Capital[SM]
Maximizing network and communication investments	• Eliminates costs of multiple, disparate systems • Scales easily as requirements evolve; provides a single, integrated communications platform
Manual/paper-based communications to parents, for administrative and emergency purposes	• Automates notifications (such as student absenteeism) • Sends vital information to digital signs
Truancy and related costs	• Creates next-generation learning environments • Improves participation and graduation rates by providing virtual tutoring and parent-teacher conferences

Whether communicating casual details like the time and location of a campus-wide assembly or notifying the educational community at large with evacuation instructions for a developing incident, you can use your existing data network to meet your needs. By adding the Cisco Unified Communications to your current IP network, you can provide:

- IP phones in every classroom and office
- Integration with public safety answering points
- Digital messaging and alerts to multiple communication devices
- Automated notifications to parents
- Broadcast messaging through a variety of notification modes
- One-touch access and single-number reach

Table 2 lists and describes the features for the partner products used in the Cisco Notifi-Ed solution.

Table 2 Cisco Notifi-Ed Solution Partner Products

Cisco Partner	Partner Specialty
SchoolMessenger	Leading automated notification system for schools, featuring: • Outbound calls over the PSTN • Centralized management; easy moves and changes • Configuration of messages for: – Absentee notification – General announcements – Emergency situations – Homework and test information – Low lunch balance reminders • Appliance and hosted options • Execute jobs through a web browser, IP phone, cell phone, or land-line • Advanced text-to-speech and instant language translation
Singlewire	Innovative InformaCast application for integrated paging, bells, alarms, and text alerts/messages; includes external speaker solution; also has a panic button for emergency notification. Singlewire InformaCast allows organizations to: • Simultaneously push audio streams and text messages to IP phones, IP speakers, desktops, and overhead paging systems • Create live, ad-hoc, or prerecorded audio broadcasts and/or text broadcasts • Schedule messages to send at preset time or on recurring basis • Use Bell Scheduler's calendar format for campuses or districts • Integrate IP speakers to provide indoor/outdoor loudspeaker option

For further information about the Cisco Unified Communications, refer to the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html

Solution Components Overview

Rapid communications for mass or audience-specific notification is delivered in Notifi-Ed through the integration of the following Cisco Unified Communications products and Cisco Technology Partner products:

- Cisco Unified Communications Manager 7.0
- Cisco 7941G, 7906, 7960G, and 7971G wired IP phones and Cisco 7921G wireless IP phones
- SchoolMessenger Flex Appliance, SaAS
- Singlewire InformaCast 6.1
- Atlas IP speakers

The Notifi-Ed solution was validated in a representative school district network that was based on the Schools Service-Ready Architecture. The Schools Service-Ready architecture was defined by the Cisco Education System and Campus Enterprise Solutions Engineers working in collaboration to identify the network infrastructure and the application-enabling network services that make up a typical school architecture.

This school district network built in the lab consisted of the following technologies and components:

- Cisco Unified Wireless 1250 and 1140 Wireless Access Points
- Cisco 4400 Wireless LAN Controller
- Three Catalyst 3750 Stackwise Plus Core switches at the school site
  - Stateful Failover
  - Non-stop Forwarding (NSF)
  - Etherchannel
- Catalyst 3750 access switches
  - VLAN segmentation of control traffic, voice traffic, and other data traffic
  - Layer-3 access
- Catalyst 4507 Core at the district office
  - Stateful Failover (SSO)
  - Non-stop Forwarding (NSF)
- Cisco 3845 Integrated Services Router at the school and district office
  - Survivable Remote Site Telephony (SRST)
  - Voice Gateway for PSTN Connectivity

Solution Features and Benefits

The Notifi-Ed solution provides school districts with a message notification system that is easy to deploy, centralized at the district office, remotely manageable, scalable, and highly-available.

Most school districts with legacy systems run separate paging, bell, and clock systems at each school in the district. There is no way to update these systems or centrally manage any of them. Changes to clocks, paging zones, or bell schedules require a site visit by someone in the Facilities department or a paid contractor. The system cannot be updated without buying a new system.

The InformaCast centrally manages all paging, bells, and clocks. There is no limit to the number of zones or the size of the zones. Clocks are always accurate and changes to bell schedules can be made by any authorized person from anywhere, so that facilities personnel are no longer required to go to the physical location of the clocks and bells to check the status of the unit or make adjustments to parameters like volume. For new construction, the InformaCast and IP speakers are 50 percent of the cost of an analog system. Since the system is software-based, it can be updated over time. In addition, the IP speakers support Power-over- Ethernet (PoE), providing significant cost savings during deployment as additional electrical wiring is not required.

Similarly, the SchoolMessenger Flex Appliance is deployed centrally at the district office and provides message notification services to all the school locations in that district.

The followin are common questions that come up when discussing centralizing services on a location such as the district office:

Q. What happens if the WAN goes down?

Q. Will each branch location still be able to continue running with their mission-critical applications?

The Cisco Unified Communications is designed to continue operating at a school branch during a WAN outage if Survivable Remote Site Telephony (SRST) is configured on the Integrated Services Router (ISR) deployed at that branch. SRST continues to service IP phones on the LAN when the centrally-deployed Cisco Unified Communications Manager (CUCM) is unreachable and management of IP phones will fall back to the CUCM once the WAN is back up. The SchoolMessenger system is designed to continue providing district-wide and remote message notification services during a WAN outage by sending out mass or audience-specific message notification over the PSTN from the SchoolMessenger-hosted service. During a WAN outage, a user at a school branch can still continue to configure SchoolMessenger jobs through the IVR interface that is accessible from any land-line phone or cell phone. The SchoolMessenger Flex Appliance at the district office works with the hosted service at the SchoolMessenger data center under normal operations when the WAN is available to offload calls to the hosted service as needed.

Many schools have been using PBX or Centrex systems in their districts for traditional "tone" services. IT departments in schools are looking for a more comprehensive business case to justify the migration to IP-based phone services and are investing in applications that provide functionality, cost savings, and benefit to the district beyond their existing systems. The Notifi-Ed solution offers the flexibility and scalability of the Service-Ready Architecture for schools with the integration of partner applications capabilities to address scalability, application, and storage performance challenges with advanced networking, internal and external messaging, and communications technologies. This end-to-end education architecture solution improves messaging best practices and provides the field and partners confidence in partnered messaging applications. Cisco, as a solution provider for unified communications and messaging, provides the most comprehensive messaging solution available in the market today. Combining a proven communications infrastructure with integrated speaker paging, desktop phone visual and audible announcements, SMS text, and automated out-dial announcement and response, Cisco provides an end-to-end solution architecture for enabling additional communication and messaging solutions.

The Notifi-Ed solution supports user workflows that allow school administrators at the district office to make district-wide announcements to all their schools at the touch of a button. The announcements can be pre-recorded to minimize response time for urgent situations such as bomb or gun threats on campus where immediate actions like evacuation are necessary. The announcements can be ad-hoc to allow for the flexibility of spontaneous announcements to suit the situation. Both pre-recorded and ad-hoc messages can also be sent from any school location out to other school sites and the district office.

Both the InformaCast and the SchoolMessenger applications can be managed through a web browser and they both have the added benefit of allowing users to configure and execute jobs from any IP phone that has been minimally configured with that support. Both applications can be integrated together via their SOAP API so that the InformaCast server can be configured to trigger a pre-configured SchoolMessenger job when an InformaCast job is executed. This allows users to send out mass notification to students and faculty on-site as well as parents, students, and staff who are remote all at the same time. This function is especially critical in emergency situations where a large number of people, local or remote, must be notified immediately.

Scope of the Solution

The overall scope of the Notifi-Ed solution is to provide an end-to-end solution architecture for a centralized, highly-available, easily-deployable message notification system that supports both audience-targeted communication as well as mass notification. The solution supports both message notification for daily operations common in a school district as well as emergency notification to students, faculty, parents, and the general public.

The solution includes deployment and configuration of Cisco Unified Communications Manager, IP phones, SchoolMessenger and Singlewire InformaCast services running on top of a network infrastructure that follows the best practices of the Service-Ready Architecture for Schools.

The following network services from the Service-Ready Architecture for Schools falls within the scope of this solution:

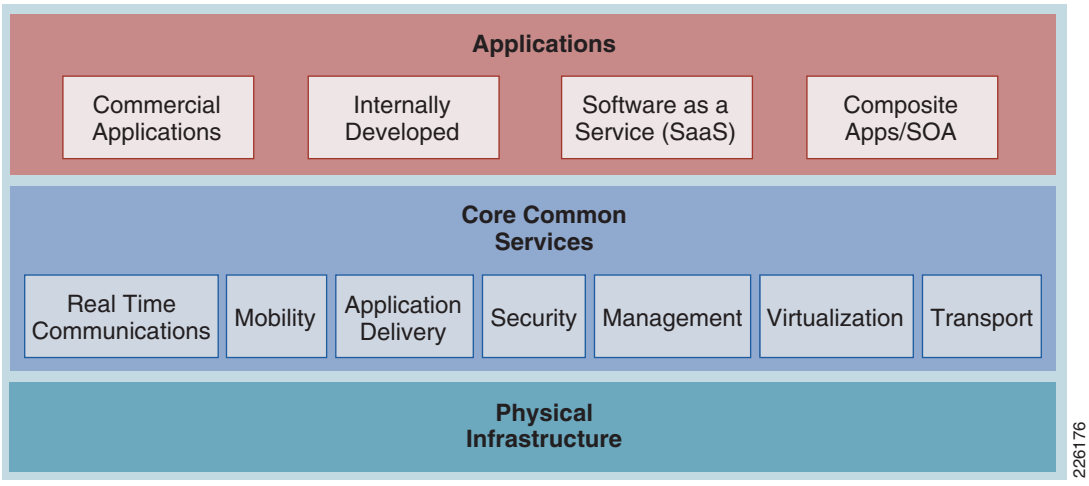
- Multicast support
- Quality of Service (QoS)
- High availability
- Cisco Unified Communications deployment best practices

The devices used in this solution represent what was required to perform functional testing. The implementation of this solution requires proper sizing of the various devices based on the individual needs of the customer.

Solution Architecture Framework

The Cisco Services-Oriented Network Architecture (SONA) framework provides a standard paradigm for designing current and next generation solutions that link network-based services with enterprise applications to drive business results. The SONA framework (see Figure 1) illustrates the components of the solution from the infrastructure providing network-based services and the applications that consume them.

Figure 1 SONA Framework



The following is a brief description of the different layers of this architectural framework:

- *Applications*—This layer represents the mission-critical applications commonly found in school environments, as well as applications that school environments will need to keep up with the evolving requirements of next-generation schools. The integration of Cisco Unified Communications with Singlewire InformaCast and SchoolMessenger form this application layer of the framework.
- *Core Common Services* —This layer represents application-enabling network services, some of which may need to be integrated with each other to support application requirements. For the CIsco Notifi-Ed, this includes mobility, security, and QoS.
- *Physical Infrastructure*—This layer represents the network architectures, typically based on the Cisco Validated Designs (CVDs) that are used in the solution. For the Cisco Notifi-Ed solution, this includes the school site and the district office network that are based on the Schools Service-Ready Architecture shown in Figure 2 below.

The Cisco Notifi-Ed solution is built using the architectural framework shown in Figure 1, enabling the solution to be developed with the appropriate supporting applications, network services, and network systems. Following this framework ensures that network services are properly integrated to meet the solution requirements. In addition, the framework facilitates the expansion of the solution scope—if applications should be added to the solution moving forward, it will be clear what additional network services and network systems need to be added to support the additional functional requirements.

The design of the Cisco Notifi-Ed solution on such an architectural framework supports the addition of other mission-critical applications and systems that are needed to address the increasing business demands of school districts in the areas of administrative efficiency, safety and security, and next generation learning.

Solution Network Architecture

The network and network services architecture for this solution is based on the design of the School Service-Ready Architecture (see Figure 2).

Figure 2 Service Ready Architecture for Schools

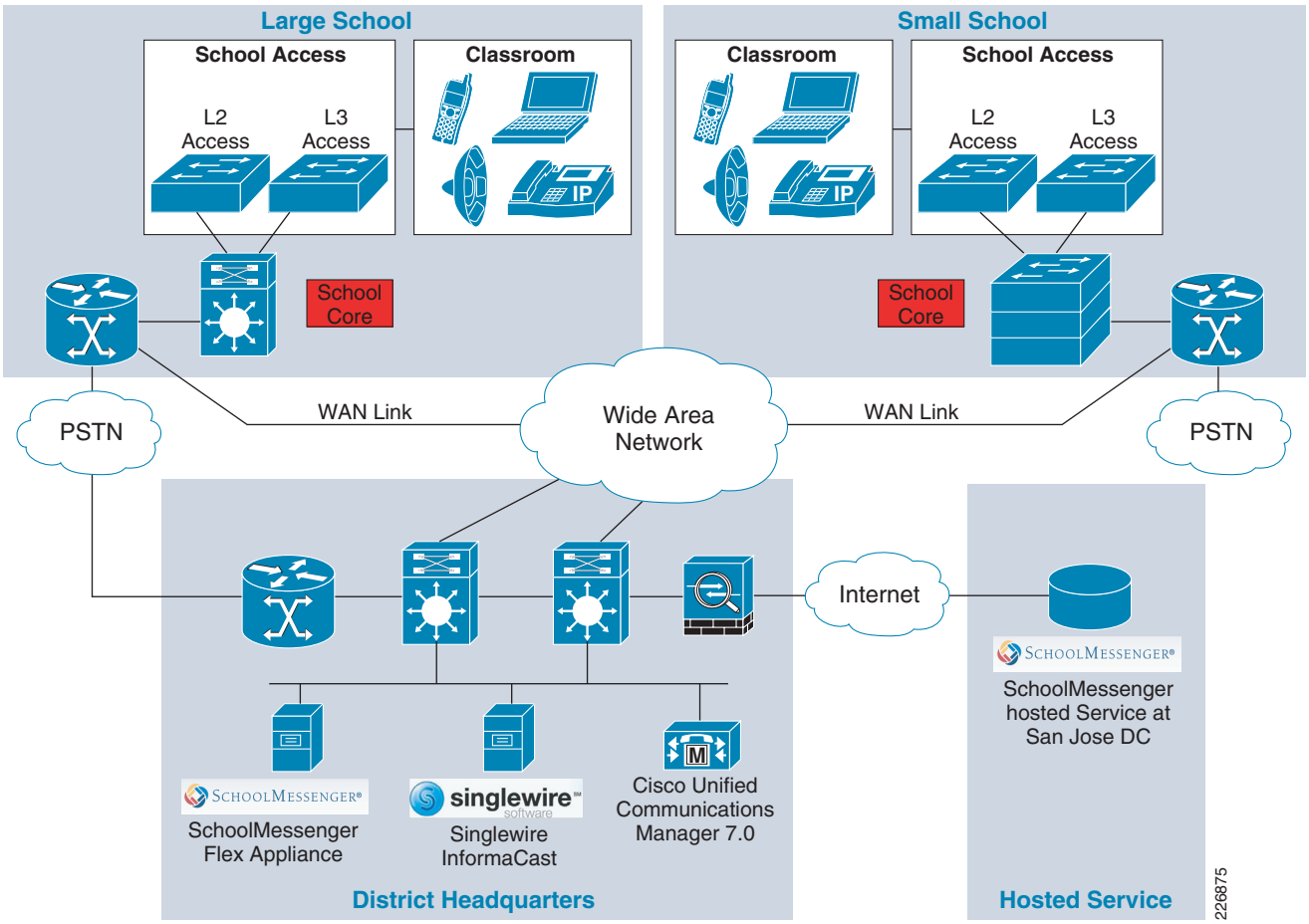


Figure 2 shows the architectural framework for delivering mission-critical services to school and district environments, all on a single network fabric. It can be scaled up or down based on the sizing, bandwidth, and budgetary requirements of the school district. It provides options and best practices for high availability, redundancy, QoS, mobility, and security and enables Unified Communications, Video Surveillance, Digital Media Systems, and other technologies that are key to transforming school districts into next-generation education environments that optimize the academic experience for its students, operate efficiently and save on administrative cost, and protect their student and faculty with the highest level of safety and security.

The Service Ready Architecture for Schools is designed to meet the following requirements of a next-generation education network:

- 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 onset of new services to the network

Integrate these new services and technical innovations with existing network equipment, protocols, and methods of communication.

The architecture was therefore designed to deliver the network technologies key to satisfying the objectives above:

- *High availability*—The high availability technologies used in the Service Ready Architecture for Schools allow network equipment to mitigate 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 sharing 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 used. In the education environment, this is important especially as schools struggle with allowing student access on the same network that is used for grading systems, safety and security, and phone conversations.
- *Differentiated services*—Certain network services demand more from the network than others. As an 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 to make decisions as to 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 their 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 the need of 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. In addition, reconvergence times for the end-to-end network can be reduced to 1 second or less and are more predictable now that spanning-tree is eliminated. Also, redundant uplinks can be fully used—without the need for Hot Standby Router Protocol/Virtual Router Redundancy Protocol (HSRP/VRRP), thereby simplifying configuration, management, and troubleshooting.

Solution Services

Security Services

The district office in the Notifi-Ed solution includes an Internet connection that provides the SchoolMessenger Flex Appliance connectivity to the hosted SchoolMessenger services at the corporate data centers located in San Jose and Minneapolis. Perimeter security against potential attacks from the public connection at the district office is provided by the Adaptive Security Appliance (ASA). While security and penetration testing falls outside the scope of this solution, the features and best practices offered by the ASA can be implemented with the Notifi-Ed solution to secure the district office Internet connection.

In particular, the ASA can be configured as a stateful firewall, VPN concentrator, and as an intrusion detection and prevention (IDS/IPS) appliance to handle Internet connections securely. The security appliance combines the above functionalities in one device; on some models, the intrusion detection and prevention is delivered on an AIP-SSM module that plugs into the ASA. Multiple security contexts (similar to virtualized firewalls), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, access-control lists (ACLs), and Network Address Translation (NAT), and IPSec or webVPN support are just a few of the features offered.

In deploying the ASA as the Internet firewall at the district office, be sure that TCP port 443 for HTTPS traffic is left open to allow for inbound communication from the SchoolMessenger-hosted service to the Flex Appliance at the district office. In addition, follow these best practices to allow the network to leverage its security features more effectively:

- The ASA can be configured easily using the Adaptive Security Appliance Device Manager (ASDM) graphical interface. While the command-line interface is available, the ASDM interface groups the different feature configurations (for example, firewall, VPN, and device access parameters) into their own GUI pages and the flow of configuration is more intuitive.
- The network interfaces on the ASA are designated in the GUI as *inside* and *outside*. The *inside* interface should be connected to the more secure network. For example, the district office, including the demilitarized zone (DMZ), if available, behind the firewall while the *outside* interface would be on the Internet side. The ASA requires a numerical security-level to be assigned to each interface; the inside (more secure) interface should always be given a value higher than the outside (Internet-facing) interface. By default, the ASA is configured to allow traffic to flow freely from a higher security level to a lower one.
- For specific inbound flows that are permitted, including the HTTPS over port 443 communication that happens between the SchoolMessenger Flex Appliance at the district office and the SchoolMessenger servers at SchoolMessenger's SaaS data center, specific ACLs that allow the traffic through the firewall but that are as specific as possible. If a specific host address can be used for the ACL instead of a broader subnet, it is best practice to do so for increased security.
- For all traffic not explicitly permitted through by the other ACL entries, create a default **deny all** ACL entry at the bottom of each ACL. Enable ACL logging.
- If using IDS/IPS on the ASA, it is important to keep the number of signatures updated to thwart the latest attacks.
- It is important to secure the ASA itself since a compromise of the device means a compromise to the network. All management access to the ASA should be secure—HTTPS instead of HTTP and SSH instead of Telnet. Non-default accounts and strong passwords should be used. Idle console session timeouts should be configured and too many retry attempts to login should result in an account lockout.

- Best practice also includes configuring the ASA to generate syslog events to an external server so that events including configuration changes, unauthorized access attempts, and IDS events can be logged and audited.

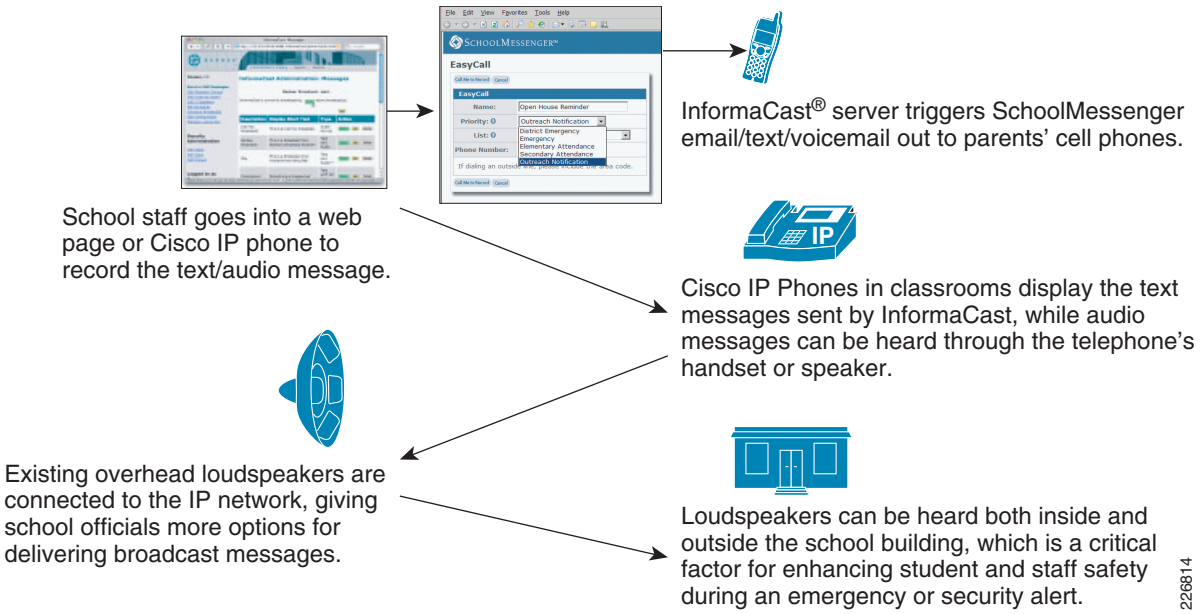
Central Management of Solution Components

In a real-world deployment, the number of school branches that must be considered could range from a few to more than a hundred, for the larger school districts. As the number of network infrastructure devices including routers, switches, and wireless access points scale, it is important to implement a central management scheme that supports easy deployment of new configurations and features, supports rapid upgrades, and allows network and system administrators to monitor the health of their network. Broadly, the central management that applies to this solution can be categorized as network management (for example, configuring and maintaining Layer-2 and Layer-3 configurations) and security management (for example, configuring and maintaining ACLs, firewall rules, and IDS/IPS rules). For suggestions of products that can be used for centralized network and security management, refer to "Appendices" section on page 36.

Designing the Solution

Figure 3 shows the user workflow supported by the Notifi-Ed solution, whether the user is physically located at the district office or at a school location.

Figure 3 Solution Work Flow



Survivable Remote Site Telephony (SRST)

SRST is configured on the voice gateway ISR in the school site. SRST provides the central CUCM functionality within the local network in the event that the WAN link is down and communication with the CUCM server at the district office is lost. SRST comprises network intelligence integrated into the Cisco IOS Software, which acts as the call processing engine for IP phones located in the school branch during a WAN outage. This solution did not require any additional SRST configuration beyond the standard configuration that is documented in the *Cisco Unified Survivable Remote Site Telephone Configuration Guide* at at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html

High Availability Considerations

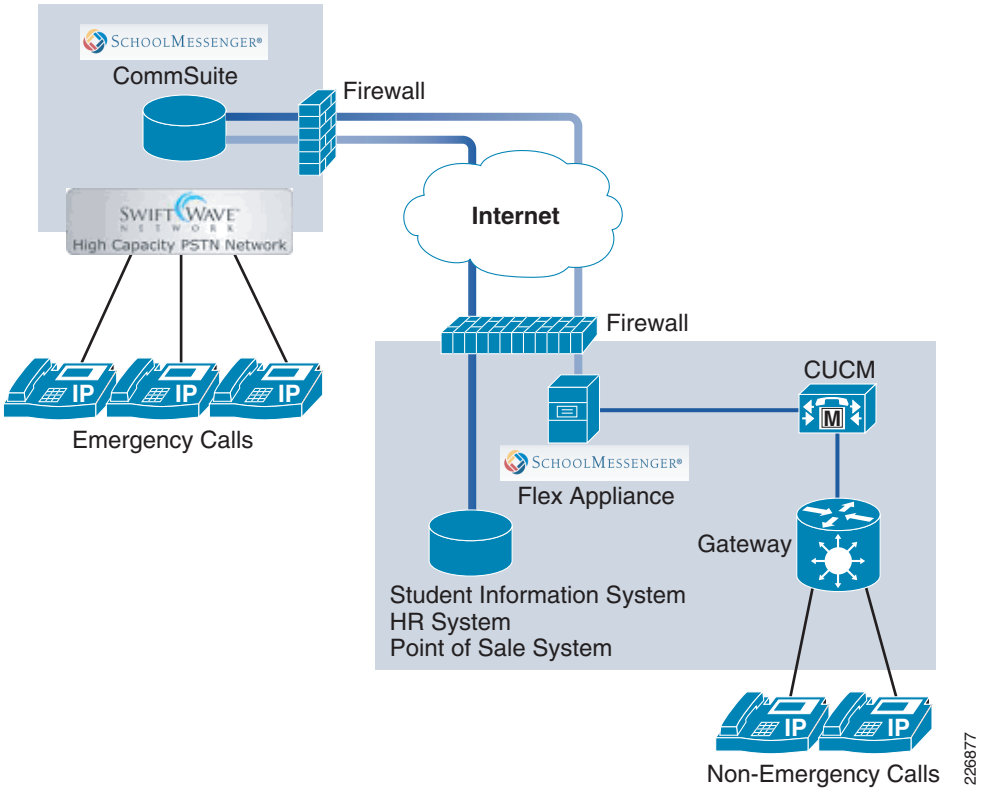
The goal of a highly-available system is to minimize network and system downtime during a failure in the network. While redundant components and redundant paths in the LAN were included in the solution, redundant WAN links at the school site was not included in this solution because school districts are not likely to invest in a secondary WAN link given that ERATE funding, which is the school districts' primary source of funding for technology, does not cover that expense. As a result, in addition to leveraging the SRST function available in the ISR, this solution relies on the application survivability that is built into the partner application deployments.

Application Survivability

While school districts are typically unwilling to invest in a secondary WAN link for each of their school locations, they still require that mission-critical services are resilient to network outages. It is important that any application features that provide application redundancy and survivability are used in this solution to deliver that resilience. Both SchoolMessenger and InformaCast can be configured to deliver continuing application services during a WAN outage between the school district and school branches.

SchoolMessenger Services

Figure 4 SchoolMessenger Services



Non-Emergency Calls

When a call job is submitted, whether using the web interface, the IP phone interface or the IVR phone interface, the application processes the job request and sends the calls to be processed to the Flex Appliance system. The necessary data is securely transferred using industry standard SSL encryption. Upon receiving the necessary data required to place a call, the Flex Appliance system places the outbound dial request through CUCM via SIP trunk. The results of each call (for example, answered, busy, no answer, etc.) are then sent back to the user account where they can be accessed in real-time. Depending on the call result and the user's account settings, the undelivered messages will be retried at certain intervals.

Emergency Calls

From an end-user's perspective, the steps for sending an emergency call notification are exactly the same as those for sending a non-emergency notification. The only difference is that the job type is specified as an emergency when the job is created. In this case, the system does not attempt to process the calls through the Flex Appliance system; instead all calls are routed through the much larger capacity of the SwiftWave network.

In the case of a WAN outage at at the school district office, all calls (both emergency and non-emergency) can be configured to route through the SwiftWave network; thus, bypassing the need to communicate with the Flex Appliance until the network outage has been resolved.

InformaCast Services

During a WAN outage at the school branch, InformaCast multicasting to IP phones will no longer function. The SchoolMessenger needs to be used in this case. While InformaCast multicasting to the local IP speakers also no longer functions, a software package called *PageKom* can be installed at the local site to enable manual paging to IP speakers while WAN connectivity is unavailable. PageKom is free software available for download from Singlewire. For more information, refer to the *PageKom User Guide* at the following URL:

http://phone-xml.Singlewire.com/iptel/download/PageKom/

PageKom uses an Analog Telephone Adapter (ATA) with a traditional analog handset connected to this ATA. An FXS port off of the Grandstream ATA would be configured to provide dial tone while the network connection, if available, on the local network. The software would reside on a server (potentially a local file and print server) at a local site to the IP speakers, but remotely from the centralized InformaCast server. Currently, the use of a Cisco ATA186 one or two-port adapter or a Grandstream ATA is recommended due to the ability to meet the requirements of Section 3.10 in RFC 2833 which describes the encoding for DTMF events.

Additional information about the Grandstream ATA's can be found at the following URL:

http://www.grandstream.com/ata.html

Additional information about RFC 2833 can be found at the following URL:

http://www.faqs.org/rfcs/rfc2833.html

The basic scenario in this model is that the WAN connection between the centralized InformaCast site and the remote site hosting IP speakers has been lost. The need for paging exists and the use of a single handset is recommended for live audio paging. The ability to page to Cisco IP phones will be lost and additional features in InformaCast like pre-recorded messages and the Bell Scheduler will not be available as this is strictly live audio paging to IP speakers. The software has the ability to do zone management to separate IP speakers.

Implementing the Solution

This section explains the implementation of the Notifi-Ed solution, provides relevant configuration, and lists reference documents. The Notifi-Ed solution provides a convenient way to notify multiple people. For example, it frees a teacher from tedious tasks to notify a large number of students, staff, and parents.

The essence of this solution is to make the following three applications work together in a Service Ready School Architecture:

- Cisco Unified Communications
- SchoolMessenger
- Singlewire InformaCast

Solution Components

The solution components required for Cisco Notifi-Ed solution span across several key technologies. These technologies, ranging from routing and switching to the Unified Communications and partner application endpoints, are deployed at different locations in the school district network and address the

requirements to improve communication flow between school sites, the school district office, and the parent community. Figure 5 shows an overview of the placement of these technologies in the school district network.

Figure 5 Placement of Technologies in the Notifi-Ed Solution

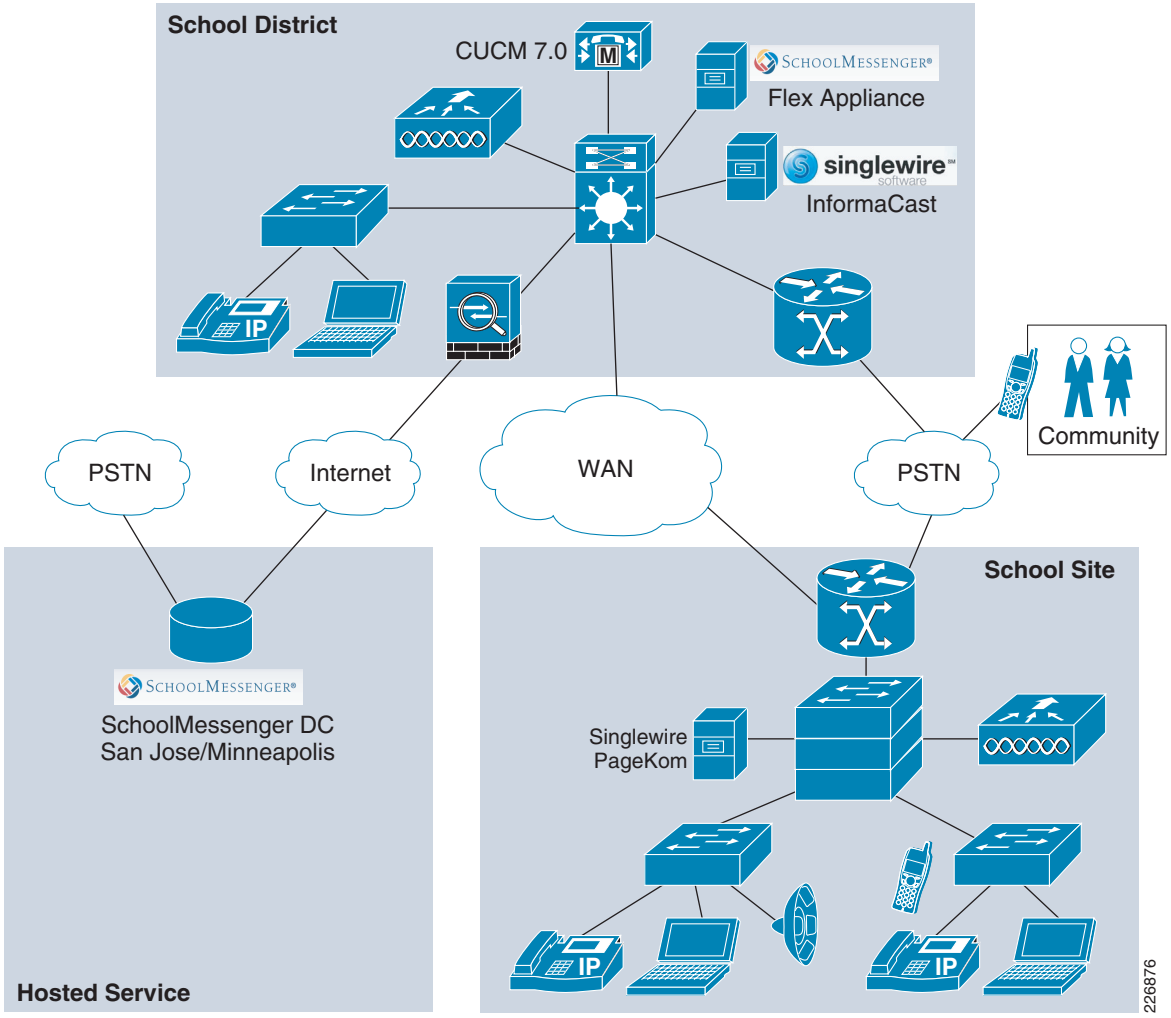


Table 3 to Table 5 list the different components and versions tested in this release of the Notifi-Ed solution.

School District Components

Table 3 District Office Components

Component	Description	Lab Configuration
Cisco Catalyst 4507-E	Core router	cat4500e-entservicesk9-mz.122-50.SG1.bin
SupV1-10GE (Qty : 2)	Catalyst 4507-E Supervisor Engine with 10GE	Not Applicable
WS-X4524-GB-RJ45V	Gigabit Ethernet line card	Not Applicable
Cisco 3845	3845 Integrated Services Router	c3845-adventerprisek9-mz.124-11.T2.bin
CUCM	Cisco Unified Communications Manager v7.0	System version 7.0.1.11000-3

School Branch Components

Table 4 School Branch Components

Component	Description	Lab Configuration
Catalyst 3750-E (Qty: 3)	Stacked core	c3750e-universalk9-mz.122-50.SE1.bin
Cisco 3825	Cisco Integrated Services Router (ISR)	c3825-advipservicesk9-mz.124-15.T1.bin
AIR-WLC4402-12-K9	4402 Wireless LAN Controller	5.2.178.0
SP-ATLAS-I8S	Atlas Indoor IP speaker	Not Applicable
Cisco 7971, 7960, 7941, 7906, and 7921 IP phones	Cisco Wired and Wireless IP Phones	

Partner Components

Table 5 Partner Components

Component	Recommended	Lab Configuration
SchoolMessenger Flex Appliance 2009-02-16 22:22:43 (with hosted CommSuite v6.2)	Quad Core Xeon Processor2x6MB Cache, 2.0GHz,2GB memory Dual 73GB 15K RPM Serial-Attach SCSI Drive, RAID 1 No Operating System Required (See http://www.schoolmessenger.com/8973452/docs/ for exact hardware specifications)	Cisco 7845 2 x dual core Xeon 3.4Ghz processors 3.5 GB memory 70GB Disk (Raid 5)
Singlewire InformaCast v6.1	Two-way 32-bit Intel Xeon 3.0 GHz Dual-core 2 GB memory RAID 1: Two 72 GB disk drives Windows Server 2003 Version 5.2	Cisco 7845 2 x Dual core Xeon 3.4Ghz processors 3.5 GB memory 70GB disk (Raid 5)

Implementation Considerations

When implementing this solution, it is vital to consider the characteristics of an organization, the network from the perspective of services, locations to add new components, and implementation sequences. This subsection discusses each of these areas.

Unlike private schools, public schools are unified into a school district according to geographic area. This provides economy of scale as services can be installed in a district office and shared by schools within this district. A district office often physically resides with one of its schools. For example, Milpitas Unified School District (in Milpitas, California) has 14 schools (9 elementary schools, 2 middle schools, 2 high schools, and 1 adult education). The Milpitas district office resides at the same location as the adult education school. This results in similarity between the network for a district office and the network for a school, as both support many end devices such as phones and computers.

Network provides services, such as security, wireless, multicast, and QoS. The services that the network can provide are more important than the actual topology or routers/switches deployed. The Cisco Notifi-Ed solution uses multiple services provided by the network. When the network topology changes and routers/switches are replaced, the solution will work fine as long as the set of services are provided by the network.

In this solution, a CUCM server, a SchoolMessenger server, and an InformaCast server were installed at the district office. The services provided by these applications are shared among all the schools in the district. Phones and IP speakers were installed at schools as well as at the district office since a district office often has a school at its location. See Figure 5 for location of application servers and IP devices.

In lab testing, the solution was implemented in following sequence:

1. Implemented the Cisco Unified Communications (UC)
2. Tested the SchoolMessenger and UC.

3. Tested InformaCast and UC: Integrated InformaCast and SchoolMessenger

Cisco Unified Communications (UC)

With the Cisco UC, all schools are able to call each other over the IP network as well as able to dial 9 to get out the PSTN. In the lab testing, the following setup was used: one CUCM residing in a district office, one ISR at each school, and various types of phones at the district office and schools. The ISR at each school acts as voice gateway in case the school cannot access each CUCM due to WAN connection failure or CUCM failure.

Whether on the same LAN on not, any phone can register to a CUCM as long as it can reach the CUCM over the network. Except for the regional/location-specific parameters for adding a phone, the procedure on CUCM is essentially the same whether the phone is in the district office (same LAN as the CUCM) or at a school (different LAN as the CUCM).

The following is a sample configuration of the port that connects to a phone:

```
interface GigabitEthernet1/0/34
 switchport access vlan 48
 switchport mode access
 switchport voice vlan 49
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 queue-set 2
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoQoS-Police-CiscoPhone
 ip dhcp snooping limit rate 100
end
```

The configuration of a CUCM is typically done by an UC technician. In a district office or a school, a common scenario is the need to add an additional phone. This can be accomplished through following steps:

Step 1 Connect the phone to the access layer switch to which existing phones connect. Configure the interface that the phone connects to.

Step 2 If this phone has been used with other CUCM, it is best to erase the phone settings associated with another CUCM.

Step 3 CUCM assigns an extension to the phone. If desired, modify CUCM to assign a different extension number to the phone.

SchoolMessenger

Once the Cisco Unified Communications is working, the next step is to bring a SchoolMessenger server into the district office network. The SchoolMessenger server automates repetitive and tedious tasks as well as supports the execution of a high volume tasks. For example, when a teacher wants to notify parents about a problem at the school (such as a breakage in the water main) or remind parents of upcoming events (such as various state and federal upcoming student testing), he or she only needs to record a message and decide to which pre-defined group of recipients to send the message. The SchoolMessenger makes the calls.

The SchoolMessenger can be deployed in the following three ways:

- *Fully-hosted*—In the fully-hosted model, the entire application is located in the SchoolMessenger data center. There is no hardware or software at the customer site. This is not selected due to high cost.
- *Standalone local server-based*—In the standalone model, the entire application is located in the district office. This is not selected due to insufficient call capacity and limited high availability in emergency situations.
- *Hybrid*—The hybrid model consists of SchoolMessenger-hosted notification service (CommSuite) and the SchoolMessenger Flex Appliance. Only the SchoolMessenger Flex Appliance is physically located at the customer site—the district office. This model provides high availability for emergency notification while benefiting from the low cost of a local server for non-emergency situations. The CommSuite-hosted service and the SchoolMessenger Flex Appliance are like a decision maker and an assistant. The decision maker handles critical tasks directly and assign non-critical tasks to the assistant.

For the Notifi-Ed solution, the hybrid model is implemented, which is the more popular deployment model. The hybrid model can be considered as a combination of a fully-hosted system during an emergency and a standalone system for non-emergency (see Figure 4).

Because the SchoolMessenger Flex Appliance places calls through CUCM through a SIP trunk, a SIP trunk needs to be configured on the CUCM. The configuration can be divided into the following steps:

Step 1 On the SchoolMessenger Flex Appliance, complete the following:

a. Install SchoolMessenger Flex Appliance software.

b. Assign it an IP address.

c. Configure it with the IP address of the CUCM.

Step 2 On the SchoolMessenger CommSuite, configure the customer's account with the IP address of the SchoolMessenger Flex Appliance. The configuration of the SchoolMessenger CommSuite customer account is done by a SchoolMessenger technician.

Step 3 On the CUCM, configure a SIP trunk along with the IP address of the SchoolMessenger Flex Appliance; configure it with an IP service for phones so that users can access the SchoolMessenger through IP phones in addition to a web interface. See Figure 6 for a screenshot of the configuration.

Figure 6 The SIP Trunk Configuration from CUCM

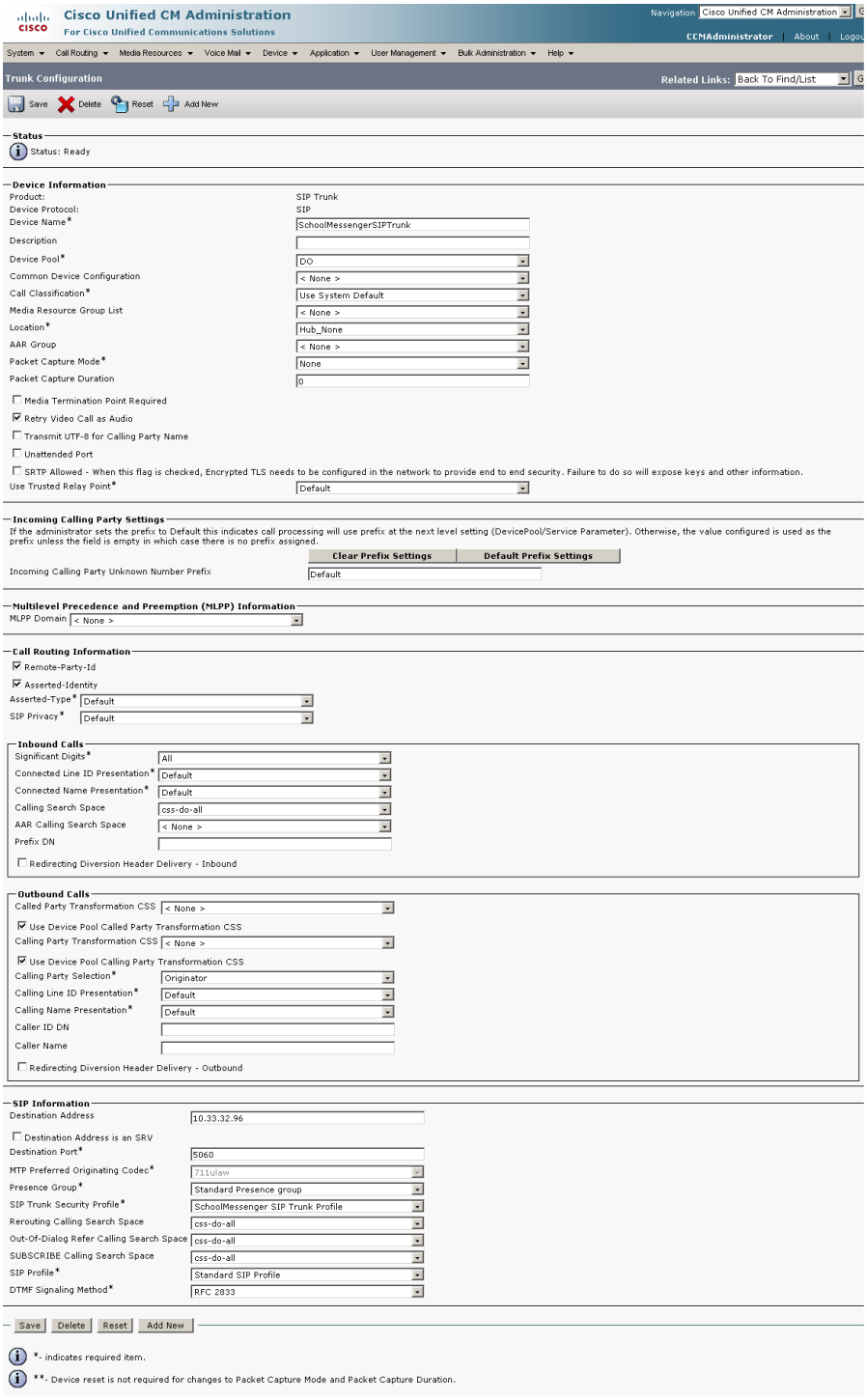


Figure 6 show the configuration used for this solution. For step-by-step instructions of performing the configuration, refer to the *SchoolMessenger Flex Appliance Product Overview and Installation Guide* at the following URL: http://www.schoolmessenger.com/8973452/docs/.

InformaCast

InformaCast is an application for broadcasting to IP devices and is used for mass notification. It knows about all the devices that are registered to a designated CUCM. Since InformaCast communicates with IP devices exclusively, it can fully use the features of the IP network. For example, it can use multicast to ring 15,000 IP phones simultaneously.

Configuring InformaCast and CUCM to Talk to Each Other

InformaCast obtains all the device information from the CUCM through Simple Network Management Protocol (SNMP). InformaCast discovers the registered IP devices from the CUCM and designates that list as "all devices." A user can divide the large device pool into groups; for example, one group for phones for first grade teachers and and another group for phones for second grade teachers. Then the user can select the relevant group to send a message.

For the solution testing, InformaCast was installed on a Windows 2003 virtual machine on an VMWare ESX 3.5 server. The InformaCast server would be located in the district office, on the same local area network as the SchoolMessenger server and CUCM. See Figure 7 and Figure 8.

Figure 7 Configure CUCM to Enable SNMP

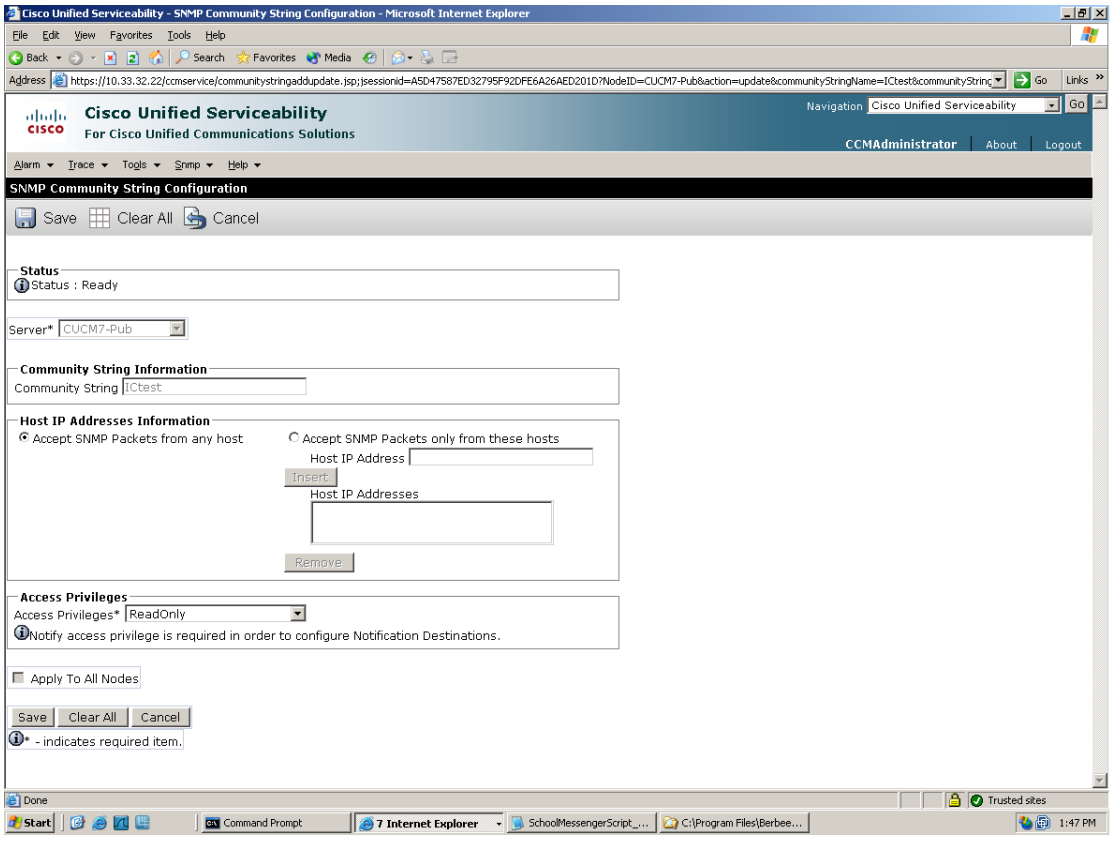
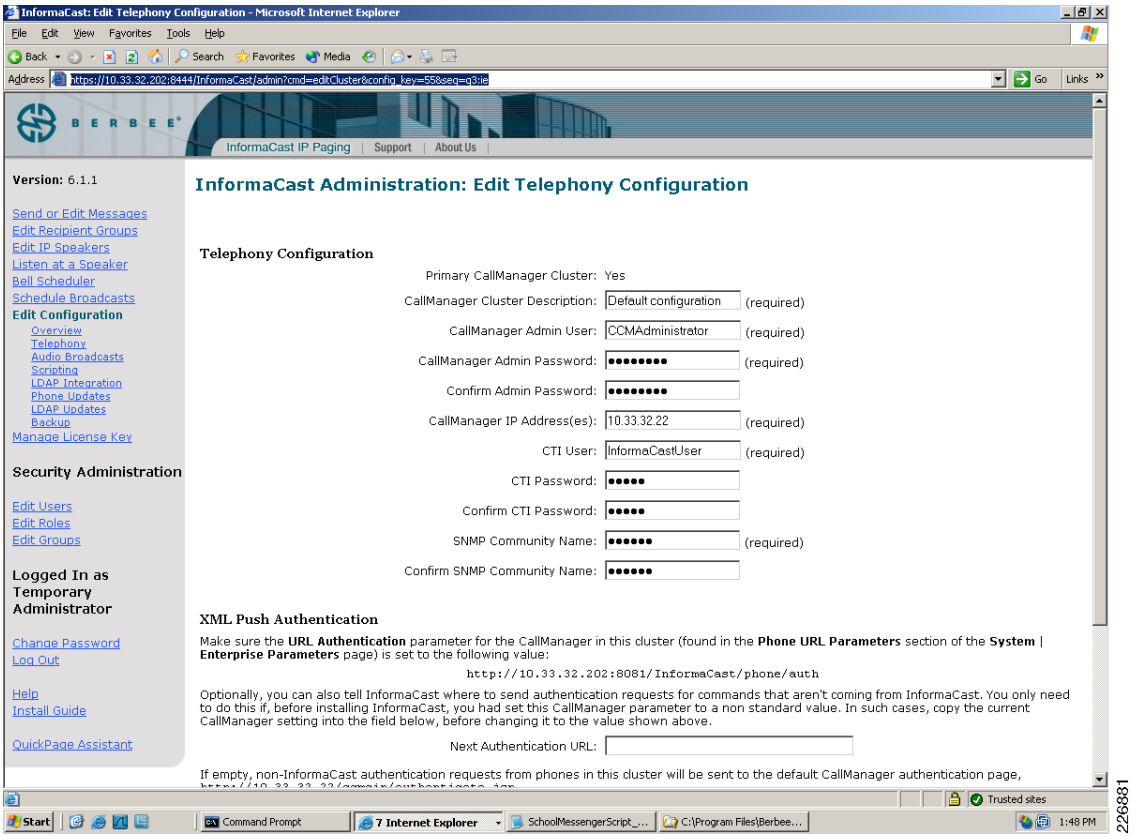


Figure 8 Configure InformaCast to Enable SNMP



After installing InformaCast, perform the following four procedures in sequence:

Step 1 Upload a license file to InformaCast.

Step 2 Download the JTAPI library.

Step 3 Configure CUCM and InformaCast for them to talk to each other through SNMP

- **a.** Configure CUCM (see Figure 7 above for configuration used in the lab testing).
- **b.** Configure InformaCast (see Figure 8 above for configuration used in lab testing).

Step 4 Let InformaCast discover all the IP devices.

For step-by-step instruction to perform the above configuration, refer to the *InformaCast™ 6.1 Installation and User Guide for a Cisco CallManager Telephony Environment* at following URL:

http://www.singlewire.com/s_informacast.html

Integrating InformaCast and SchoolMessenger

Most of the time, customers use the InformaCast software or the SchoolMessenger software directly. In unique circumstances, such as as an emergency notification, customers want a single interface. They want to be able to "hit one button" at a point when time is critical. To achieve a single interface, InformaCast will launch SchoolMessenger through a script. For example, a community school with 18 campuses integrated InformaCast with SchoolMessenger. During the many storms in 2008, the school was able to send the "*School is cancelled today due to inclement weather*" message on all connected IP phones using InformaCast and 15,000 students via SMS using SchoolMessenger.

Comparing InformaCast and SchoolMessenger

The InformaCast and SchoolMessenger complement each other. InformaCast's strength includes sending a message to multiple IP devices at the same time through multicast and communicating to other IP-enabled devices (IP speakers, bells, etc) while SchoolMessenger can communicate to non-IP-enabled devices, such as cell phones and land lines. See Table 6 for a comparison of the two applications.

Table 6 Comparison of InformaCast and SchoolMessenger Functionalities

	SchoolMessenger	InformaCast
Typical usage	External application, i.e., it is for devices off the IP network, such as phones on the public switched telephone network (PSTN). Usage scenarios include notification to parents, teachers, and staff.	Internal application, i.e., it is for devices on the IP network. Usage scenarios include internal paging, general announcement, bell schedule.
Notification speed	Place multiple calls simultaneously out of the PSTN. The scale depends on the PSTN capacity and the notification job configuration. For the hybrid model, calls are initiated through the SchoolMessenger-hosted gateway with a speed up to thousands of calls per minute.	Simultaneously reaches all the IP phones on the network.
Non-IP devices (cell phones, land lines)	Yes	No
Non-phone devices (IP speakers, bells)	No	Yes
Communicate to CUCM	Through SIP trunk	Through SNMP
Place calls	Through CUCM out the PSTN gateway	Through Multicast
Notification methods	phone, email, and SMS	Audio and text to IP phones

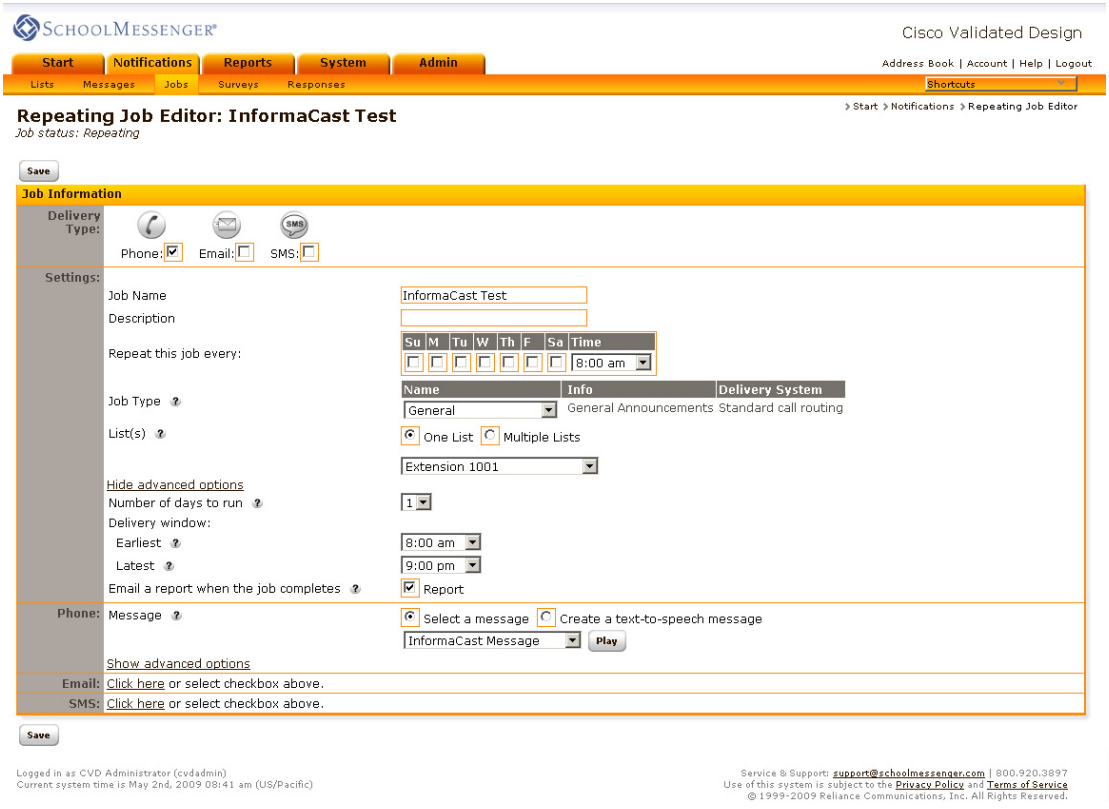
Devices registered to a CUCM will be known to the InformaCast server and be classified as an internal device. Devices not registered to a CUCM (for example, devices that are reachable through PSTN) are classified as an external device.

Because InformaCast application is not limited to local area network, a user can broadcast a message to multiple schools if their phones are registered to the communication manager in the district office.

Adding a Script to Launch SchoolMessenger

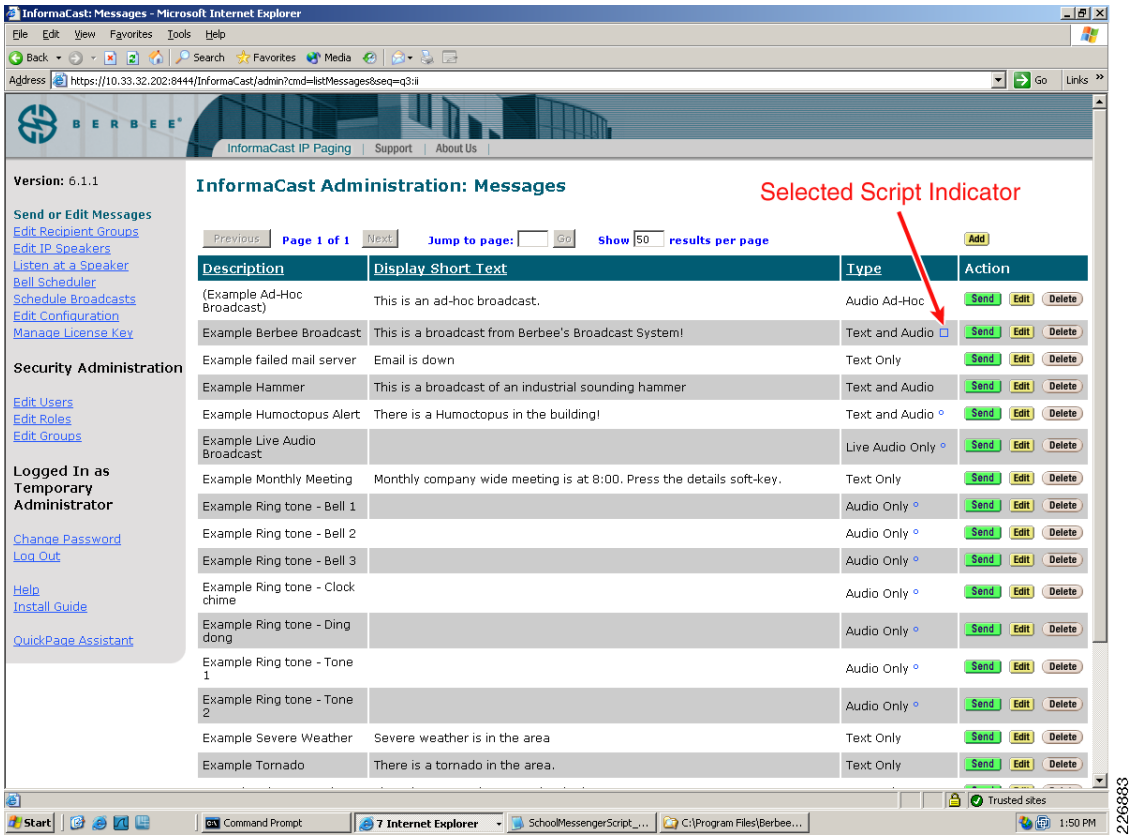
InformaCast uses a script to launch SchoolMessenger so that a user can do internal and external notifications through the same interface. On the SchoolMessenger, a repeatable job, such as "*notify_parents*" message, can be created (see Figure 9). A repeating job is like a template. It does not have the message content. Instead, the message content will come from InformaCast interface. Each time, a user can change the message content; for example, "*School is cancelled for Monday, April 27, 2009*" from the InformaCast interface. When triggered by InformaCast, SchoolMessenger works according to preset rules, such as "*what is the latest time to call*" and "*how many times to retry*".

Figure 9 Setting UP a Repeating Job on SchoolMessenger



In Figure 10, the blue square (see where the arrow is pointing to in the figure) indicates that a script has been selected.

Figure 10 Selecting a Script



For using the integrated interface of SchoolMessenger and InformaCast, the following steps are performed in advance:

Step 1 On the SchoolMessenger server, configure a repeating job, such as "*notify_parents*".

Step 2 On the InformaCast application, select a message, click on **Edit** to specify a script.

Step 3 On the InformaCast application, customize the message content, then click on **Send** to broadcast the message to a group of IP devices and also trigger the SchoolMessenger job.

Whenever an emergency occurs, the customer only needs to perform Step 3 (customize the message content, click on **Send** to send to a group of internal devices and also trigger external notification).

Perform the following steps to specify and run a script:

Step 1 Edit a message in InformaCast to select a script.

Step 2 From the main page of InformaCast, click on **Send or Edit Messages** on the upper left side.

Step 3 Select a message, such as *"This is a broadcast from Berbee's Broadcast System!"*.

Step 4 Click on **Edit**.

Step 5 At the bottom of the page, click on **Edit** under **Scripting**.

Step 6 Browse and select a script file. Once the script file is selected, a blue color square is shown on the left side of **Send** button.

Step 7 Click on the **Send** button to select a group, such as *first grade teachers*, then click on **Send**. InformaCast sends the message "*This is a broadcast from Berbee's Broadcast System!*" to first grade teachers. It also triggers a script that goes to the SchoolMessenger website to submit a job—to call first grade parents with this message.

Step 8 InformaCast launches SchoolMessenger through Simple Object Access Protocol (SOAP) requests. The SchoolMessenger server URL for submitting jobs manually and the URL for SOAP requests are different. For example, in the lab testing, the URL for submitting jobs manually was as follows:

http://asp.schoolmessenger.com/ciscocvdtest

While the URL for SOAP requests was as follows:

https://asp.schoolmessenger.com/ciscocvdtest/api/smapi.php

Modifying the Script

InformaCast provides a sample script. The following were modified to reflect the actual installation in lab testing:

1. The SchoolMessenger server URL for SOAP requests.
2. The user ID and password on the SchoolMessenger.
3. The name of the SchoolMessenger job that will be run.
4. The credentials of a valid InformaCast user to access the audio associated with the InformaCast message.

InformaCast releases a script builder to make this process convenient.

IP Speakers

IP speakers are connected to the same switch as IP phones. Similar to IP phones, IP speakers receive power from the Power- over-Ethernet (PoE) switch. The port connecting an IP phone has both voice VLAN and data VLAN configured because an IP phone has both a network port and an access port for connecting to the Ethernet cable and to a PC, respectively. On the other hand, the port connecting an IP speaker has only voice VLAN because an IP speaker does not have an access port for connecting to a PC that requires data VLAN.

The configuration of the port connecting to an IP speaker is similar to the configuration of the port connecting to an IP phone, except there is no data VLAN statement:

```
interface GigabitEthernet1/0/47
 description IP Speaker
 switchport mode access
 switchport voice vlan 49
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10   0   0   0
 queue-set 2
 priority-queue out
```

```
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoQoS-Police-CiscoPhone
 ip dhcp snooping limit rate 100
end
```

IP speakers obtain configuration from an InformaCast server. IP speakers do not communicate with a CUCM directly. The boot up sequence of an IP speaker has both similarity and difference to the boot up sequence of an IP phone. The steps are as follows:

Step 1 The IP speaker contacts a DHCP server for IP address.

Step 2 The IP speaker uses Service Location Protocol (SLP) to request the address of an InformaCast server; when it does not succeed using SLP, it uses DHCP option 150 to find the address of a TFTP server.

Step 3 The IP speaker gets configuration from the InformaCast server.

While its boot up scheme is similar to the boot up of an IP phone, two differences exist:

a. An IP speaker talks to an InformaCast server instead of a CUCM.

b. An IP speaker can use either SLP or TFTP to find a server in order to download configuration.

Step 4 After an IP speaker and an InformaCast server establish communication, a user can use the **Edit IP Speakers** menu from the InformaCast server to control the IP speaker, such as adjusting volume of the IP speaker.

High Availability

Cisco UC, SchoolMessenger, and InformaCast provide high availability in different ways.

UC High Availability

In case CUCM at the district office is not reachable (CUCM failure or WAN goes down), the school site ISR keeps IP phones online using SRST. In the lab testing, when the connection between the district office and a school was shutdown, we were able to call phones within the school as well as outside phones through PSTN.

SchoolMessenger High Availability

Emergency notification is done by fully-hosted, highly availability network. For all notifications, SchoolMessenger retries multiple times according to user configuration.

InformaCast High Availability

In InformaCast, high availability is accomplished through the following two methods:

1. Installing InformaCast into a virtual machine on different physical machines.
2. Setting up a standalone server, PageKom, at a school site to control IP speakers when WAN goes down.

Quality of Service

Quality-of-service (QoS) is used to treat different types of traffic differently when congestion occurs. For example, during congestion, priority needs to be given to voice traffic over data traffic, since voice, as a class of IP network traffic, has strict requirements concerning packet loss, delay, and delay variation (also known as jitter).

No new QoS policy is applied for SchoolMessenger and InformaCast. Since the main objective is to enable QoS for IP Telephony only, AutoQoS VoIP macro is used to automatically generate the best-practice QoS configuration. For a port connecting to an IP phone, the automatically generated Cisco VoIP configuration is as the following:

```
srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape  10  0  0  0
 queue-set 2
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cosb
 auto qos voip cisco-phone
service-policy input AutoQoS-Police-CiscoPhone
```

For detailed information on AutoQoS VoIP, refer to the *Enterprise QoS Solution Reference Network Design Guide* Version 3.3 that can be found at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

Multicast

Multicast feature avoids sending duplicate information on the network. When the user sends the message "*Please implement emergency evacuation procedure immediately: this is not a drill* " to the 50 IP phones in a school from the InformaCast server in the district office, there is only one copy of this message over the WAN to the school.

PIM sparse mode is configured on each router interface and multicast routing is enabled globally to support multicast traffic for InformaCast audio messages. Because the WAN is Metro Ethernet, multicast can be routed over the WAN without further encapsulation or tunneling.

For a router to participate in multicast, first enable multicast globally on the router, then enable multicast for each interface that has an IP address, whether it is a physical interface or a virtual interface.

The following is an example configuration for the router in the district office:

Global configuration:

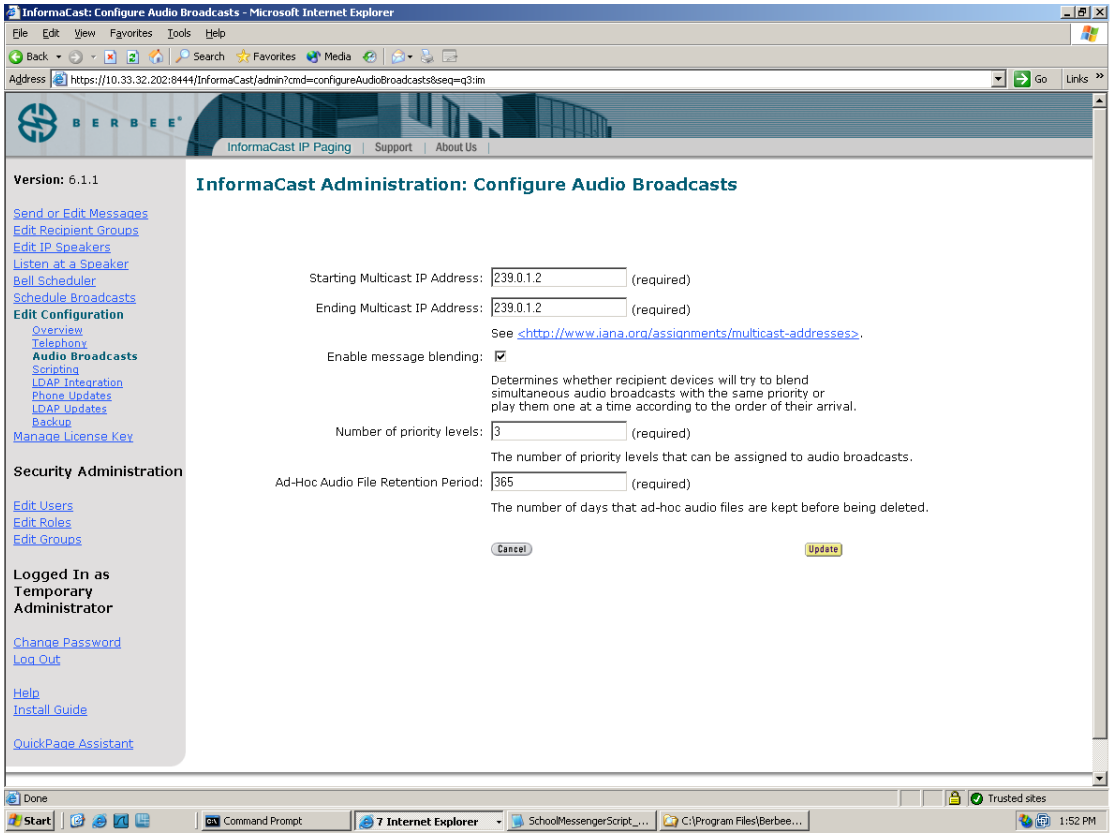
```
ip multicast-routing
ip pim rp-address 10.33.9.1
ip pim spt-threshold infinity
```

Configuration for each interface with an IP address:

```
interface FastEthernet5/2
 ip pim sparse-mode
```

Figure 11 shows the multicast address used by the InformaCast application.

Figure 11 Multicast Setting on InformaCast



Many applications use multicast features to decrease the bandwidth usage of the WAN. In the lab, the following were tested:

- Music on hold feature of IP phones was tested to verify multicast configuration.
- Audio notification to multiple phones from the InformaCast server in the school district office.

For this implementation, recommended campus multicast design was used. For details, refer to the *Cisco AVVID Network Infrastructure IP Multicast Design SRND* at the following URL: http://www.cisco.com/application/pdf/en/us/guest/tech/tk363/c1501/ccmigration_09186a008015e7cc.pdf

Appendices

Appendix A—Management of Router and Switch Configurations

For the Notifi-Ed solution, CiscoWorks LAN Management Server (LMS) can be used to configure and manage the Layer-2 and Layer-3 configurations on the ISR and the Catalyst switches. CiscoWorks LMS can be deployed at the district office and managed remotely through a web browser.

Table 7 describes the composition of applications within LAN Management Solution 3.1.

Table 7 Composition of Applications within LAN Management Solution 3.1

This LMS 3.1 Application...	Provides...
CiscoWorks Common Services 3.2 (CS)	Common software and services for LMS applications. Common Services provides a set of shared application services that are used by all LMS applications.
Resource Manager Essentials 4.2 (RME)	The ability to manage: • Device inventory and audit changes. • Configuration files, software images, and syslog analysis. • Network monitoring and fault information for tracking devices that are critical to network uptime.
Campus Manager 5.1 (CM) Campus Manager is sometimes referred to as Campus.	The following functions: • Visualize network topology. • Locate and display data about users and hosts in the network. • Manage VLANs. • Detect network discrepancies and Best Practice Deviations
CiscoView 6.1.8 (CV)	The ability to monitor and troubleshoot devices across your network being a graphical device management tool.
Device Fault Manager 3.1 (DFM)	The following functions: • Monitor device faults in real-time, and determine the root cause by correlating device-level fault conditions. • Monitor fault history. • Configure E-mail, SNMP trap, and syslog notifications.
Internetwork Performance Monitor 4.1 (IPM)	The ability to pro-actively troubleshoot network response time, jitter, and availability.
CiscoWorks LMS Portal 1.1	The ability to: • Customize information, based on the applications installed. • View frequently used information in a common place. With this you do not need to navigate through many pages. • Display application-related information as portlets. • Customize home page to have all information on a single screen from all the installed applications.

Table 7 Composition of Applications within LAN Management Solution 3.1 (continued)

CiscoWorks Assistant 1.1	Workflows to: • Set up and manage CiscoWorks LAN Management Solution (LMS) servers. • Collect troubleshooting information.
CiscoWorks Health and Utilization Monitor 1.1	Monitors the device for performance parameters, report violations based on the threshold values configured, and provides extensive reporting.
Integration Utility 1.8 (NMIM)	Support for third-party Network Management Systems (NMS). This is an integration module.

Appendix B—Security Management

The Cisco Security Manager can be used to manage security on the school branch and district office infrastructure devices. While there is only one branch and one district office implemented in the validation of the Notifi-Ed solution, the implementation and design guidance developed in this solution is applicable to larger-scale networks.

Cisco Security Manager is suitable for efficiently managing networks that range from a few devices to thousands of devices. Scalability is achieved through powerful policy-based management techniques, which allow settings to be defined once and then optionally assigning the settings to individual devices, groups of devices, or across the enterprise. When a setting is changed, Cisco Security Manager automatically applies the change to all affected network devices. The firewall or VPN policies are platform-neutral, and can be applied across different device platforms such as Cisco routers, security appliances, or services modules. Cisco Security Manager also provides flexible device-level overrides; this allows policy re-use and sharing while retaining the ability to customize device-specific settings as necessary.

While the deployment of the Cisco Security Manager was outside the scope of solution validation, the following link provides more information on how to deploy the Cisco Security Manager for your network:

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.1/user/guide/ug31.html

Appendix C—Netformx DesignXpert Supported Design

The Notifi-Ed solution has been incorporated into the Netformx DesignXpert library updates. Using Netformx, sample solution designs and bill-of-materials can be referenced and, if needed, can be modified to fit the specific deployment scenario required for a given healthcare organization. Over time, when the need to update the design becomes necessary, the Netformx updater mechanism automatically downloads the Cisco verified solution blueprints and corresponding part numbers that comprise the solution to all Netformx subscribers.

The Cisco Industry Solution Engineering team has partnered with Netformx to offer its solution designs in the DesignXpert quoting tool. By using Netformx DesignXpert, quoting a solution becomes significantly simplified, increases productivity, and helps eliminate missed components—promoting customer satisfaction. DesignXpert helps you and your customer establish a validated solution blueprint that becomes a reliable reference source for managing the overall life cycle of the solutions.

More information about the Netformx DesignXpert is available at the following URL:

www.cisco.com/go/designxpert

Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.