Cisco Unified Communications Media Display Design and Implementation Guide

Cisco Validated Design I

October 12, 2007

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

Customer Order Number:
Text Part Number: OL-14441-01

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.

Cisco Unified Communications Media Display Design and Implementation Guide

CONTENTS

Cisco Unified Communications Media Display Design and Implementation Guide

This guide describes how to implement the Cisco Unified Communications Media Display solution using the LiteScape OnCast product and Cisco Unified Communication technologies. It provides a proof of concept via interoperability testing using multiple retail reference architectures. This enables a retailer to expedite their implementation of media displays within their environment.

The Unified Communications Media Display target audience is sales engineers that have retail accounts interested in using an IP telephony environment as a method for digital media displays. It is assumed that administrators of the Unified Communications Media Display have experience with installation and acceptance of the products covered by this network design. In addition, it is assumed that the administrators understand the procedures required to upgrade and troubleshoot networks at a basic level.

Other users of this guide include the following groups:

- Marketing personnel familiar with content creation and distribution
- Retail customers with technical networking/telephony background and experience
- System administrators who are familiar with the fundamentals of IP telephony
- Sales engineers responsible for supporting retail accounts

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

Unified Communications Media Display Solution—Overview

The Unified Communications Media Display (a feature of LiteScape OnCast) represents an innovative approach for delivering multimedia content to both customers and sales associates on the store floor. A variety of capabilities, such as two-way communications, dynamic content management, and interactive control, expand the possibilities compared to more expensive and restrictive kiosks. Combined with the flexibility of the Cisco Unified Communication environment, retailers expand the utility of their existing infrastructure.

The following are Unified Communications Media Display solution core components:

- OnCast Directory Server
- OnCast Composer
- Cisco Unified Communication Manager
- 7970 IP Phones

This solution was validated using Cisco Intelligent Retail Network architectures as the foundation representing an actual retailer.

Solution Description

Retailers are challenged to send consistent and clear messaging to both customers and employees in hundreds if not thousands of store locations. Current methods rely on printed signage/postings or a relay of information from store management to communicate price promotions, product information, corporate branding, store operational targets, and leadership updates. Each manager needs to read and then interpret the information before sharing with the customer/store staff, which can lead to messaging inconsistency from store-to-store locations. The method for sending this information is typically postal (received weekly), e-mail to store management (checked daily), and voicemail to store management (checked daily). This process cannot be provided real-time, because management is typically on the store floor, where they do not have computer access or notification of new voicemails.

This traditional method of communication is pushed down (one-way) from corporate, and does not provide the means for valuable collaboration (two-way) between customers, employees, store management, and corporate. The latency of communication impacts the quality of service and the time it takes for a customer service agent to respond to a customer request. These factors contribute to an unsatisfactory customer experience and potential “abandoned cart”, where customers walk away from retail stores because of the lack of the personal touch or customer attention.

Using Cisco Unified Communications and LiteScape OnCast, retailers can broadcast advertising, branding, and other content to affordable color IP phones throughout each store. Content can be customized to different audiences, changed in real time, and can include text, text-to-speech, images, pre-recorded audio, live audio, configurable softkeys, and surveys. IP phones enable users to have pushbutton control for calling a help desk, playing back prerecorded messages, displaying related product information of interest, or filling out a survey.

By replacing a single kiosk with multiple always-on, interactive, communication-enabled display devices, retailers benefit both customers and employees. Customers can make better informed purchases and enjoy faster service. Using OnCast, store employees gain a much-needed connection to company headquarters; the executive team can affordably deliver personalized audio and visual content to individual departments or the entire company. Urgent product or emergency procedure information can instantly reach store employees when recalls and other public safety issues arise. As a powerful work flow management tool, the Unified Communications Media Display solution improves productivity.

Target Market

The target market of the Unified Communications Media Display is retailers interested in deploying IP telephony and/or digital media displays throughout their enterprise.

Solution Features and Benefits

The Unified Communications Media Display allows store communications personnel to send images, audio/text messages, and surveys to any phone or group of phones within one or many stores.

Benefits to the store employee include the following:

- Consistent communication of corporate policy and promotional messaging to associates ensures that corporate messaging is received at the same time.
- Increased message penetration into the associate ranks ensures that more associates see the message.
- Delivery of multimedia communication for higher associate recall ensures that more associates remember the message.
- Delivery of vendor-driven promotional and training content.
- Faster response to security/safety threats.

Benefits to the customer include the following:

- Dynamic, real-time content delivery and faster service for increased customer satisfaction
- Communication enhancement, with instant connection to customer service
- Visual, audio, and interactive content, for richer information exchange

Benefits to the retailer include the following:

- Affordable end devices, for flexible placement and mobility throughout the store
- Ability to target the audience (customers, employees, managers) and rapidly distribute customized time-critical content, serving multiple purposes with the same solution and increasing sales
- Collection of customer and employee feedback through survey tool

Scope of the Solution

The tests that were performed by Cisco and LiteScape (as described in Testing, page 50) demonstrate a proof of concept that specific services of LiteScape OnCast will perform in a Cisco IP telephony environment. The LiteScape OnCast Server provides a wide variety of services. Cisco did not test every service that is available on the OnCast Server, but only services related to the digital media display needs of retailers.

The Unified Communications Media Display solution was deployed and tested within three retail network environments: small, medium, and large stores. These three store models were constructed using Cisco Intelligent Retail Network reference architectures. Each store model has varying degrees of redundancy and resiliency. The Unified Communications Media Display solution was tested at the Cisco lab in San Jose, CA.

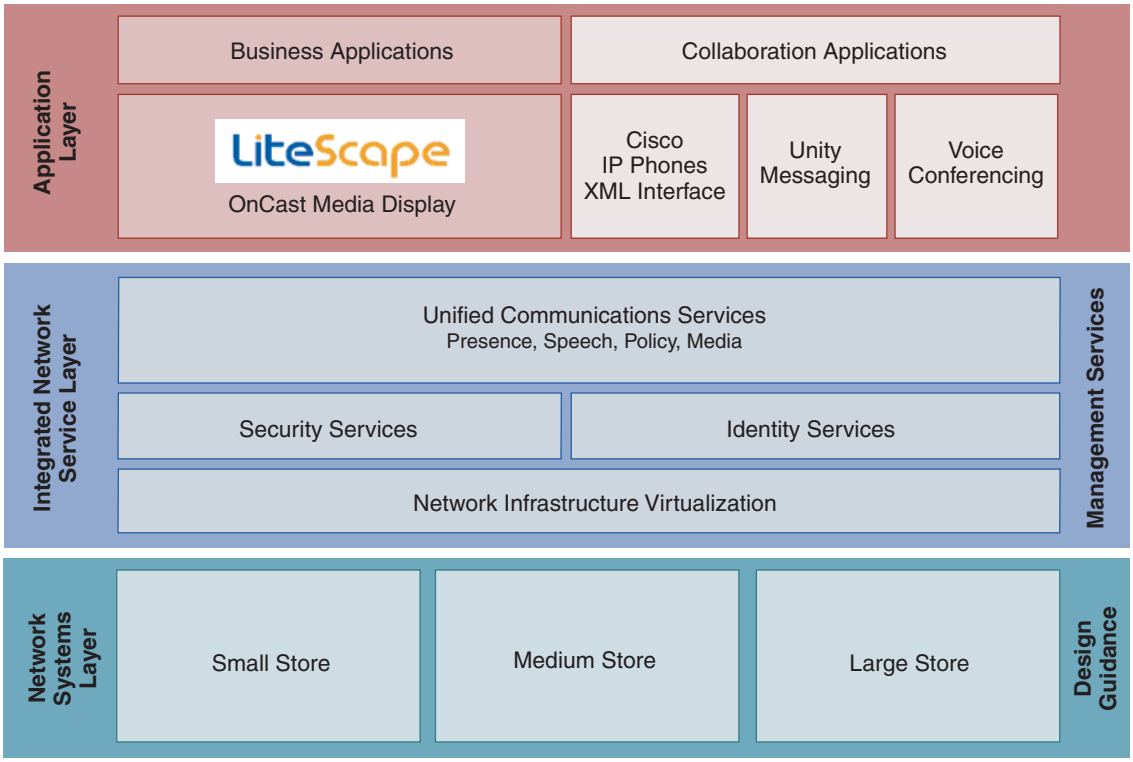
The Unified Communications Media Display solution is a Cisco Validated Design, level 1 (CVD1), and as such, scale performance testing is not within the scope of this document. For more information, see the following URL:
http://www.cisco.com/en/US/netsol/ns741/networking_solutions_program_home.html.

Unified Communications Media Display Solution Architecture

Intelligent Retail Network and the SONA Framework

The framework for the Unified Communications Media Display solution is based on the Cisco Service Oriented Network Architecture (SONA), as shown in Figure 1. Using a SONA framework, the Intelligent Retail Network (IRN) reference architectures serve as the foundation of the network systems layer. These network architectures exhibit best practices for retail networks and provide the robust foundation for the higher-level services and applications. For more information about IRN, see the following URL: http://www.cisco.com/web/strategy/retail/irn.html.

Figure 1 Unified Communications Media Display Solution Framework



Application Layer

Business and collaboration applications connect users and business processes to the infrastructure. The application layer of the framework includes the combined business and collaboration applications from Cisco and LiteScape.

LiteScape OnCast integrates with a Cisco Unified Communications IP telephony system to deliver multi-modal communications (data, voice, and visual content) to any connected IP device. OnCast enables timely content in many formats. Content can be quickly collected from a variety of sources, filtered for important details, and broadcast immediately or automatically to the people who need it.

The Cisco Unified Communications suite enables collaboration through XML-based applications.

The Cisco 7970 Series color IP phones have touchscreen-enabled displays. Users have pushbutton control for calling a help desk, playing back prerecorded messages, displaying related product information of interest, or filling out a survey.

Combined, retailers can broadcast advertising, branding, and other content to affordable IP phones throughout each store. Content can be customized to different audiences, changed in real time, and can include text, text-to-speech, images, pre-recorded audio, live audio, surveys, and RSS feeds.

Application services are the connection from the applications to the shared services of the infrastructure services layer. This is where filtering, caching, and protocol optimization interact with applications or application middleware services to optimize the performance from the network to the end user.

Integrated Network Services Layer

Process control is simplified by using common infrastructure services such as collaboration, security, and identity. These are key advantages that aid in operational reporting and security policy enforcements. Fewer services that are shared across more intelligent devices increases the operational efficiency of the whole system.

- *Voice and collaboration services* are created by adding the Voice IOS service to the store routers, and adding Cisco Unified Communication Manager and media servers to the data center.
- *Network virtualization* can be viewed by the use of Cisco Integrated Services Routers (ISRs), which virtualize store security appliances, routers, switches, and voice and application services into intelligent IT appliances that are centrally managed and monitored.
- *Security services* are used extensively in the IRN architectures. These services are a combination of in-store security services shared across multiple physical devices, central management in the data center, and virtual access to the security control plane from anywhere in the retail network.
- *Identity services* are used to ensure that access to each application is allowed only for authenticated and authorized users. A central LDAP-based directory service enhances secure identity services to both Cisco and LiteScape suites.

Note For more information on securing IRN architectures, see the *PCI Solution for Retail Design and Implementation Guide* at the following URL: http://www.cisco.com/web/strategy/retail/pci_imp.html. This guide describes services that can be used to provide a secure posture for the Unified Communications Media Display solution.

Intelligent Retail Network Store Architectures

Small Store

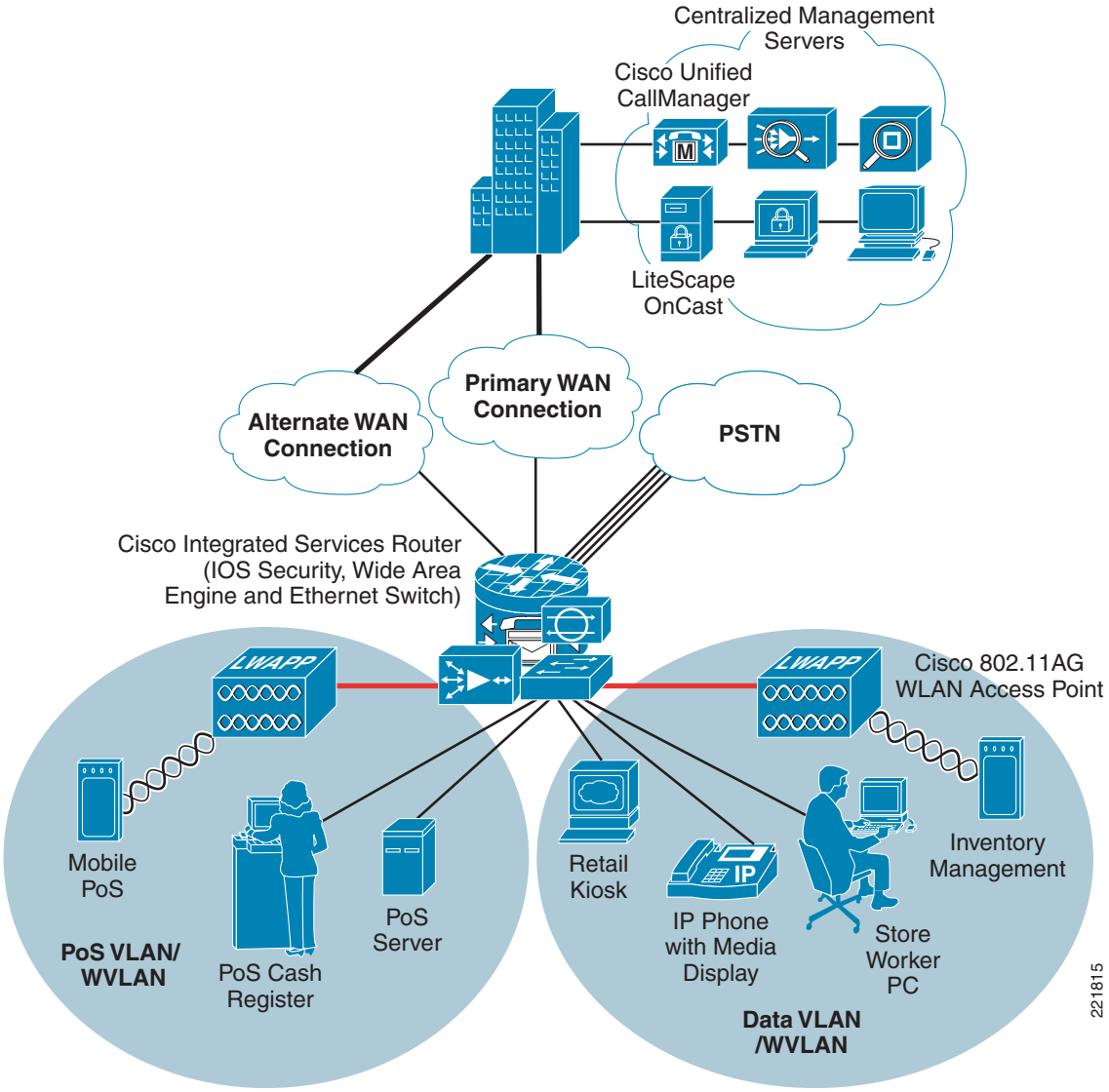
The small store reference architecture (see Figure 2) is a powerful platform for running an enterprise retail business that requires simplicity and a compact form factor. This combination appeals to many different retail formats that can include the following:

- Mall-based retail stores
- Quick-serve restaurants
- Convenience stores
- Specialty shops

- Discount retailers who prefer network simplicity over other factors

This network architecture is widely used, and consolidates many services into fewer infrastructure components. The small store also supports a variety of retail business application models because an integrated Ethernet switch supports high-speed LAN services.

Figure 2 Small Store Network Design



Primary Design Requirements

Primary design requirements are as follows:

- Store size averages between 2000–6000 square feet
- Fewer than 25 devices requiring network connectivity
- Single router and integrated Ethernet switch
- Preference for integrated services within fewer network components because of physical space requirements

Advantages

Advantages are as follows:

- Lower cost per store
- Fewer parts to spare
- Fewer software images to maintain
- Lower equipment maintenance costs

Limitations

Limitations are as follows:

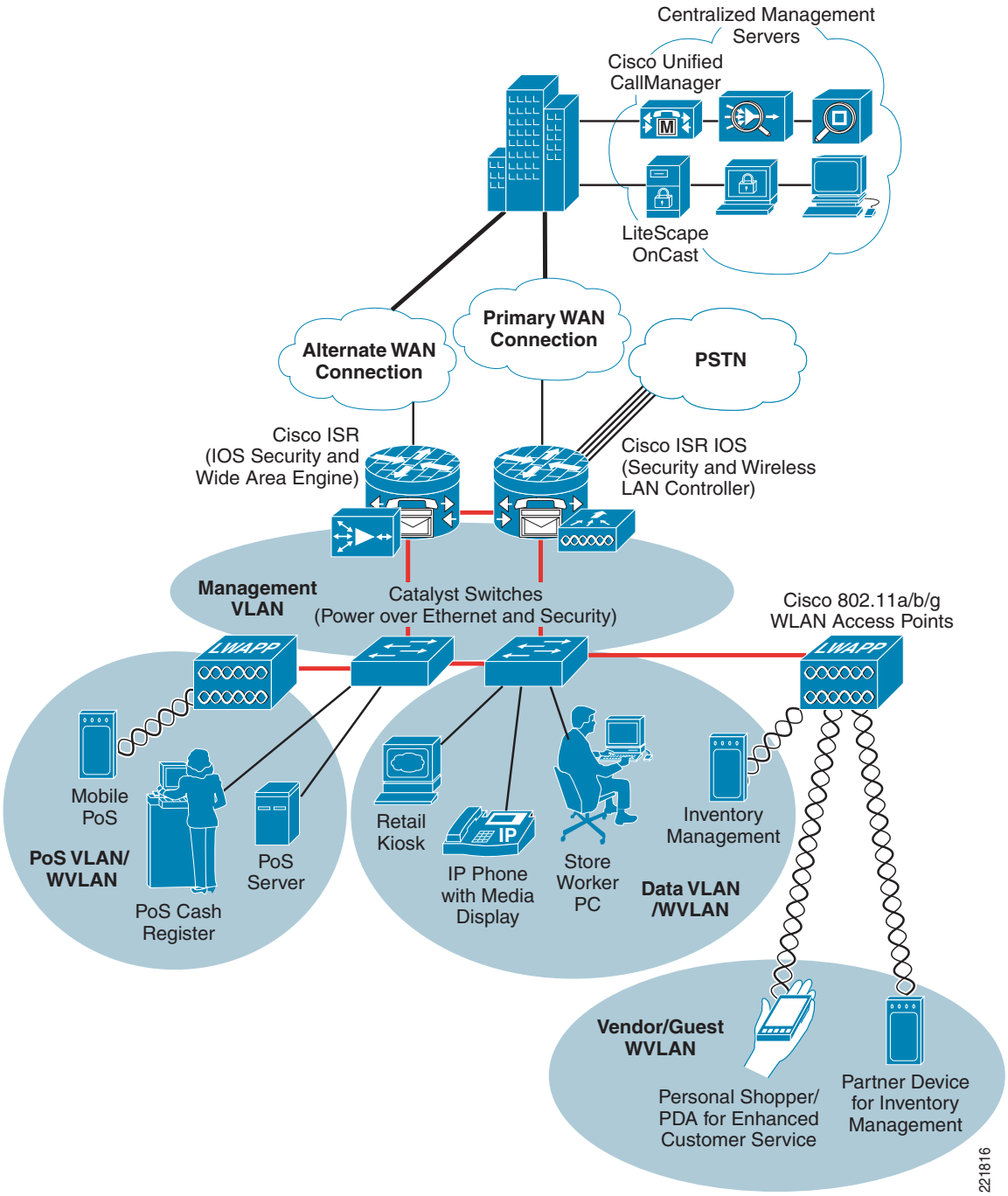
- Decreased levels of network resilience
- Greater potential downtime because of single points of failure

Medium Store

The medium retail store reference architecture (see Figure 3) is designed for enterprise retailers who require network resilience and increased levels of application availability over the small store architecture and its simple, single-threaded approach. As more mission-critical applications and services converge onto the IP infrastructure, network uptime and application availability are more important. The dual-router and dual-LAN switch design of the medium store supports these requirements. Each of the ISR routers can run Cisco IOS security services and other store communication services simultaneously. Each of the ISR routers is connected to a dedicated WAN connection. Hot-Standby Routing Protocol (HSRP) is used to ensure network resilience in the event that the network connection fails.

The access layer of the network offers enhanced levels of flexibility and more access ports compared to the small store. The distributed Cisco Catalyst switches can support a combination of larger physical buildings or a larger number of endpoints than the small store.

Figure 3 Medium Store Network Design



Primary Design Requirements

Primary design requirements are as follows:

- Store size averages between 6,000–18,000 square feet
- Physical size of store is smaller than a large store, so a distribution layer of network switches is not required
- Number of devices connecting to the network averages 25–100 devices

The medium retail store reference architecture is designed for enterprise retailers that require network resilience and increased levels of application availability over the small store architecture and its single-threaded, simple approach. As more mission-critical applications and services converge onto the IP infrastructure, network uptime and application availability are more important. The dual-router and dual-LAN switch design of the medium store supports these requirements. Each of the ISR routers can run IOS security services and other store communication services simultaneously. Each of the ISR routers is connected to a dedicated WAN connection. Hot Standby Routing Protocol (HSRP) is used to ensure network resilience in the event that the network connection fails.

Advantages

Advantages are as follows:

- More adaptive access layer with support for a greater number of endpoints and more diverse building requirements (multiple floors, sub-areas, and so on)
- Multiple routers for primary and backup network requirements
- Improved network resilience through parallel device design
- Improved network and application availability through parallel paths

Limitations

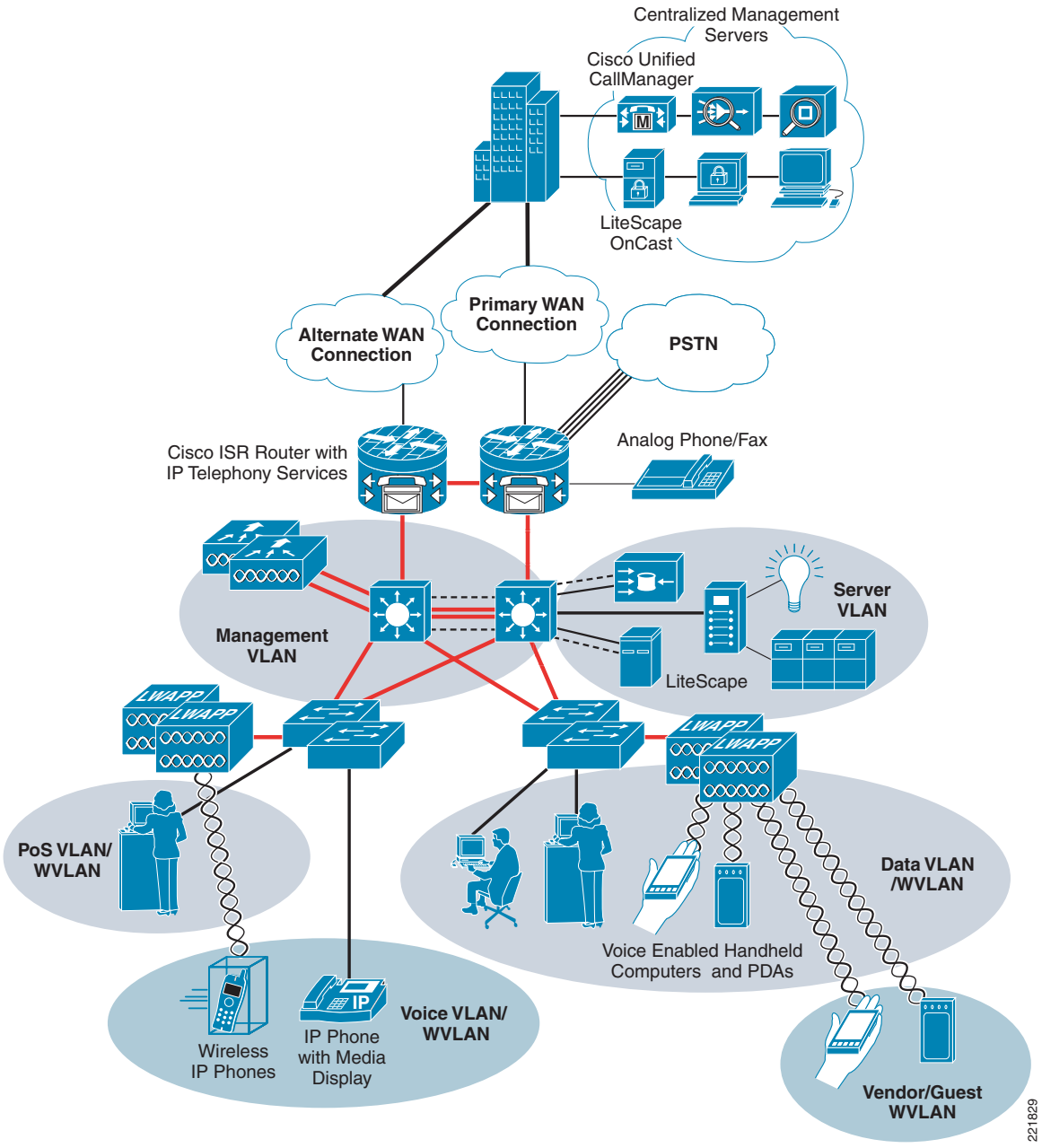
The limitation is as follows:

- No distribution layer between core layer (the ISR) and the access layer switches

Large Store

The large retail store reference architecture (see Figure 4) takes some of the elements of Cisco campus network architecture recommendations and adapts them to a large retail store environment. Network traffic can be better segmented (logically and physically) to meet business requirements. The distribution layer of the large store architecture can greatly improve LAN performance while offering enhanced physical media connections. A larger number of endpoints can be added to the network to meet business requirements. This type of architecture is widely used by large-format retailers globally. Dual routers and distribution layer media flexibility greatly improve network serviceability because the network is highly available and scales to support the large retail store requirements. Routine maintenance and upgrades can be scheduled and performed more frequently or during normal business hours through this parallel path design.

Figure 4 Large Store Network Design



Primary Design Requirements

Primary design requirements are as follows:

- Store size averages between 15,000–150,000 square feet
- More than 100 devices per store requiring network connectivity
- Multiple routers for primary and backup network requirements
- Preference for a combination of network services distributed within the store to meet resilience and application availability requirements

- Three-tier network architecture within the store; distribution layer switches are employed between the central network services core and the access layer connecting to the network endpoints (point-of-sale, wireless APs, servers, and so on)

Advantages

Advantages are as follows:

- Highest network resilience based on highly available design
- Port density and fiber density for large retail locations
- Increase segmentation of traffic
- Scalable to accommodate shifting requirements in large retail stores

Limitations

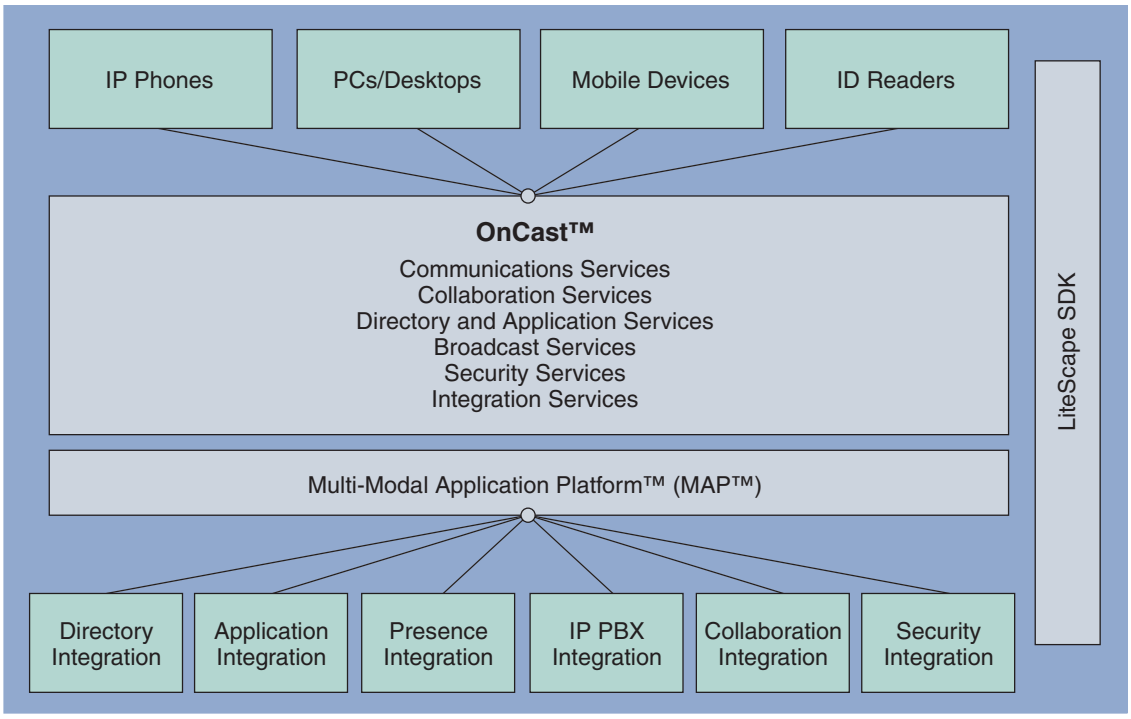
The limitation is as follows:

- Higher cost because of network resilience based on highly available design

OnCast Architecture Framework

OnCast provides unified access to traditionally disparate business applications, collaboration tools, and communications devices. OnCast directly ties together user IP phones with their desktops and allows them to move seamlessly between these disparate devices. With OnCast, the tasks that users perform on their IP phones directly complement and enhance tasks they perform on their PC, and vice versa. Figure 5 shows how OnCast brings together users and services.

Figure 5 OnCast Services

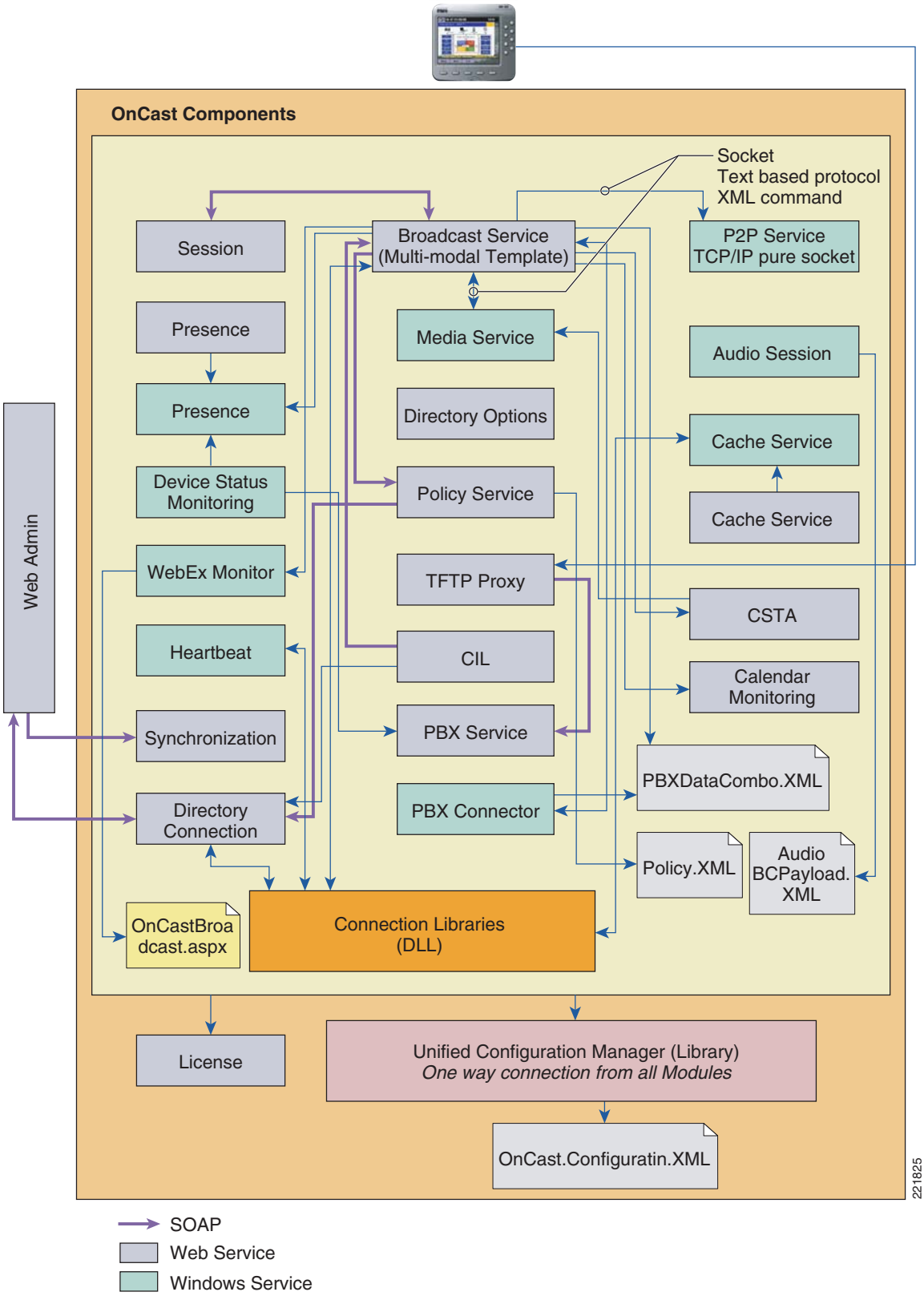


OnCast is composed of various components. The solution is based on a distributed, service-oriented architecture and is composed of a collection of Windows services and Simple Object Access Protocol (SOAP)-based web services.

The independence of the modules enables administrators to configure and distribute various components independently. In addition, the service based approach provides integration/customization and simplifies troubleshooting and pinpointing points of failure and bottlenecks.

Figure 6 shows the various OnCast components.

Figure 6 OnCast Components



The OnCast system connects IP-enabled phones with the following:

- Business applications
- Directory servers
- IP PBXs
- PCs

Figure 7 illustrates how the web administration interface is used to make configuration changes to the OnCast system. These configuration changes are recorded in an XML file named *OnCastConfiguration.xml*. You can edit this file directly, but LiteScape does *not* recommend doing so.

Figure 7 Architecture Connections

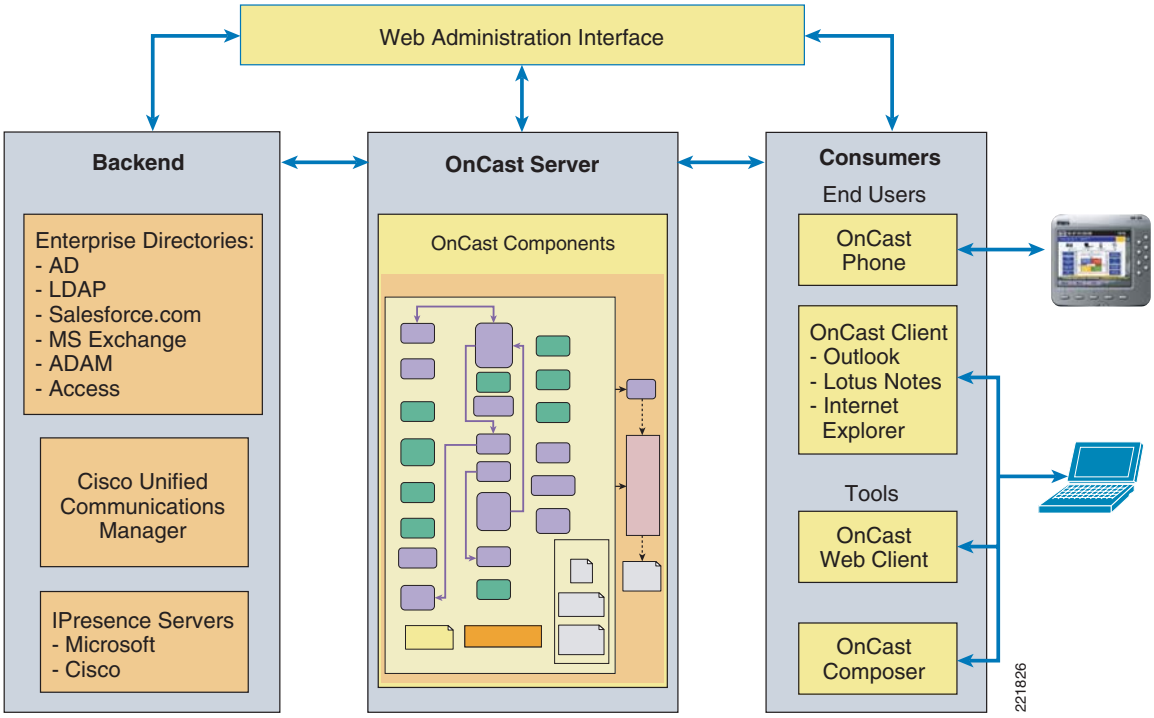
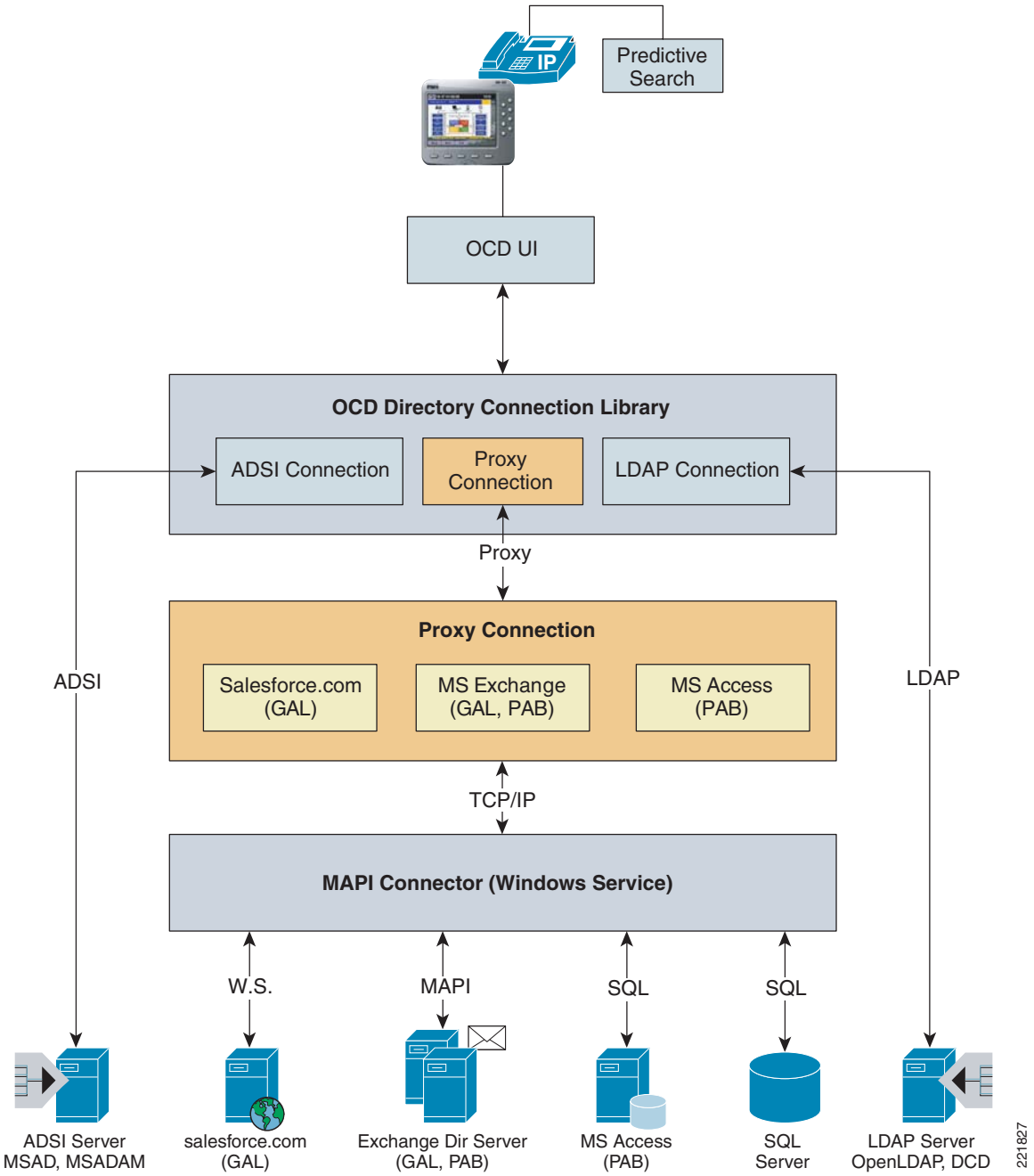


Figure 8 shows how Active Directory is linked to OnCast within the Unified Communication Media Display solution.

Figure 8 Directory Connection Architecture

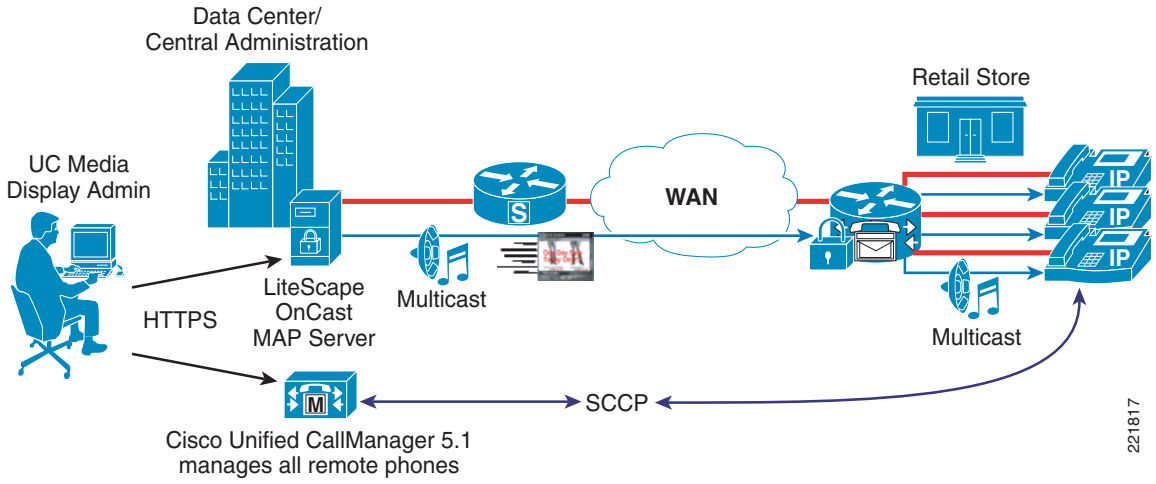


LiteScape OnCast Deployment Models and the Intelligent Retail Network

Each of the following OnCast deployment models can be implemented as desired across the three Intelligent Retail Network architectures. The solution uses the centralized model for the small and medium stores, and the distributed model for the large store. A retailer that has a variety of store sizes or regional technical challenges can implement a hybrid approach with both central and distributed OnCast Servers. All three deployment models have been tested within this solution.

Figure 9 shows the LiteScape OnCast centralized deployment model.

Figure 9 LiteScape OnCast Centralized Deployment Model

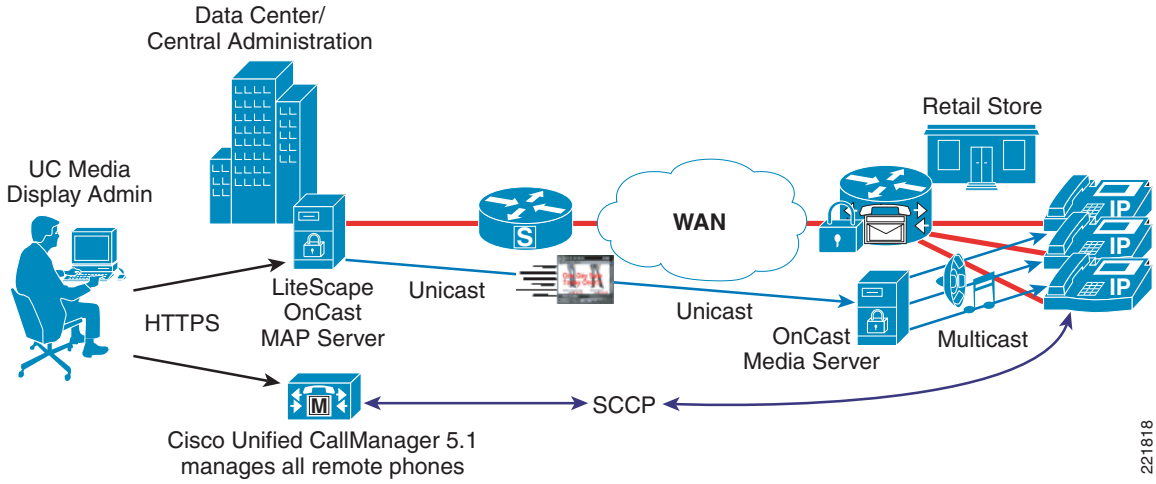


The centralized model operates as follows:

- The Admin creates media objects and copies them to the centralized OnCast server.
- The central OnCast Server pushes the media to IP phones.
- The central Cisco Unified Communication Manager cluster manages all IP phones.

Figure 10 shows the LiteScape OnCast distributed deployment model.

Figure 10 LiteScape OnCast—Distributed Deployment Scenario

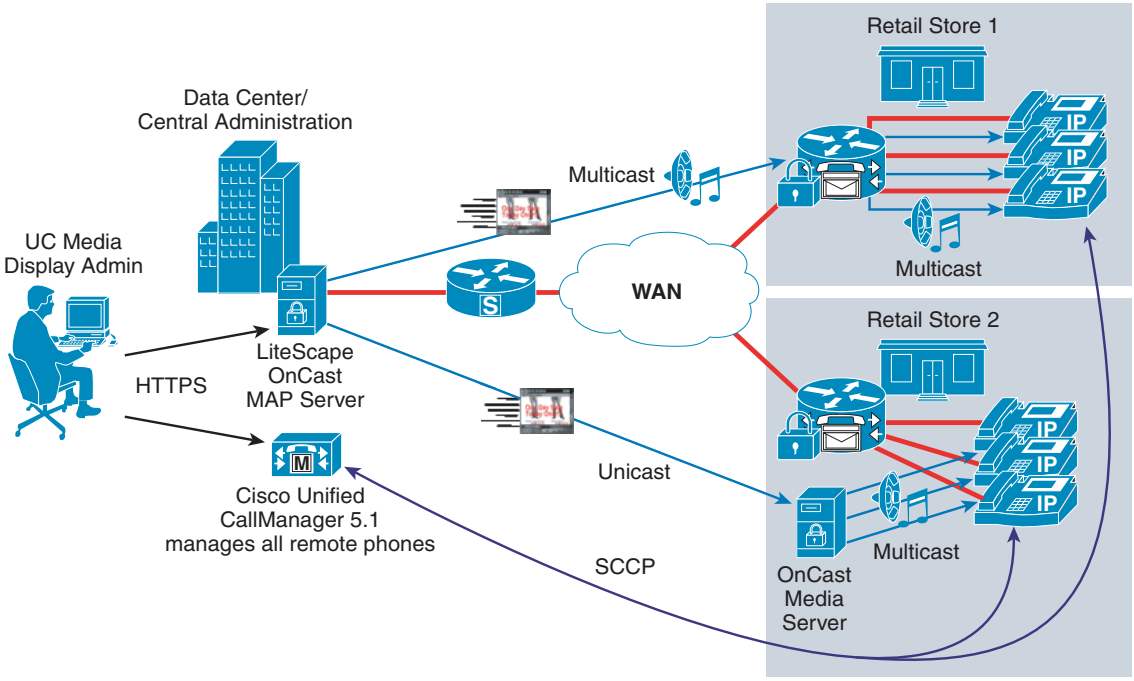


The distributed model operates as follows:

- The central OnCast server pushes media to the OnCast media server of the store.
- The OnCast media server of the store streams media to IP phones.
- The central Cisco Unified Communication Manager cluster manages all IP phones.

Figure 11 shows the LiteScape OnCast hybrid deployment model.

Figure 11 LiteScape OnCast—Hybrid Deployment Scenario



The hybrid model operates as follows:

- Some stores have a local OnCast media server.
- Others receive media from the central OnCast server.
- The central Cisco Unified Communication Manager cluster manages all IP phones.

Note This choice of multicast implementation was made by the designers of the Cisco lab and does not reflect any technical difference between the relationship of the store models back to the central OnCast server. Thus, a small store retailer that is not willing to deploy multicast across the WAN can choose a distributed multicast deployment model like that of the large store lab, and vice versa.

Unified Communications Media Display Solution—Components and Services

Solution Components

The following components are required to implement the Unified Communications Media Display solution:

- OnCast Directory Server—OnCast Directory is both the collective directory of all known users within the system, as well as the intuitive interface used from a VoIP phone to send broadcasts, initiate calls, and create phone and WebEx conferences. A retailer can also use OnCast Directory from a VoIP phone to join WebEx meetings as an organizer or participant. This OnCast phone component also allows searching across multiple phone address books using customizable search criteria.
- OnCast Composer—OnCast Composer is used to create and send voice, text, and image broadcast messages from Microsoft Outlook to VoIP phones. Advanced content such as surveys, RSS, or stock tickers can also be sent.
- Cisco Unified Communication Manager—Cisco Unified Communication Manager is the core call processing software for Cisco IP Telephony. It builds call processing capabilities on top of the Cisco IP network infrastructure. Cisco Unified Communication Manager software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, voice gateways, and multimedia applications.
- 7970 IP Phone—IP phones have all the functions expected from a telephone, as well as more advanced features including the ability to access XML-based applications.
- Oncast Directory Server (distributed optional)—Provides local, synchronized, OnCast Directory services at each store location, preserving bandwidth and accessibility to OnCast services in the event of a WAN failure.

Hardware/Software

Table 1 lists the hardware/software products installed for the Unified Communications Media Display solution.

Table 1 Hardware/Software Installed

Solution Component (Required)	Software Version	Solution Location
OnCast Directory (LiteScape) • OnCast WebAdmin • OnCast Policy • OnCast DirDialer Cisco • OnCast Directory Connection • OnCast Directory Configuration • OnCastWebService • OnCast Session Service • OnCast Sync • OnCast Presence Web Service • OnCastPBXService • OnCast Audio Session Service • OnCast P2P Hub Service • OnCast Configuration Setup • OnCast Media Service • OnCastPresenceService • OnCastDeviceStatusService • OnCastWebExMeetingStatusLib • CILConnectionWebServiceApp • OnCastWebClientManagers	Version 4.3.4 SP2 • Version 4.3.4.24 • Version 4.2.1.4 • Version 4.3.4.28372 • Version 4.3.5.28333 • Version 4.3.4.28329 • Version 4.3.4.3 • Version 4.0.2117.33260 • Version 4.1.4.41353 • Version 4.1.7.26562 • Version 4.3.5.2 • Version 4.1.4.40094 • Version 4.2.0.20816 • Version 4.3.3.8354 • Version 4.0.2686.31096 • Version 4.3.4.2 • Version 1.0.0.0 • Version 1.0.0.0 • Version 1.0.0.0 • Version 4.3.3.0	Windows 2003 Server in data center
LiteScape OnCast Composer	Version 4.3.5.0	Data center (XP SP2 desktop)
Cisco Unified Communication Manager	5.1.2.1000-11	Data center
Cisco 7970G IP Phone	SCCP70.8-2-2SR2S	All stores
Solution Component (Optional)	**Software Version**	**Solution Location**
Local store OnCast Server (distributed model)	Version 4.3.4 SP2	Large store
CiscoSecure Access Control Server	4.1(3) Build 12	Data center
Cisco ISR 3845	12.4.9T–Adv IP Services	Large store
Cisco ISR 3825	12.4.9T–Adv IP Services	Medium store
Cisco ISR 2821	12.4.9T–Adv IP Services	Small store
Catalyst 4500	12.2(20)EW 3	Large store
Catalyst 3750G	12.2.25-SEE2–IP Services + Web-based Dev Mgr	Large and medium store
Cisco 7960G IP Phone	P00308000500	All stores
Cisco 7940 IP Phone	P00308000500	All stores

Table 1 Hardware/Software Installed (continued)

Microsoft Products	Software Version	Solution Location
Microsoft SQL Server 2005 Standard	SQL Server 9.0.1399 with SP2	Windows 2003 Server in data center
MS Outlook 2003	11.6568.6568 with SP2	XP SP2 desktop in data center
MS Exchange Server 2003	6.5.7638.1	Windows 2003 Server in data center
MS Active Directory on Windows 2003 Server	5.2.3790.3959	Windows 2003 Server in data center
Internet Explorer 6	6.0.2900.2180 with SP2	XP SP2 desktop in data center
Internet Explorer 7	7.0.5730.11CO	Windows 2003 Server in data center
Microsoft Windows 2003 Server Enterprise Edition SP2	5.2 R2 Build 3790.srv03_sp2_gdr.070304-2240	Solution servers
Microsoft Internet Information Services 6.0 with ASP.NET 1.1 and 2.0 framework	.NET 1.1.4322 and 2.0.50727	OnCast Server in data center and large store

For planning purposes, the software requirements for OnCast Client and OnCast Composer are as follows:

- Windows XP SP2 or higher
- Microsoft Internet Explorer 6.0 SP1 and above
- Microsoft Office Outlook 2003 SP2 or higher

Services and Functionality

Table 2 lists the services that were enabled to optimize OnCast within the Cisco network environment.

Table 2 Services Enabled

Cisco Feature	Platform/Software Release
Multicast (recommended)—Small, medium, and large store LAN Multicast (optional)—Across the WAN	ISR 2821, 3825 and 3845 IOS 12.4.9T
QoS (recommended)	ISR 2821, 3825 and 3845 IOS 12.4.9T
Survivable Remote Site Telephony (SRST) (optional)	ISR 2821, 3825 and 3845 IOS 12.4.9T
IOS firewall (optional)	ISR 2821, 3825 and 3845 IOS 12.4.9T

Table 2 Services Enabled (continued)

LiteScape Services	
Scheduling service	

Limitations and Caveats

There are no known caveats or limitations.

Designing the Unified Communications Media Display Solution

The Unified Communications Media Display solution provides a proof of concept implementation of OnCast within a Cisco Unified Communication Manager and VoIP network. The small, medium, and large Intelligent Retail Network reference architectures provide a “real world” retail contextual backdrop for this solution. Each IRN store is centrally connected to a data center with traditional data center services such as DNS and NTP, as well as Cisco Unified Communication Manager and the OnCast Directory Server. This is a cost-effective implementation that leverages a highly available data center staffed with trained personnel and minimizes the number of additional servers required throughout the network. For very large locations where edge web caching is not available, it is advantageous to implement a distributed OnCast Directory Server. This synchronizes with the central server, reducing the amount of bandwidth needed because media is served up locally to those local devices once scheduled. This distributed model is used in the large store architecture in contrast to the centralized model used in the small and medium stores.

A number of servers and workstations were implemented as VMware Server virtual machines. This allowed greater flexibility within the lab environment and aligns with industry trending towards greater virtualization. Dedicated hardware and increased resources may be required for more consistent performance in larger implementations.

LiteScape

LiteScape OnCast is a feature-rich product with many capabilities beyond the subset of items that comprise the Unified Communications Media Display solution. Implementation of the solution requires a full installation of OnCast Directory Server and OnCast Composer. OnCast Composer is a desktop application that integrates with Microsoft Outlook.

OnCast Directory Server enables end users to invoke various communication features from the user interface on Cisco IP phones. The product provides integration with existing corporate and personal directories. Using customizable search criteria to find users and groups across the enterprise directory or within personal address books, OnCast also enables dialing, teleconferencing, and broadcasting to users and groups from the search results. OnCast enables retrieval of detailed information about directory members, as well as attributes such as alternative phone numbers, group members, presence, and availability indicators, and so on. The OnCast Directory web interface enables users to quickly create and send content-rich broadcasts across the enterprise to these targeted recipients.

OnCast Composer is used to create and send voice, text, and image broadcast messages from Outlook to VoIP phones. Advanced content such as surveys, RSS, or stock tickers can be sent.

LiteScape OnCast Directory Server has been evaluated under the Cisco Technology Developers Program (CTDP), where mid-scale and interoperability testing has been performed. Partner information and product status can be found on the Cisco website at the following URL: http://www.cisco-partners.info/showpart.asp?i=76.

OnCast Directory Server

OnCast Directory Server is installed with a complete set of components to integrate functions between a variety of services and devices. OnCast was configured to communicate with the Microsoft Active Directory server for retrieving usernames, authentication, and user phone extension information. This allows for centralized user administration and security.

OnCast Directory Server version 4.3 interoperates with Cisco Unified Communication Manager using Simple Network Management Protocol (SNMP), computer-telephony integration (CTI), and the web management interface. The solution uses a default installation of a single Cisco Unified Communication Manager 5.1.1 server with Service Package 5.1.2 applied.

Table 3 describes the various OnCast Directory components.

Table 3 OnCast Components and Descriptions

Component	Description	Installable Module
Phone UI	Responsible for the phone user interface including rendering menus and softkeys, communicating with other components to send the user requests, and showing responses on the phone.	OnCastDirDialer (Cisco)
Broadcast server	Responsible for all the broadcasts to the users and phones. The broadcast server uses OCM file templates for all broadcasts. These templates can be designed and changed with a separate tool called OnCast Broadcast Designer.	Broadcast web service
Session server	Maintains various session information about broadcasts and service invocations in progress. The service is also responsible for media port management and distribution of load information among distributed OnCast broadcast servers.	Session web service
Synchronization server	OnCast servers in high-availability/distributed environments share data/configuration information. This component is responsible for synchronizing various data/configuration files among OnCast Directory Servers participating in one server “cluster”.	Synchronization web service
Policy server	Controls the rights for all the available functions in OnCast. The policy server determines whether one user is able to broadcast, make a phone call, group call/conference to other users and groups, or see detailed information of the user.	Policy web service

Table 3 OnCast Components and Descriptions (continued)

Presence server	Tracks user and device presence.	Presence web service
Directory Connector	Responsible for any communication with the enterprise directory servers. Directory Connector uses ADSI to connect to Microsoft Active Directory, LDAP to any standard LDAP server, and MAPI to connect to Microsoft Exchange for detailed information of the user.	Directory connection web service
Detail Info Service	Retrieves detailed user contact information from the enterprise directory. Using Directory Connector, this information can be anywhere on Microsoft Active Directory, LDAP servers (such as Cisco DCD), or Microsoft Exchange Servers (GAL and PAB).	Directory Connection web service
PBX Connector	Retrieves information from IP PBX server using SNMP to retrieve extension numbers and device network information. SNMP information and changes from various IP PBXs can be polled or trapped by the PBX connector.	PBX service
Media server	Responsible for voice streaming between two endpoints and between media servers. The media server supports RTP (multicast and unicast) and can reach a variety of IP devices. The media server uses SOAP for communicating between servers at various locations.	Broadcast web service
TFTP proxy server	Provides proxy connections from phones to the cluster, allowing the extension mobility functionality to take place properly when used across PBX clusters.	TFTP proxy
Client Integration Library (CIL)	This is an application-independent module that provides the majority of the OnCast client functions, allowing an external or third-party application to use any or all of its functionality.	OnCast CIL
WebEx service	Functions with the broadcast service to provide links into WebEx for transmitting WebEx screens to the phones.	WebEx Meeting Status Service
Peer-to-Peer (P2P) service and hub service	The OnCast P2P Service facilitates communication between OnCast servers. The P2P hub service receives P2P agent TCP connections and returns a list of all other agents registered with it, to facilitate agent-to-agent direct connections.	P2P service P2P hub service
PBX service	Gets all device information from the IP PBXs and Directory Servers and combines the data into a single file that is used by OnCast to easily identify users and phones.	OnCast PBX service

Table 3 OnCast Components and Descriptions (continued)

Cache service	Copies content from existing systems (such as LDAP or Exchange servers) into a directory that OnCast uses to avoid constantly accessing the enterprise systems. This avoids placing excessive loads on the primary servers. Synchronization and refreshing of the data can happen as often as desired.	Directory cache service
On Cast Directory Options	Creates and updates user options.	Device status
Monitoring	Monitors the status of phones in real-time; for example, if they are on-hook (idle) or off-hook (in use) to facilitate calling. This information is also fed into the presence server.	Device status
Calendar web service	Provides calendaring functionality (storing, retrieving, editing, and monitoring scheduled broadcasts) in the absence of corporate scheduling servers.	Calendar web service
Configuration Manager	Manages and stores all the configurations in a centralized XML depository. With the provided web user interface, administrators are easily able to change and set configuration values.	Base product OnCast Directory WebAdmin
Heartbeat server	Maintains a connection between OnCast Directory and your specified enterprise directories.	Heartbeat service
Audio session service	Manages in-progress and scheduled broadcast sessions.	OnCast audio session service
Film strip service	This component receives film strip sets from the Composer application, then broadcasts them to the assigned devices.	OnCastFilmStripServerService

OnCast can access the following directory services:

- Microsoft Active Directory
- LDAP v2, v3, and Open LDAP compliant directories
- Microsoft Exchange (global and personal address books)
- Microsoft Outlook MAPI
- Salesforce.com
- SQL-based directory repositories

The minimum hardware requirements for an OnCast Directory Server are as follows:

- Processor—Intel Xeon (dual processor required)
- Processor speed—2 GHz or higher
- Memory—2 GB or more
- Hard disk space—40 GB or more

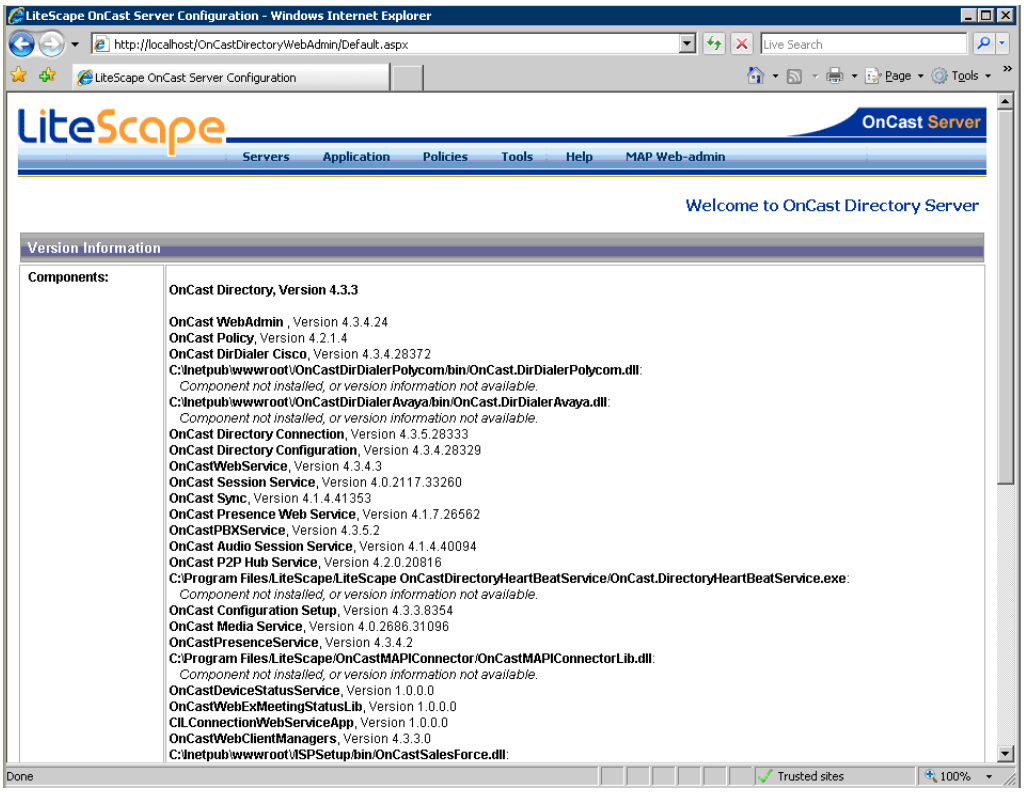
The software requirements are as follows:

- Microsoft Windows 2003 Server Enterprise Edition SP2
- Microsoft SQL Server 2005 Standard SP2
- Only required if calendaring, reporting, or presence integration is used
- Microsoft Internet Information Services 6.0 with ASP.NET 1.1 and 2.0 framework

The checklist in the OnCast Directory Administration Guide provides an easy way to record all the information you need for installation and customization/configuration. Management is performed using the web administration interfaces shown in Figure 12.

Note Documentation manuals are available from the LiteScape Partner Portal at the following URL: https://www.sharemethods.net/nepal/servlet/category3?cid=75450&csubid=75488&c3id=75661&main_only=. Note that you need a Cisco Partner login to access this LiteScape ShareMethods products manual page.

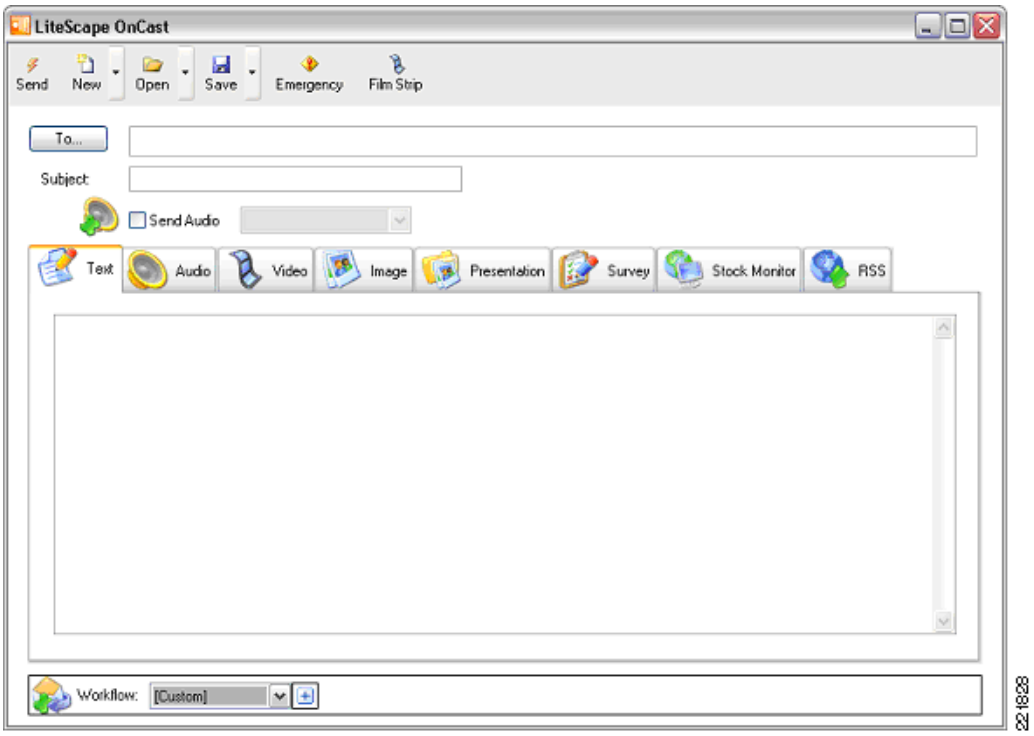
Figure 12 LiteScape OnCast Web Administration Interface



OnCast Composer

OnCast Composer (see Figure 13) allows you to create and send a variety of message types to VoIP phones from your PC.

Figure 13 OnCast Composer



Message types include the following:

- Text
- Audio
- Images
- Video
- Microsoft PowerPoint presentation shows (.pps)
- Surveys
- Stock monitor messages
- RSS messages
- Film strips

Any message type can be designated as an emergency message, which is played even if the recipient phone is in use.

A “workflow” consists of one or more keys (that is, “buttons”) that appear with a broadcast message on recipient phone screens. Each workflow button consists of at least two elements: a name and an action. You can create custom keys for use in any type of broadcast, or use the modifiable, predefined default workflow templates.

Cisco Unified Communications Media Display Solution Components

The Unified Communications Media Display solution consists of LiteScape OnCast servers and Cisco Unified Communication Manager and IP phones. To facilitate the testing of this solution, additional Cisco components were used to provide a retail network infrastructure context. A simulated retailer was created, complete with a data center and three stores; small, medium, and large. This environment provided the services and enhancements described in the following sections that contributed to the performance, security, and management of the solution.

Intelligent Retail Network

The small, medium, and large stores were built to the specifications of the IP telephony designations of the Intelligent Retail Network reference architectures. Each store consists of access routing, switching, and security services. For additional information on the Intelligent Retail Network, see the following URL: http://www.cisco.com/web/strategy/retail/irn.html.

Unified Communications

The following components were used:

- Cisco Unified Communication Manager

  The Unified Communications implementation was a default installation of Cisco Unified Communication Manager 5.1. It is assumed that an actual retailer would implement a clustered implementation of Cisco Unified Communication Manager. For additional guidance on installing Unified Communications, see the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guide09186a0080792e5e.html.

- VoIP phones

  The solution used G7.29a as the compression protocol for phone calls, and Skinny Call Control Protocol (SCCP) as the telephony control protocol. For the use of streaming media, the only currently supported phone compression codec is G7.11. This restriction is based on current OnCast Server processing capabilities. SCCP is required because the firmware image is smaller than the SIP firmware image. Current phones lack sufficient memory to support XML applications in the larger SIP image.

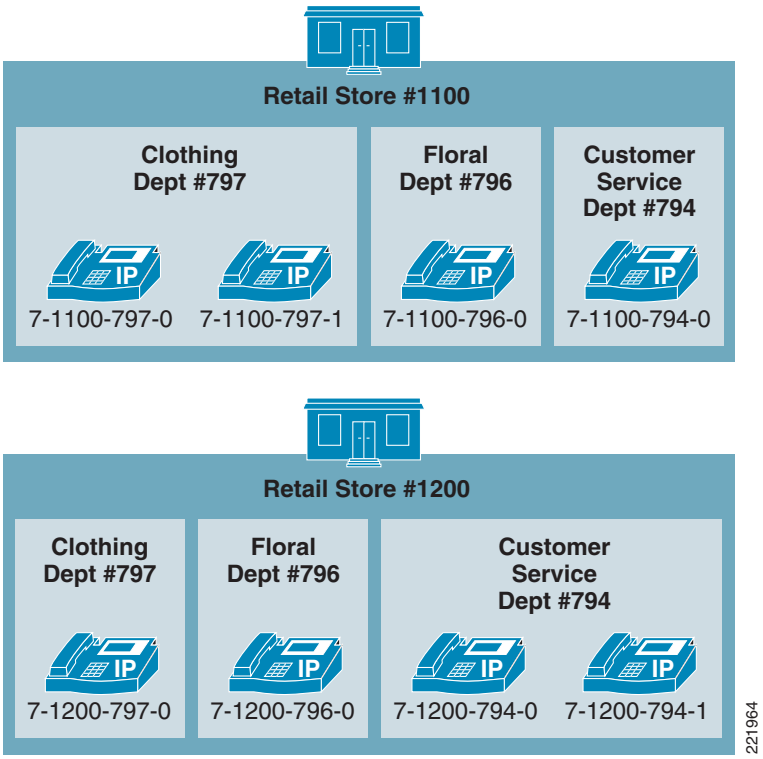
Dial Plan

The Unified Communication Media Display solution works with any existing dialing plan. The dialing plan is important because the Litescape application uses these dial numbers to identify unique endpoints when distributing media to specific departments.

Store standardization allows retailers to efficiently engineer, support, and maintain the enterprise network. Typically, retail stores are hierarchically organized by store number, department number, and extension number. A preferred dialing plan would align with existing enterprise information. Several large retailers were interviewed on how they would engineer a green field dialing plan. The Unified Communication Media Display solution utilized this logic in Cisco's labs for solution testing (see Figure 14):

Access number- store number- department number- extension number

Figure 14 Dial Plan Logic



This creates a simple 9-digit dialing plan as follows:

x-xxxx-xxx-x (for example, 7-1100-797-0 for access number, store #1100, department 797, and extension 0).

This logic provides globally unique phone numbers for each line and phone and avoids overlapping dial patterns within partitions. Using unique phone extension numbers simplifies the sending of media display information to each VoIP device without having to create additional user accounts or use an extensive naming system for each device.

For more examples of dial plan recommendations, see the Cisco Unified Communications SRND :

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a008085f6ba.html

Multicasting

The Unified Communications Media Display solution uses several types of communication. Multicast is used to send audio messaging. It is assumed that certain retailers are not willing or able to deploy multicast across the enterprise. Therefore, the Unified Communications Media Display solution has been tested using several OnCast server deployment scenarios:

- Centralized—In the small and medium store implementation, multicast was configured globally, including the corporate WAN to minimize the bandwidth impact of the audio messaging.
- Distributed—In the large store implementation, multicast was configured locally to each store and was not deployed over the corporate WAN. This requires an additional server in each store, which reduces bandwidth utilization but increases overall solution cost.

Note The choice of multicast implementation was made by the designers of the lab and does not reflect any technical difference between the relationship of the store models back to the central OnCast server. Thus, a small store retailer that is not willing to deploy multicast across the WAN can choose a distributed multicast deployment model such as that of the large store lab, and vice versa.

Multicast is a complex topic with varying degrees of design concerns for individual retailers. This document provides configuration examples that were used to provide multicast functionality within the lab. For additional multicast design guidance, see the following URL: http://www.cisco.com/en/US/tech/tk828/tech_design_guides_list.html.

Quality of Service

The Unified Communication Media Display solution can potentially be a disruptive technology if not provisioned correctly because the application and media is bandwidth consumptive (see Performance). The use quality-of-service (QoS) protects the retailer's enterprise POS, voice, and media traffic from being disturbed by other forms of consumptive traffic.

QoS in this solution is implemented as Class-Based Weighted Fair Queueing (CBWFQ) with priority express forwarding for the voice traffic. Policy maps are used to classify traffic inbound on LAN interfaces and to queue traffic outbound on WAN interfaces.

Common performance issues today are often the result of misbehaving applications generating excessive traffic. By properly classifying and queuing network traffic, performance can be greatly improved. Through the use of QoS and multicast, retailers can remain extremely conservative on their WAN bandwidth provisioning.

The method of QoS used in the lab testing was based on the Cisco Enterprise Quality of Service reference design (see Table 4).

Table 4 QoS Baseline Model

QoS Baseline Model	Description
Voice	Voice in Low Latency Queue Priority
Interactive-Video	Video conferencing in Low Latency Queue Priority
Streaming-Video	IPTV Streaming Video
Call-Signaling	Bandwidth guaranteed for Call-Signaling
IP Routing	Routing bandwidth guarantee
Network-Management	Network Management bandwidth guarantee
Mission-Critical Data	Identified Mission Critical Data (for example: POS, timeclock etc.)
Transactional Data	Transactional Data Applications (for example: media display, remote desktop, etc.
Bulk Data	General background transfer traffic (for example: file transfers, e-mail, TFTP, etc.)
Best-Effort	All other traffic not identified
Scavenger	Undesired traffic (for example: P2P file sharing, napster, etc.)

For more information on QoS, see the following URL: http://www.cisco.com/en/US/products/ps6558/prod_white_papers_list.html.

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) is configured in each store environment. SRST provides the central Cisco Unified Communication Manager functionality within the local store router in the event that the router loses communication with the Cisco Unified Communication Manager. Typically, this occurs during a WAN outage at the store. It is unlikely that the Cisco Unified Communication Manager itself will be unavailable because it is usually a clustered deployment.

The following two implementation scenarios of Unified Communications Media Display are specified:

- Centralized model—The OnCast server is centrally located. In the event of a WAN failure, Unified Communications Media Display services are unavailable until WAN service are restored.
- Distributed model—The OnCast server is both centrally located and distributed at every store. In the event of a WAN failure, OnCast services are still available via SRST services being performed by the store router.

Security

Security is an integral component of all retail networks requiring adherence to industry regulations such as the Sarbanes-Oxley Act of 2002 (SOX) and Payment Card Industry (PCI). Additional retail-focused security recommendations are located the *PCI Solution for Retail Design and Implementation Guide* at the following URL: http://www.cisco.com/web/strategy/retail/pci.html.

Segmentation for security purposes occurs in all locations. Within each store, retail traffic is segmented by type, such as point-of-sale, wireless, voice, and so on, and assigned an appropriate VLAN. The store ISR protects these segments with integrated Cisco IOS security features, such as packet filtering, stateful inspection firewall, NAT, IPS, and other services, applied as appropriate. Within the data center, segmentation and firewalling is implemented between data center services such as OnCast Directory, Cisco Unified Communication Manager, DNS, NTP, and so on. Management of network devices is secured using Access Control Server and Active Directory. This guide identifies the ports and protocols used by IP telephony with Cisco Unified Communication Manager, LiteScape OnCast Directory, and the Desktop Composer application. These services can then be accommodated in specific implementations as needed. Multicast addressing is filtered on the WAN connections to allow only the appropriate ranges used by this solution.

High Availability

Availability of telephony is a business necessity. To ensure high availability of the telephony system, the Cisco Unified Communication Manager installation used voice software in the store routers configured in SRST mode. In the event of a WAN failure, this allows the continued use of station-to-station dialing within the store as well as external calls when using local gateways to the PSTN.

LiteScape OnCast Directory operates on typical installations of Windows 2003 server; standard high availability techniques may be implemented and desired if using other available features within the product. For more details, see the OnCast Administration Guide at the following URL: https://www.sharemethods.net/nepal/servlet/category3?cid=75450&csubid=75488&c3id=75661&main_only=.

Design Considerations

Calculating Solution Traffic

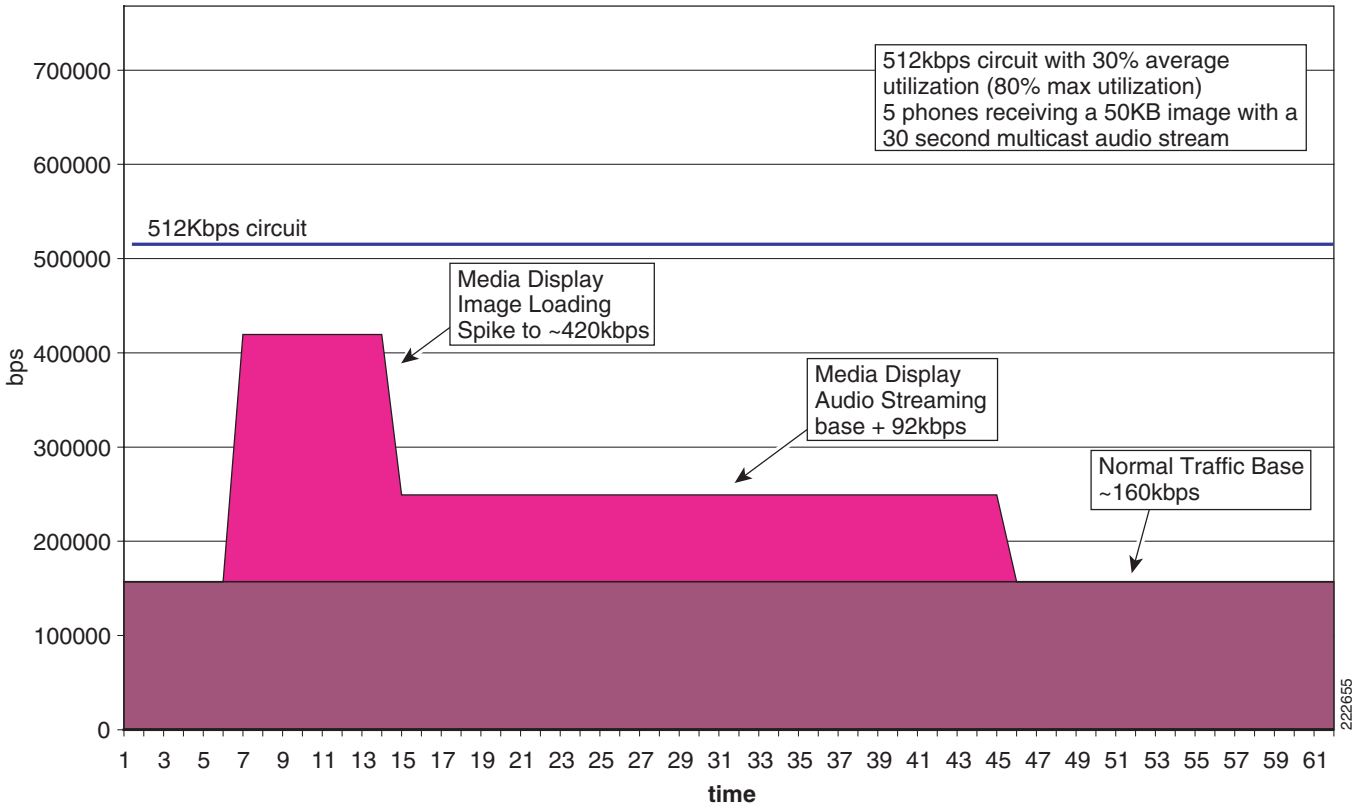
Calculating the traffic characteristics of the Unified Communications Media Display solution includes factors such as media file size, number of phones, circuit size (including average utilization), and deployment method. For example, a store with a 256 kbps circuit (average utilization of 30%, maximum utilization of 80%) sending a 50 KB image to five phones would require 16 seconds to send images to the phone:

```
IMAGE ONLY
5 phones x 50 KB image x 8 bits/Byte     2000 bits
------------------------------------ = ---------------- = ~16 seconds to transfer images
256 kbps x (80% max util- 30% avg util)  128 kbps Available
```

In another example, a store with a 512 kbps circuit (average utilization of 30%, maximum utilization of 80%) sending a 50 KB image to five phones would require 8 seconds to send images to the phone and continue to use an additional 92 kps for the duration of the audio file(see Performance):

```
IMAGE with AUDIO
5 phones x 50 KB image x 8 bits/Byte    2000 bits
------------------------------------ = ----------- = ~8 seconds to transfer images
512 kbps x (80% max util- 30% avg util) 256 kbps Available
```

Figure 15 Circuit Ultlization



See the multicast and QoS sections for optimization services that mitigate the traffic impact of the solution.

Implementing and Configuring the Solution

The Unified Communications Media Display solution was implemented and validated as a proof of concept. Testing involved the validation of functionality across a variety of Cisco IP phones within a Cisco Unified Communication Manager 5.1.2 environment. Using the three store reference architectures, each store included three phone models (7970, 7960, and 7940s) in combination with an ISR router performing SRST functionality.

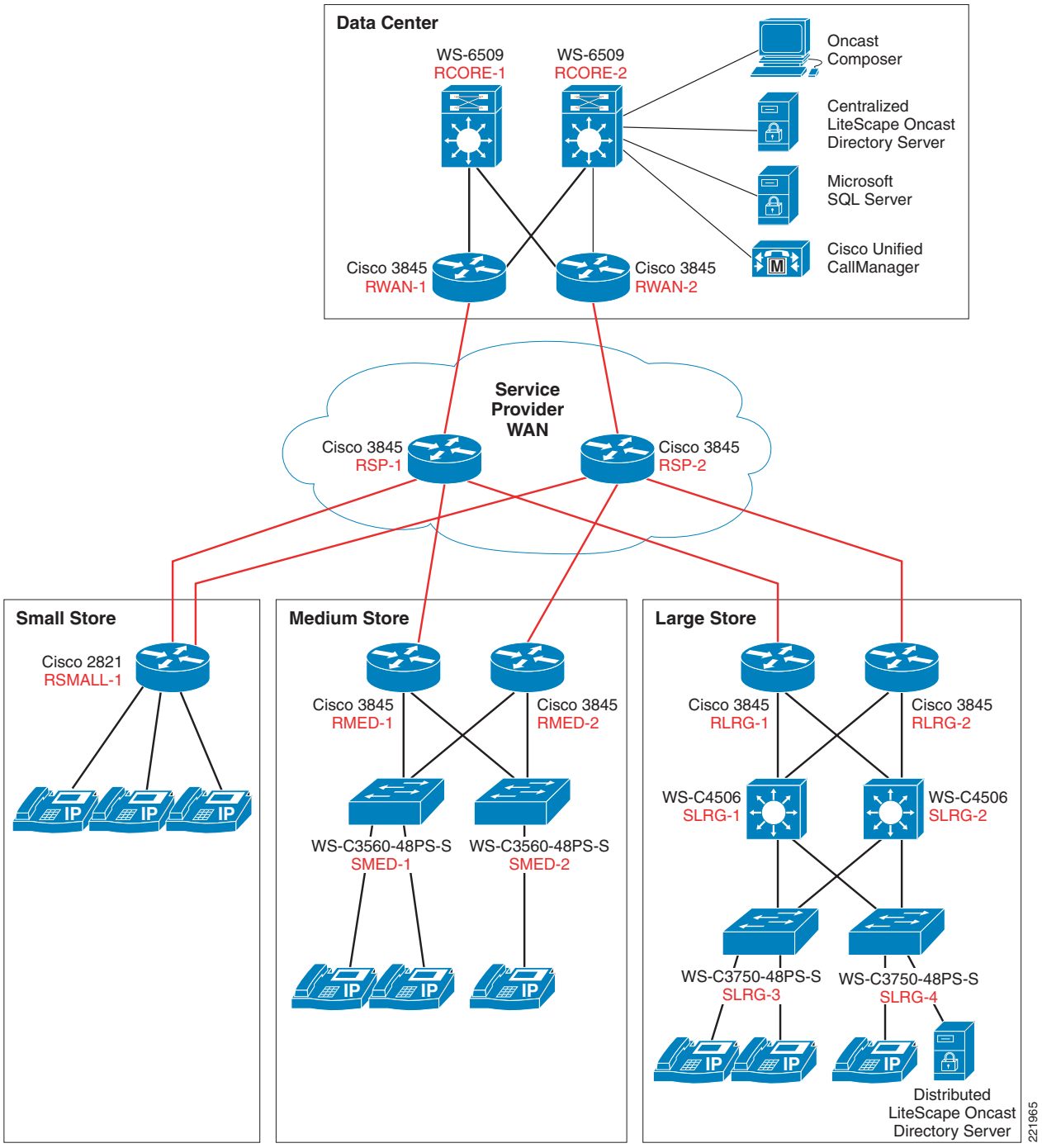
Two LiteScape OnCast Directory servers were deployed. One is located centrally in the data center location, sending media to the small and medium stores. The second server, located in the large store, synchronizes with the data center server, minimizing WAN utilization.

The goal of the testing was to articulate the functionality of the media display features of OnCast. It provides guidance on how to build various types of media messaging and distribute them to different phones in an enterprise.

Topology

The small, medium, and large Intelligent Retail Network reference architectures provide a “real world” retail contextual backdrop for this solution. Each IRN store was centrally connected to a data center with traditional data center services such as domain name service (DNS) and Network Time Protocol (NTP), as well as Cisco Unified Communication Manager and the OnCast Directory Server. The logical topology of the validation lab is represented in Figure 16. For specific places in the network details, see Appendix B—Network Diagrams, page 71.

Figure 16 Logical Topology



Testing Tools

Table 5 lists and describes the testing tools used.

Table 5 Testing Tools

Testing Tool	Function
IPerf	IPerf is a traffic generation utility. It was used to create both multicast UDP traffic as well as session-based TCP traffic simulating an FTP file transfer and web traffic stream.
Ethereal	Network traffic analyzer

Configuration Task Lists

Cisco Unified Communication Manager Server

Cisco Unified Communication Manager was installed using the current implementation guide available at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guide09186a0080792e5e.html.

The following steps outline the setup of Cisco Unified Communication Manager:

1. Installed Cisco Unified Communication Manager server 5.1.1.3000 and added service pack 5.1.2.1000 using MCS7845-H server
2. Created small, medium, and large device pools representing each store location
3. Added gateway routers and endpoint ports for small, medium, and large store routers
4. Added phones and assigned appropriate dial plan, partitions, translations, locations, and SRST settings
5. Created application user account *OCDAdmin* and assigned all available phone devices
6. Added the following roles to the OCDAdmin account:
   - Standard CCM Admin Users
   - Standard CCM Phone Management
   - Standard CCMADMIN Read Only
   - Standard CTI Allow Control of All Devices
7. Verified SNMP settings for read-only access
8. Added new Cisco Unified Communication Manager phone service for the LiteScape OnCast Directory Service: LS OnCast
9. Service URL: http://oncast.cisco-irn.com/oncastdirdialer/xmldirectory.aspx
10. Subscribed all phones to newly-created LS OnCast service

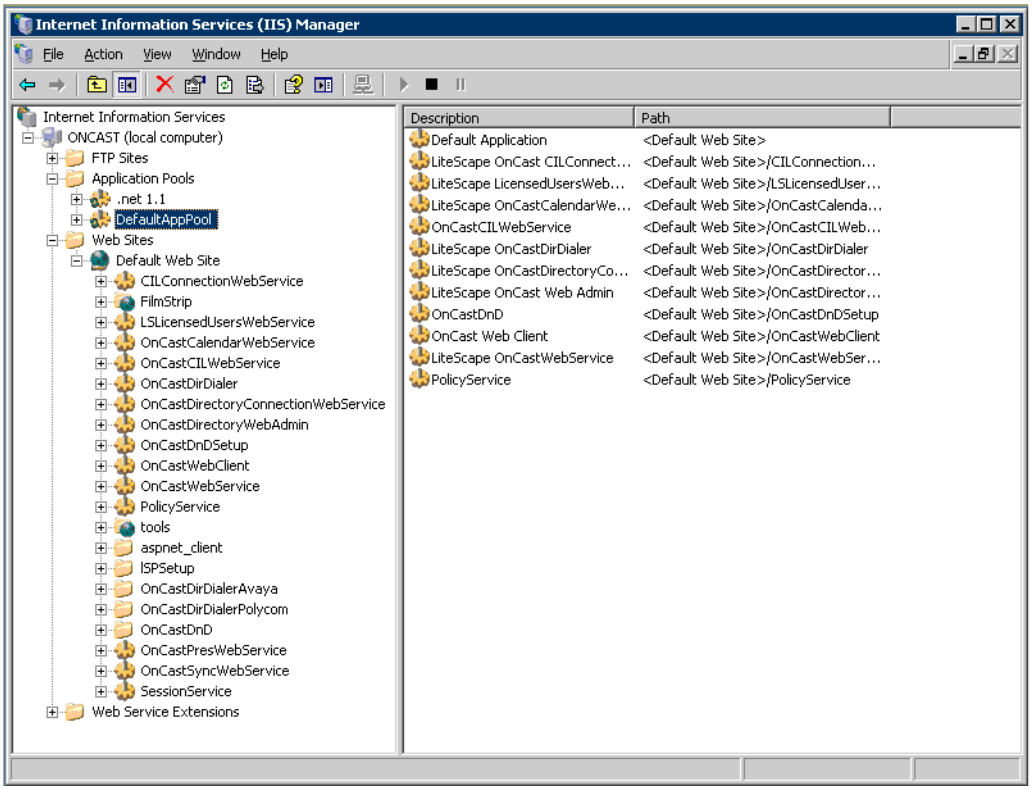
OnCast Directory Server

The LiteScape OnCast Directory server was installed using the current version of the administration guide provided with the installation software CD, and available via the LiteScape Partner Portal: https://www.sharemethods.net/nepal/servlet/category3?cid=75450&csubid=75488&c3id=75661&main_only=. Note that you need a Cisco Partner login to access this LiteScape ShareMethods products manual page.

The following steps outline the setup of the OnCast Server:

1. Created virtual machine and installed Microsoft Windows 2003 Server R2 SP2
2. Started with Microsoft Windows 2003 Server R2 SP2
3. Installed IIS 6 with ASP.Net (Microsoft .Net 1.1)
4. Installed Microsoft .Net Framework 1.1 SP1
5. Installed Microsoft .Net Framework 2.0
6. Installed Java VM version 1.4.2
7. Installed Java VM Version 1.6.0
8. Installed Java Media Framework Ver 2.1.1e
9. Copied over OnCast Directory software
10. Started the OnCastDirectoryInstaller.exe
11. Selected appropriate modules using the Advanced button, then installed the modules
12. Supplied security account information for each module as needed, including license registration file
13. Fine-tuned Microsoft IIS settings per the OnCast Administrator Guide
14. Created new AppPool based on the DefaultAppPool and named it *.net 1.1*. Assigned applications to appropriate App Pool, as shown in Figure 17.

Figure 17 IIS Application Pools



15. Changed worker processes settings for DefaultAppPool
16. Set the anonymous access account used by each virtual directory to the OCDAdmin account user

17. Changed the ASP.Net version to 2.0 for all but the last three virtual directories that OnCast created, and assigned them to the newly-created .Net 1.1 AppPool (see the OnCast Administration Guide):
    - OnCastPresWebService
    - OnCastSyncWebService
    - SessionService

Microsoft SQL Server

The following steps outline the setup of the Microsoft SQL Server:

1. Started with Microsoft Windows 2003 Server R2 SP2
2. Installed MS SQL 2005 with SP2
3. Executed OnCast Reporting database creation script
4. Executed OnCast Scheduling database creation script

OnCast Composer System

The following steps outline the setup of OnCast Composer:

1. Started with Microsoft Windows XP SP2 workstation
2. Installed Microsoft Outlook 2003 and SP2
3. Installed Java VM 1.4
4. Installed OnCast Composer
5. Configured OnCast Composer to work with Cisco Unified Communication Manager and the OnCast Directory Server

Existing Resources

The following resources were existing:

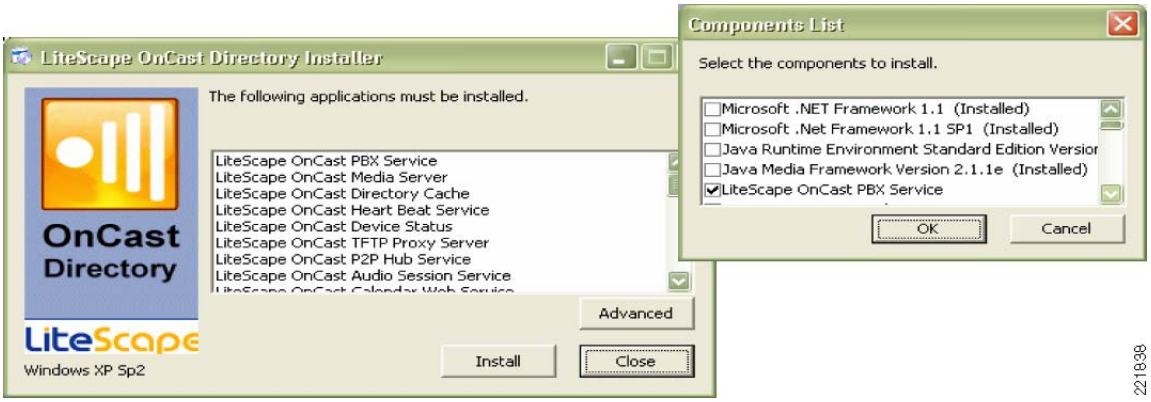
- Microsoft Active Directory Domain controller server
- Microsoft Exchange Server 2003

LiteScape OnCast Directory Server Configuration

The following steps describe how LiteScape OnCast Directory Server was configured.

1. During the first part of the installation process, the software installer prompts to install a number of OnCast services. The selection of these services can be modified by means of the advanced button, which brings up the Components List selection window, as shown in Figure 18.

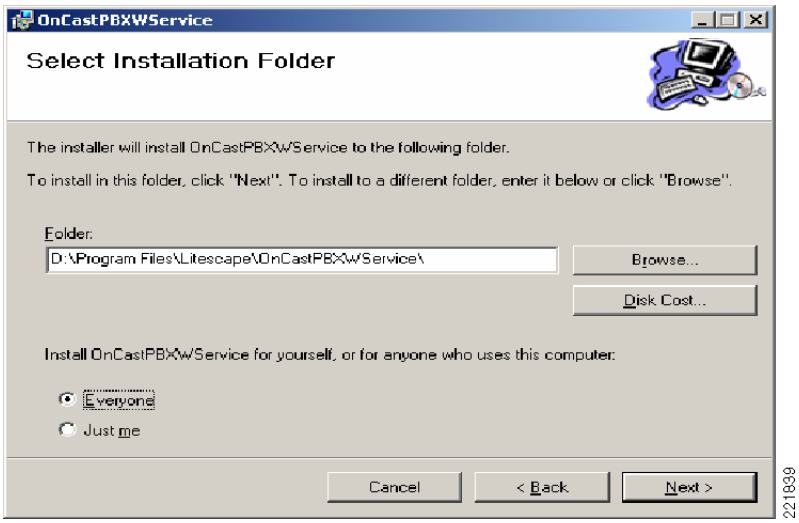
Figure 18 OnCast Installer



2. Each module executes its own installation routine with folder installation and user domain selection.

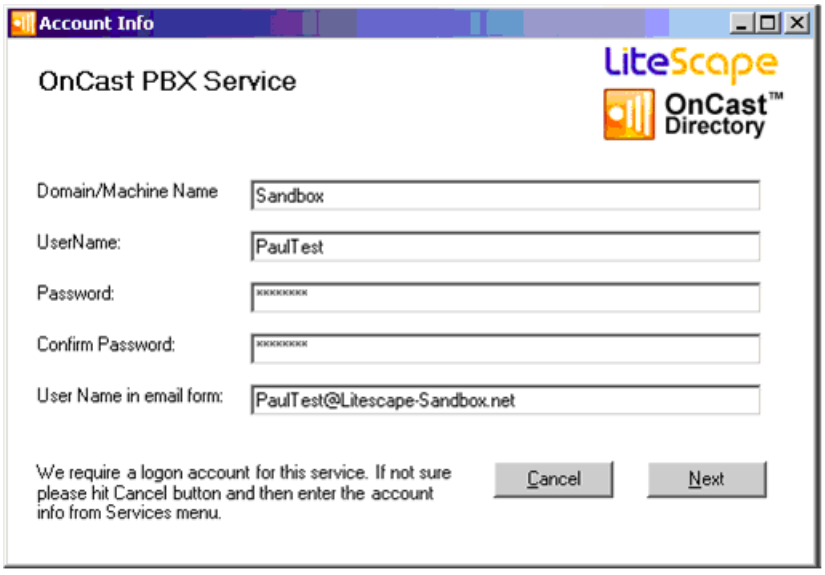
   In the Select Installation Folder screen for each module, the default folder path was used and the "Everyone" radio button was selected, as shown in Figure 19.

Figure 19 Service Installation



3. The requested information from the pre-installation checklist was entered into the Login Information screen, as shown in Figure 20.

Figure 20 Security Credentials

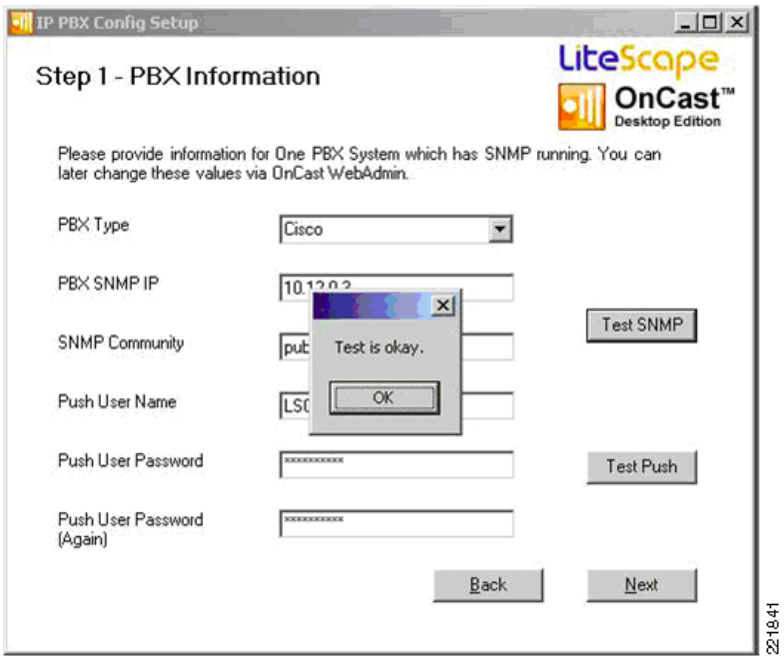


4. In the PBX Information screen in Figure 21, the following information was required:

- The PBX type—Cisco
- The IP address of the PBX that can deliver SNMP
- The SNMP community string
- The authorized username and password in the PBX that is allowed to push content to the phones

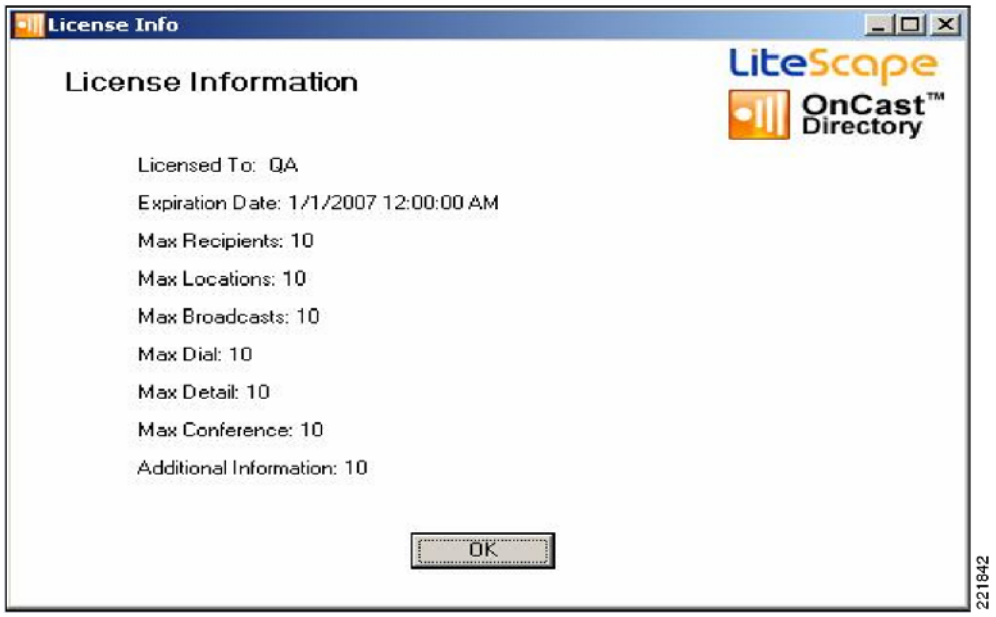
After entering the required information, the Test buttons were used to verify proper functionality.

Figure 21 PBX Information and Test Buttons



Each module installation followed these steps, and information from the pre-installation checklist was entered as appropriate. At the end of the module installation, the installation program requests a valid license file, after which the License Information screen appears, as shown in Figure 22.

Figure 22 License Screen



Troubleshooting Configuration

The OnCast Directory Server is a complex product with many configuration options. LiteScape professional services are required to properly install and integrate this solution.

The following file locations were helpful in troubleshooting issues on the OnCast Server:

1. Location of the configuration files:

   C:\Documents and Settings\All Users\Application Data\Litescape\OnCast

2. Location of the event logs:

   C:\Documents and Settings\All Users\Application Data\Litescape\OnCast\Logs

3. Location of the database configuration:

   C:\Documents and Settings\All Users\Application Data\Litescape\OnCast\AppData

For OnCast Composer:

1. Location of the configuration files:

   C:\Documents and Settings\bmcgloth\Application Data\Litescape\OnCast

2. Location of the event logs:

   C:\Documents and Settings\bmcgloth\Application Data\Litescape\OnCast\Logs

Ethereal was extremely helpful for monitoring traffic on the wire, and for validating ports and protocols used by the devices and services. An example is streaming audio being sent via unicast or multicast from the OnCast Directory Server.

IPerf was used to generate multicast, FTP, and web traffic. These flows helped identify proper queue sizing and access restrictions for QoS and multicast configurations.

Implementation Guidance

The following product components needed additional configuration after installation.

OnCast Composer

The installation of OnCast Composer required the application of an updated OIDS.xml file in support of the latest Cisco Unified Communications Manager version 5.1 SNMP MIB (this was not part of the default installer). The patch additionally required updating registry settings in support of the latest CM 5.1 locale settings. All updates are part of an updated OnCast Composer installer.

OnCast Directory Broadcast Server

The installation guide did not cover the following configuration changes that were needed:

- Configured WebDAV to allow for Composer film strips to be executed from the OnCast server
- Turned on WebDAV in IIS (IIS Manager > Web Service Extensions > WebDAV: Allowed)
- Created a new WebDAV virtual directory in IIS “FilmStrip”, pointing to directory named “c:\Documents and Settings\All Users\Application Data\Litescape\OnCast\FilmStrip”
- Installed updated Java file allowing OnCast Media Server to send packets with a TTL = 255 for multicast broadcasts.

- Updated JRE to 1.5.0_05-b05 to support the Java patch for multicast; the patch was compiled on a new SDK.

Licensing Issue Encountered

To overcome a third-party (/nsoftware ™) embedded component licensing issue that was discovered, a temporary license was applied to the lab server installation. This issue could not been replicated with a new OCD 4.3.4 SP3 install.

SQL Server

When installing the MS-SQL optional calendaring schema for the web client interface, the automatic installer did not work properly, possibly because of security issues. If the retailer uses only MS-Outlook/Exchange calendaring for scheduling, this database feature is not required.

Implementation Lessons Learned

The following items are solution details that were documented during implementation:

- When opening an already built .SET file in Film Strip, only the first extension number is listed in the TO: addresses, but other extensions exist in the system file. These extensions get overwritten when re-saving the film strip set.

  To avoid losing this information, re-enter all the desired phone extensions before re-saving film strip set.

- To be able to send multi-screen/image workflow via the OnCast Directory Server, the Film Strip .OCM files need to be manually edited and manually uploaded to the appropriate server directory.
- When adding an .OCM to a Film Strip .SET, the .OCM gets modified and updated, adding the numbers from the TO: into it when the Film Strip .SET is saved. This behavior may not be desired because the retailer may wish to send the same .OCM to different extensions on different schedules.
- When using the OnCast Directory server and sending an image with touchscreen area (image map), the image map on the touch screen does not work for 7970 phones.
- The Workflow softkey *must* be used to place the call for customer assistance.
- When trying to schedule an image to be displayed at a time in the future, the calendar button did not work within Composer.

  The workaround is to open Outlook and add an event with the .SET file attached.

- OnCast Composer periodically loses IP Communicator extensions. Removing and adding the phone extension back to Cisco Unified Communication Manager fixes the problem for a short time.

  The workaround is to manually edit the PBXDataCombo.xml file and set the file properties to read only.

Cisco Services Configuration

Multicast Implementation

Two types of multicast implementations were deployed: centralized and distributed.

Centralized Deployment Model of OnCast

Enabling multicast across the enterprise allows retailers to minimize the impact of bandwidth-consuming applications such as OnCast. The multicast service allows OnCast to send a multicast stream to the desired stores rather than unicasting an audio stream to each individual phone at each individual store.

For example, assume a retailer wants to deploy the Unified Communications Media Display solution within its stores. The retailer has 100 stores with 10 phones in each store. Without multicast enabled, 1000 audio streams (100x10) would be sent from the central OnCast server. With multicast enabled, the central OnCast server multicasts a single audio stream to each store router (100 audio streams total in this example) and allows the local store router to replicate the streams to the phones. This avoids taxing the valuable WAN bandwidth.

1. Multicast routing was enabled across all routers using the following:

   ip multicast-routing *Enables the router to route multicast traffic*

2. All routers were configured to use the loopback 0 interface of RCORE-1 as the PIM rendezvous point because it is centrally located, configured on a highly available chassis, and loopback interfaces do not fail. PIM Sparse-Dense mode was selected for its flexibility in supporting multicast applications. Every router had the following statement configured.

   ip pim rp-address 192.168.1.10 *192.168.1.10 is the loopback 0 interface of RCORE-1*

3. IP PIM Sparse-Dense Mode was used to enable interfaces that were needed to participate in the multicast domain.

```
!
interface Vlan45
 description VOICE SERVICES
 ip pim sparse-dense-mode Enables interface to receive/send multicast traffic
!
On the WAN interfaces of the WAN-facing routers, a multicast filter was applied to
protect the enterprise from rogue multicast applications consuming valuable WAN
bandwidth.
!
ip access-list standard BlockMLocal
 permit 239.192.0.0 0.0.0.255 Creates a standard access list that only permits the
multicast addressing allowed for the OnCast Directory Server.

interface Serial1/0.1 point-to-point
ip pim sparse-dense-mode
ip multicast boundary BlockMLocal  Filters unauthorized multicast traffic from
traversing the WAN. This statement stops bi directional traffic and needs to be
applied on both sides of the WAN connection.
!
```

Configurations are available in Appendix A—Configurations, page 59.

Distributed Deployment Model of OnCast

Some retailers are unable or unwilling to enable multicast across the enterprise because of management, security, or performance reasons. The Unified Communications Media Display solution supports a deployment model where the centralized OnCast directory server communicates via unicast with a distributed OnCast Directory server located within the store. This distributed local server of the store then performs the OnCast functions locally after synchronizing with the central server. This model avoids the use of multicast across the WAN and avoids the unnecessary replication of OnCast traffic across the valuable WAN bandwidth. However, the cost and management of the solution increases.

In this model, enterprise-wide multicast is not enabled; only the LAN of the local store router is enabled for multicast. The lab used the large store to test this deployment model.

1. On the store router RLRG-1

   ip multicast-routing *Enables the router to route multicast traffic*

2. Both large store routers were configured to use the loopback 0 interface of RLRG-1 as the PIM rendezvous point because it is the primary store router and its loopback interface does not fail.

   ip pim rp-address 10.10.62.1 *10.10.62.1 is the loopback 0 interface of RLRG-1*

3. IP PIM Sparse-Dense Mode was used to enable interfaces that were needed to participate in the multicast domain.

```
!
interface GigabitEthernet0/0.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.50.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode Enables GigabitEthernet0/0.13 interface to receive/send
multicast traffic
 standby 13 ip 10.10.50.1
 standby 13 priority 101
 standby 13 preempt
!
```

4. On the WAN interfaces of the large store routers, multicast was not enabled. This protects the enterprise from rogue multicast applications.

Quality of Service Implementation

The Unified Communication Media Display solution can potentially be a disruptive technology if not provisioned correctly because the application and media is bandwidth consumptive (see Performance).

The use of QoS protects the retailer's enterprise POS, voice, and media traffic from being disturbed by other forms of consumptive traffic. The following configurations were used consistently across the small, medium and large stores:

```
ip access-list extended MISSION-CRITICAL-SERVERS
remark ---POS Applications---
permit ip 192.168.52.0 0.0.0.255 any
permit ip any 192.168.52.0 0.0.0.255
ip access-list extended TRANSACTIONAL-DATA-APPS
remark ---LiteScape Application---
permit ip host 192.168.46.82 any
permit ip 239.192.0.0 0.0.0.255 any
permit ip host 239.255.255.250 any
permit ip any host 192.168.46.82
permit ip any 239.192.0.0 0.0.0.255
permit ip any host 239.255.255.250
remark ---Remote Desktop---
```

```
permit tcp any any eq 3389
permit tcp any eq 3389 any
ip access-list extended BULK-DATA-APPS
    remark ---File Transfer---
permit tcp any eq ftp any
permit tcp any eq ftp-data any
permit tcp any any eq ftp
permit tcp any any eq ftp-data
remark ---E-mail traffic---
permit tcp any any eq smtp
permit tcp any any eq pop3
permit tcp any any eq 143
permit tcp any eq smtp any
permit tcp any eq pop3 any
permit tcp any eq 143 any
remark ---other EDM app protocols---
permit tcp any any range 3460 3466
permit tcp any range 3460 3466 any
remark ---messaging services---
permit tcp any any eq 2980
permit tcp any eq 2980 any
remark ---Microsoft file services---
permit tcp any any range 137 139
permit tcp any range 137 139 any
ip access-list extended NET-MGMT-APPS
remark - Router user Authentication - Identifies TACACS Control traffic
permit tcp any any eq tacacs
permit tcp any eq tacacs any



class-map match-all VOICE
match ip dscp ef                  ! IP Phones mark Voice to EF
class-map match-all INTERACTIVE-VIDEO
match ip dscp af41 af42           ! Recommended markings for IP/VC
class-map match-any CALL-SIGNALING
match ip dscp cs3                 ! Call-Signaling marking
class-map match-all ROUTING
match ip dscp cs6                 ! Routers mark Routing traffic to CS6
class-map match-all NET-MGMT
match ip dscp cs2                 ! Recommended marking for Network Management
class-map match-all MISSION-CRITICAL-DATA
match ip dscp 25                  ! Interim marking for Mission-Critical Data
class-map match-all TRANSACTIONAL-DATA
match ip dscp af21 af22           ! Recommended markings for Transactional Data
class-map match-all BULK-DATA
match ip dscp af11 af12           ! Recommended markings for Bulk Data
class-map match-all SCAVENGER
match ip dscp cs1                 ! Recommended marking for Scavenger traffic

class-map match-all BRANCH-MISSION-CRITICAL
match access-group name MISSION-CRITICAL-SERVERS

class-map match-any BRANCH-BULK-DATA
match protocol tftp           ! Identifies TFTP traffic - Retailers
match protocol nfs            ! Identifies NFS traffic - Retailers
match access-group name BULK-DATA-APPS   ! ACL to reference

class-map match-any BRANCH-TRANSACTIONAL-DATA    ! Must use "match-any"
match protocol citrix                    ! Identifies Citrix traffic
match protocol ldap                      ! Identifies LDAP traffic
match protocol telnet                    ! Identifies Telnet traffic
match protocol sqlnet                    ! Identifies Oracle SQL*NET traffic
match protocol http url "*SalesReport*"  ! Identifies "SalesReport" URLs
```

```
match access-group name TRANSACTIONAL-DATA-APPS  ! Other Apps

class-map match-any BRANCH-NET-MGMT
match protocol snmp        ! Identifies SNMP traffic
match protocol syslog      ! Identifies Syslog traffic
match protocol dns         ! Identifies DNS traffic
match protocol icmp        ! Identifies ICMP traffic
match protocol ssh         ! Identifies SSH traffic
match access-group name NET-MGMT-APPS  ! Other Network Management Apps

class-map match-any BRANCH-SCAVENGER
match protocol napster     ! Identifies Napster traffic
match protocol gnutella    ! Identifies Gnutella traffic
match protocol fasttrack   ! Identifies KaZaa (v1) traffic
match protocol kazaa2      ! Identifies KaZaa (v2) traffic
!
policy-map BRANCH-LAN-EDGE-IN
class BRANCH-MISSION-CRITICAL
set ip dscp 25
class BRANCH-TRANSACTIONAL-DATA
set ip dscp af21     ! Transactional Data apps are marked to DSCP AF21
class BRANCH-NET-MGMT
set ip dscp cs2      ! Network Management apps are marked to DSCP CS2
class BRANCH-BULK-DATA
set ip dscp af11     ! Bulk data apps are marked to AF11
class BRANCH-SCAVENGER
set ip dscp cs1      ! Scavenger apps are marked to DSCP CS1

policy-map BRANCH-WAN-EDGE
class VOICE
priority percent 18  ! Voice gets 552 kbps of LLQ
class INTERACTIVE-VIDEO
priority percent 15  ! 384 kbps IP/VC needs 460 kbps of LLQ
class CALL-SIGNALING
bandwidth percent 5  ! Minimal BW guarantee for Call-Signaling
class ROUTING
bandwidth percent 3  ! Routing class gets 3% explicit BW guarantee
class NET-MGMT
bandwidth percent 2  ! Net-Mgmt class gets 2% explicit BW guarantee
class MISSION-CRITICAL-DATA
bandwidth percent 15 ! Mission-Critical class gets min 15% BW guarantee
random-detect        ! Enables WRED on Mission-Critical Data class
class TRANSACTIONAL-DATA
bandwidth percent 12 ! Transactional-Data class gets min 12% BW guarantee
random-detect dscp-based ! Enables DSCP-WRED on Transactional-Data class
class BULK-DATA
bandwidth percent 4  ! Bulk Data class gets 4% BW guarantee
random-detect dscp-based ! Enables DSCP-WRED on Bulk-Data class
class SCAVENGER
bandwidth percent 1  ! Scavenger class is throttled
class class-default
bandwidth percent 25 ! Default class gets min 25% BW guarantee
random-detect        ! Enables WRED on the default class

policy-map BRANCH-LAN-EDGE-OUT
class class-default



interface Serial0/0/1:0
description T1 to SERVICE PROVIDER
frame-relay traffic-shaping
max-reserved-bandwidth 100               ! overrides the default 75% BW limit
```

```
interface Serial0/0/1:0.1 point-to-point
description PVC CONNECTION TO DATACENTER
frame-relay interface-dlci 201
  class fr_qos

map-class frame-relay fr_qos
 frame-relay fragment 160
 frame-relay traffic-rate 1536000 1536000
 frame-relay adaptive-shaping becn
 service-policy output BRANCH-WAN-EDGE

interface VlanXX
 description POS
 no service-policy input set_priority
 service-policy output BRANCH-LAN-EDGE-OUT
 service-policy input BRANCH-LAN-EDGE-IN
```

Survivable Remote Site Telephony Implementation

In the event that the store WAN goes down or if the store router loses connection to the central Cisco Unified Communication Manager, SRST allows the store router to perform the Cisco Unified Communication Manager functions during its absence. This not only allows the store voice services to remain functional but within the context of the Unified Communications Media Display, it allows the OnCast Directory Services to remain functional. This feature is available only in the distributed model of OnCast deployment; for example, where the large store architecture has a server deployed onsite.

Security

Table 6 lists the ports and protocols used by the Unified Communications Media Display Solution.

Table 6 Traffic Flows

Source Device	Source port	Destination Device	Destination Port	Protocol	Comments
OnCast Server data center	<HIGH>	MS-SQL	1433	TCP	OnCast read and write to SQL Server
OnCast Server large store	<HIGH>	MS-SQL	1433	TCP	OnCast read and write to SQL Server
XP Composer Station	<HIGH>	Phones	80	TCP	Composer sent post back URL to phones
Phones	<HIGH>	XP Composer Station	5050	TCP	Phones perform an HTTP Request to Composer on port 5050
XP Composer Station	<HIGH>	Phones	<HIGH>	UDP	Composer sending unicast audio stream
XP Composer Station	<HIGH>	MS Exchange	135	TCP	Composer looking up phone numbers and names
XP Composer Station	<HIGH>	MS Exchange	1040	TCP	Composer looking up phone numbers and names

Table 6 Traffic Flows (continued)

XP Composer Station	<HIGH>	MS Exchange	1115	TCP	Composer looking up names MAPI request
XP Composer Station	2060	Cisco Unified Communication Manager	69 (high)	UDP	Composer gets ring list via TFTP (sets up negotiated port)
XP Composer Station	162	Cisco Unified Communication Manager	161	UDP	Composer queries Cisco Unified Communication Manager
Cisco Unified Communicatio n Manager	161	XP Composer Station	162	UDP	Cisco Unified Communication Manager reply to Composer
XP Composer Station	<HIGH>	Microsoft	80	TCP	Code signature check
XP Composer Station	<HIGH>	OnCast Server data center	80	TCP	Composer sending a set to OnCast Server
XP Composer Station	<HIGH>	OnCast Server data center	80	TCP	Composer checking for remote film strip sets on OnCast Server
XP Composer Station	333	231.31.31.31	333	UDP	Composer multicast to OnCast Server
Web client users	<HIGH>	OnCast Server data center	80	TCP	Web client interface
OnCast Server data center	<HIGH>	Phones	80	TCP	OnCast Server to phones
Phones	<HIGH>	OnCast Server data center	80	TCP	Phones to OnCast Server
OnCast Server data center	<HIGH>	Active Directory	389	TCP	Server performing an LDAP lookup
OnCast Server data center	<HIGH>	Phones	<HIGH>	UDP	OnCast sending unicast audio stream
OnCast Server data center	<HIGH>	239.192.0.0-255	<HIGH>	UDP	Sending multicast audio stream
OnCast Server data center	<HIGH>	Active Directory	53	UDP	DNS lookup
OnCast Server data center	<HIGH>	OnCast Server large store	80	TCP	Data center OnCast Server forwards set to large store OnCast Server via HTTP
Phones	68	255.255.255.255	67	UDP	DHCP request for services
Phones	<HIGH>	Cisco Unified Communication Manager	69 (high)	UDP	Check phone load file
Phones	<HIGH>	Cisco Unified Communication Manager	6970	TCP	Register with Cisco Unified Communication Manager

Table 6 Traffic Flows (continued)

XP Composer Station	<HIGH>	MS Exchange	1115	TCP	Composer looking up names MAPI request
XP Composer Station	2060	Cisco Unified Communication Manager	69 (high)	UDP	Composer gets ring list via TFTP (sets up negotiated port)
XP Composer Station	162	Cisco Unified Communication Manager	161	UDP	Composer queries Cisco Unified Communication Manager
Cisco Unified Communicatio n Manager	161	XP Composer Station	162	UDP	Cisco Unified Communication Manager reply to Composer
XP Composer Station	<HIGH>	Microsoft	80	TCP	Code signature check
XP Composer Station	<HIGH>	OnCast Server data center	80	TCP	Composer sending a set to OnCast Server
XP Composer Station	<HIGH>	OnCast Server data center	80	TCP	Composer checking for remote film strip sets on OnCast Server
XP Composer Station	333	231.31.31.31	333	UDP	Composer multicast to OnCast Server
Web client users	<HIGH>	OnCast Server data center	80	TCP	Web client interface
OnCast Server data center	<HIGH>	Phones	80	TCP	OnCast Server to phones
Phones	<HIGH>	OnCast Server data center	80	TCP	Phones to OnCast Server
OnCast Server data center	<HIGH>	Active Directory	389	TCP	Server performing an LDAP lookup
OnCast Server data center	<HIGH>	Phones	<HIGH>	UDP	OnCast sending unicast audio stream
OnCast Server data center	<HIGH>	239.192.0.0-255	<HIGH>	UDP	Sending multicast audio stream
OnCast Server data center	<HIGH>	Active Directory	53	UDP	DNS lookup
OnCast Server data center	<HIGH>	OnCast Server large store	80	TCP	Data center OnCast Server forwards set to large store OnCast Server via HTTP
Phones	68	255.255.255.255	67	UDP	DHCP request for services
Phones	<HIGH>	Cisco Unified Communication Manager	69 (high)	UDP	Check phone load file
Phones	<HIGH>	Cisco Unified Communication Manager	6970	TCP	Register with Cisco Unified Communication Manager

Table 6 Traffic Flows (continued)

Phones	<HIGH>	Cisco Unified Communication Manager	2000	TCP	Register with Cisco Unified Communication Manager-Skinny
Phones	<HIGH>	SRST Router	2000	TCP	SRST/Skinny keepalive
Phones	<HIGH>	Cisco Unified Communication Manager	8080	TCP	Check services, directory
Phones	ICMP	OnCast Server data center	ICMP	ICMP	Destination port unreachable

Multicast

Multicast routing can be a potential security/performance risk. The nature of multicast is dynamic and pervasive throughout the enterprise. Cisco recommends that filters be placed on the WAN routers, both central at the data center and local to the store edge, that specifically allow approved address ranges. The Oncast Directory server uses multicast addressing with in the range of 239.192.0.0 /24.

Testing

Test Plan

Testing included creating several types of media and sending them to various phones using the several methods available. Some methods of sending content were not able to support all of the desired tests. The sending methods used are as follows:

- Composer from Desktop
- Composer via Film Strip
- Composer to OnCast Directory Server Film Strip service
- OnCast Directory Server Web Client Interface
- Composer to OnCast Directory Server Film Strip service (multicast)

The following tests were performed (test results are listed in Figure 30):

1. Display text message on all phones

   Store alert: “POS systems have gone down and the issue will be resolved in 15 minutes”
2. Display single image set on all phones
3. Display two image sets on all phones with softkey button transition to second image
4. Display image and play audio file on all phones
5. Display image and provide softkey to play audio file on all phones
6. Display image and softkey/touchscreen to call customer assistance (data center phone)
7. Display and take survey on all phones:

   How was our service? 1. Great, 2. Good, and 3. Needs improvement

   Receive survey results from e-mail, and send to the summary to the Exchange server group account media—display@cisco-irn.com
8. Schedule an image to display at a future time to designated phones (7970 only—small, medium, and large)
9. Display a 5-image film strip on all phones using Composer and OnCast Directory Server

Testing Steps

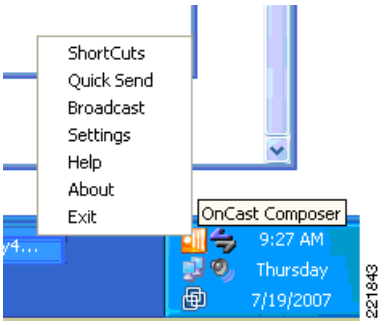
Many of the tests used OnCast Composer to create the media that was sent to the phones.

The following steps describe one of the tests where an image and audio track were sent to a group of phones using the Film Strip feature.

Sending Media Using Composer

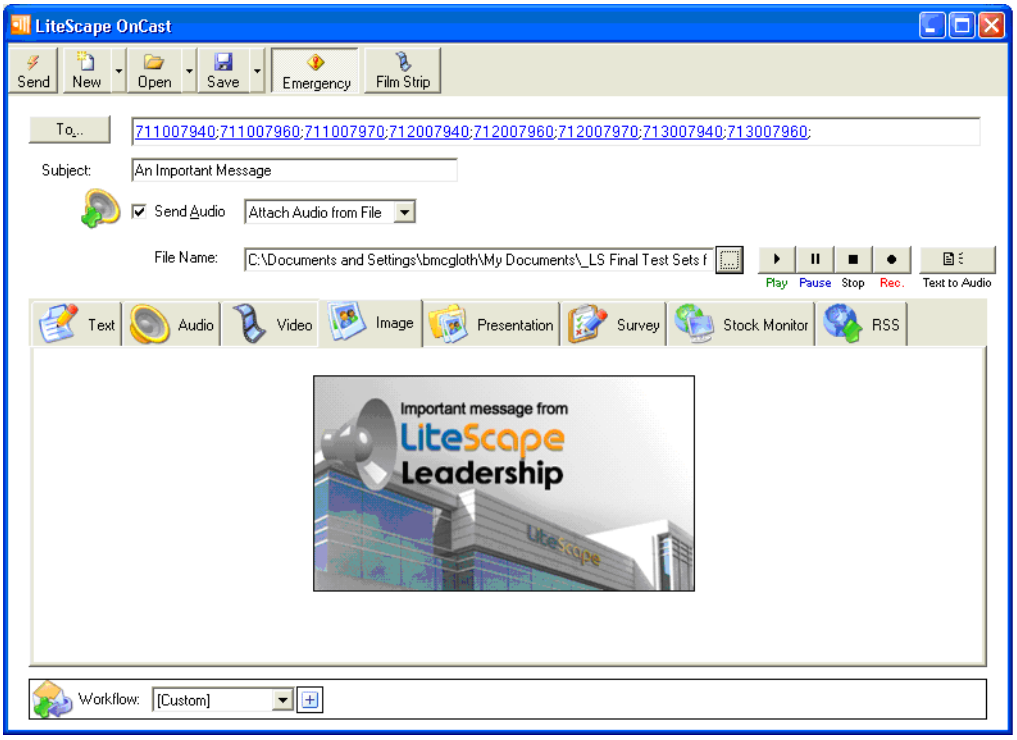
1. Composer was opened by right-clicking on the task tray icon and **Broadcast** was selected, as shown in Figure 23.

Figure 23 Selecting Broadcast Option



2. After OnCast Composer was open, the video button was selected, the desired destination device phone numbers were entered, an image and audio track were selected, and the Emergency button was clicked, as shown in Figure 24.

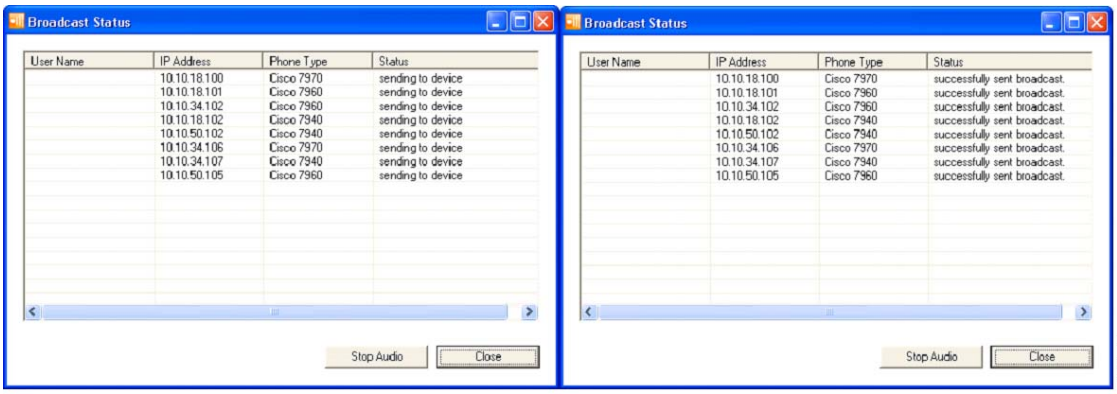
Figure 24 Creating Image and Audio Set



3. This information can now be sent to the selected phone endpoints by pressing the **Send** button.
4. After pressing the Send button, a screen opens that shows the status of the media transmission, as shown in Figure 25.

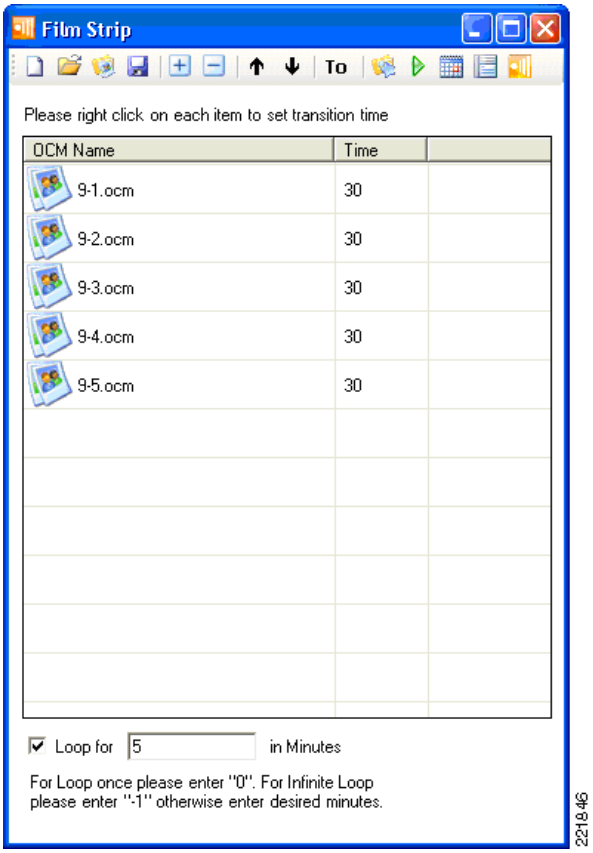
   Each of the entered phone numbers is translated into the appropriate device IP address based on information retrieved from the Cisco Unified Communication Manager server using SNMP.

Figure 25 Media Transmission



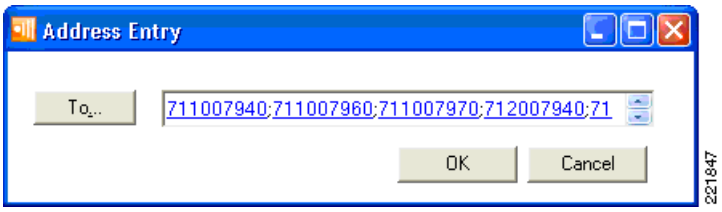
5. To send multiple sets of differing media to the devices in succession, save each composition separately. Open the Film Strip module by pressing the button in Composer. In Film Strip, open and add each saved media set, adjust the transition time between OCM items, and select a total loop runtime, as shown in Figure 26.

Figure 26 Film Strip



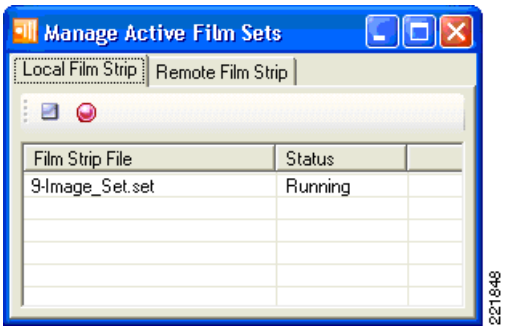
6. To send the film strip set, you enter the desired destination numbers in the “TO” list. This is a popup window that appears after pressing the “to” button, as shown in Figure 27. Save the strip set, then press the green Play button to send the media set to the selected phones.

Figure 27 Destination Device Address Entry



7. After the film strip set has been sent, monitor its status using the monitoring utility, as shown in Figure 28.

Figure 28 Active Strip Sets

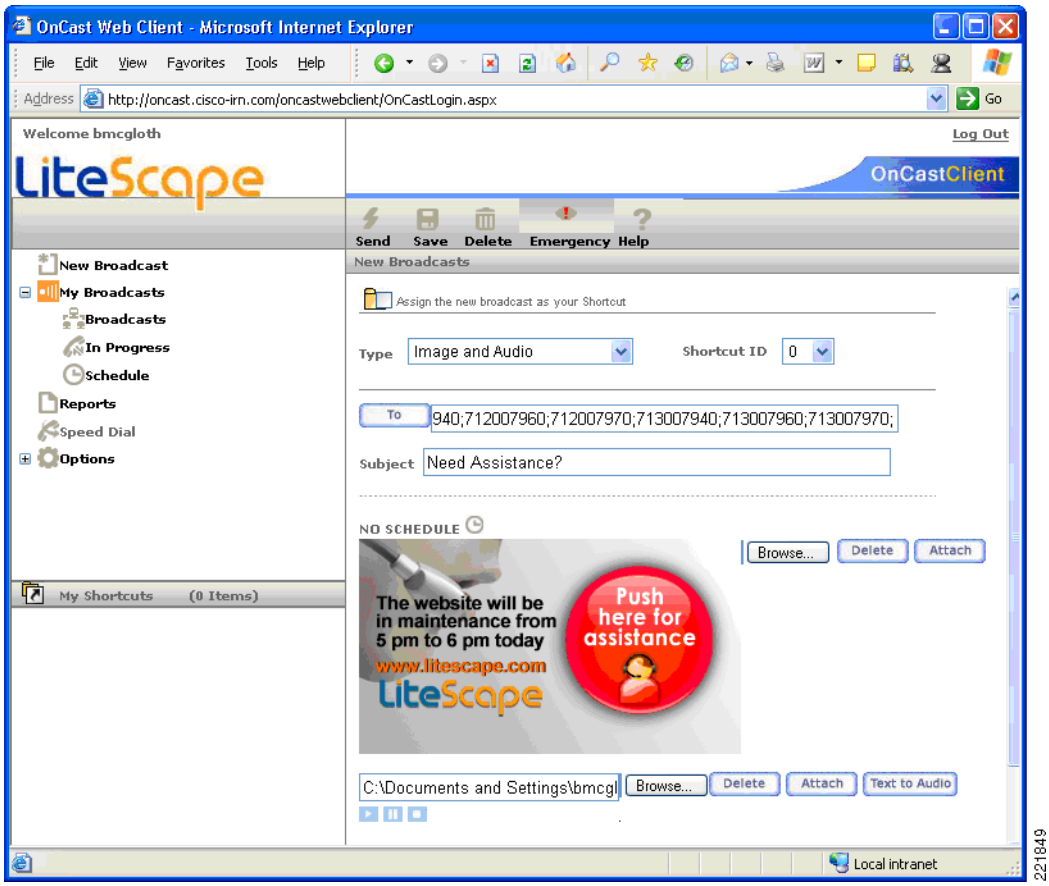


8. Sending tests via the OnCast Directory server Film Strip service via Composer is accomplished by selecting the orange button in the upper right corner of the Film Strip window, as shown in Figure 26.

Sending Media using OnCast Web Client

Much of the same functionality available in OnCast Composer is available by using the OnCast Directory Server web client interface. An example of this interface is shown in Figure 29.

Figure 29 OnCast Directory Server Web Interface



Test Results

Figure 30 summarizes the results achieved from the tests performed as outlined in Testing Steps, page 50.

Figure 30 OnCast Testing Results

Tests	Times			Small			Medium			Large-Unicast			Large-Distributed		
	Init	end	clear	7970	7960	7940	7970	7960	7940	7970	7960	7940	7970	7960	7940
Display text only message															
Test 1 to phones - Composer from desktop	0:04	no end	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC			
Test 1 to phones - Composer via Strip	0:04	2:39	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC			
Test 1 to phones - Composer to server	0:08	2:38	3:39	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Test 1 to phones - Server Web Interface	0:04	0:35	0:35	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Display single image															
Test 2 to phones - Composer from desktop	0:07	no end	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC			
Test 2 to phones - Composer via Strip	0:08	2:54	3:28	OK	OK	OK	OK	OK	OK	OK	OK	OK			
Test 2 to phones - Composer to server	0:06	2:32	3:05	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Test 2 to phones - Server Web Interface	0:03	0:39	0:39	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Display image with softkey to show a second image															
Test 3 to phones - Composer from desktop	0:06	no end	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC			
Test 3 to phones - Composer via Strip-no touch	0:06	2:48	4:27	OK	OK	OK	OK	OK	OK	OK	OK	OK			
Test 3 to phones - Composer via Strip-press softkey	0:06	2:46	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC			
Test 3 to phones - Composer to server	0:04	no end	4:48	W	W	W	W	W	W	W	W	W	W	W	W
Display image while playing Audio file															
Test 4 to phones - Composer from desktop	0:06	no end	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC			
Test 4 to phones - Composer via Strip	0:11	2:32	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC			
Test 4 to phones - Composer to server	0:08	2:46	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
Test 4 to phones - Server Web Interface	0:04	0:48	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
Test 4 to phones - Composer to server-Mcast	0:10	2:54	no clear	NC	NC	NC	NC	NC	NC				NC	NC	NC
Show image, press key to hear message															
Test 5 to phones - Composer from desktop	0:08	no end	no clear	ANC	ANC	ANC	ANC	ANC	ANC	ANC	ANC	ANC			
Test 5 to phones - Composer via Strip	0:06	2:55	no clear	ANC	ANC	ANC	ANC	ANC	ANC	ANC	ANC	ANC			
Test 5 to phones - Composer to server	0:04	2:58	3:39	W	W	W	W	W	W	W	W	W	W	W	W
Call for assistance															
Test 6 to phones - Composer from desktop	0:08	no end	no clear	NC	NC	NC	NC	NC	NC	NC	NC	NC			
Test 6 to phones - Composer via Strip	0:07	2:31	3:37	OK	OK	OK	OK	OK	OK	OK	OK	OK			
Test 6 to phones - Composer to server	0:09	2:35	3:24	W	OK	OK	W	OK	OK	W	OK	OK	W	OK	OK
Take a Survey															
Test 7 to phones - Composer from desktop	0:09	no end	+0.45	OK	OK	OK	OK	OK	OK	OK	OK	OK			
Schedule image to display at future time															
Test 8 to phones - Composer from Outlook	0:55	3:48	4:51	OK	OK	OK	OK	OK	OK	OK	OK	OK			
Test 8 to phones - Composer via Outlook to server	1:14	3:51	4:11	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Test 8 to phones - Server Web Interface	0:12	1:37	1:37	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
Send a 5 image strip using 30sec interval for 5 minutes															
Test 9 to phones - Composer via Strip	0:07	5:36	7:10	OK	OK	OK	OK	OK	OK	OK	OK	OK			
Test 9 to phones - Composer to server	0:09	5:42	5:54	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK

Test results KEY
W - Workflow problem A - Audio problem, not received X - Set not received NC - Set received, phone did not clear after set >3 min OK - All received ok, phone cleared after set automatically

221850

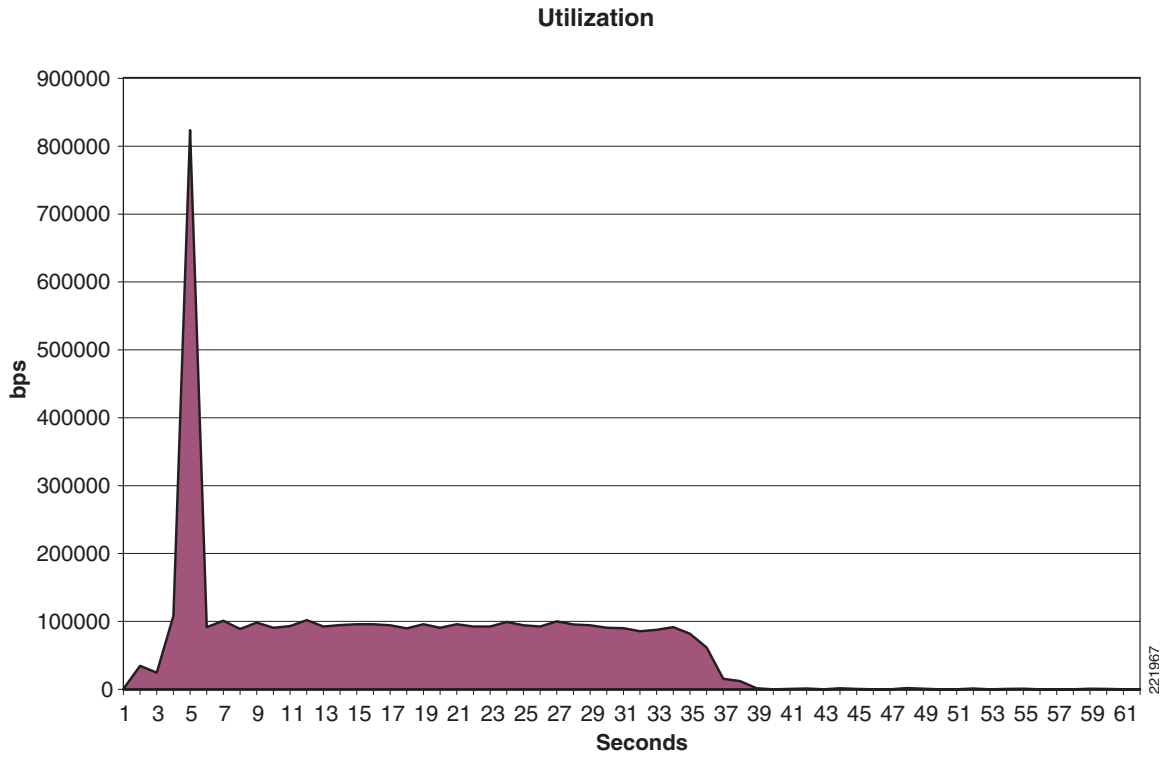
Performance

The following data characterizes the traffic generated by the media sent to a single phone during testing. Figure 31 shows the utilization as captured on the network. This transmission uses G7.11. Future codec support will include G7.29a.

- Sending image from server to phone:
  - Size of image file—79 KB
  - Network traffic from phone to server—96 KB
  - Network traffic from phone to server—3 Kb
  - Phone traffic to and from Cisco Unified Communication Manager—1.6 KB
  - Average throughput of image—500 Kbps for 1.5 seconds
- Sending image and 35 second audio clip to phone:

- Network traffic from server to phone—479 KB
- Network traffic from phone to server—8 Kb
- Traffic to and from Cisco Unified Communication Manager—3.8 KB
- Average throughput of audio stream—92 Kbps for 36 seconds
- Average throughput of audio and image—109 Kbps for 36 seconds
- Size of image file—79 KB
- Size of WAV audio file—274 KB

Figure 31 Traffic Utilization for Single Phone—Image and Audio Clip Stream



Testing Lessons Learned

The following items were documented during testing:

- Test 3—Display two image sets on all phones with softkey button transition to second image.
  - During Test 3 from the Composer local service, the screens cleared after about four minutes on all phones except for those that had their soft key pressed. The phones that had their softkey pressed to go to the next image stay on the current image and do not clear within five minutes.
  - Sending dual image in a workflow (Test 3 using just the first .OCM) via the server, when clicking the softkey on 7940/60 phones, the screen changes and displays “none”; no image is displayed. On 7970 models, the screen clears altogether.

  - Sending dual image using two .OCM files, images rotate as expected from a film strip set. Soft buttons do not work properly on each .OCM. If no softkeys are pressed, images clear off phone properly.

- Test 5—Display image and provide softkey to play audio file on all phones.
  - Test 5 sent to the server loaded and cleared fine, but when pressing softkey to listen to audio, the next broadcast with the audio showed page “none”, the same as in Test 3. Server does not support issues with workflows sent via the Composer Film Strip interface.
- Test 6—Display image and softkey/touchscreen to call customer assistance (data center phone).
  - Test 6 clears screen after call to customer assistance completes. If no call is placed, screens stay on the image.
- Test 7—Display and take survey on all phones.
  - The best implementation for a survey was to use a workflow starting with an image broadcast and a softkey to a text survey. The survey sent e-mail results per phone well. Another method was using an image with soft command keys that send the key name pressed as an e-mail (that is, good, great, poor messages). The only issue of this method was the limited amount of text allowed for a button (Cisco phone limitation).

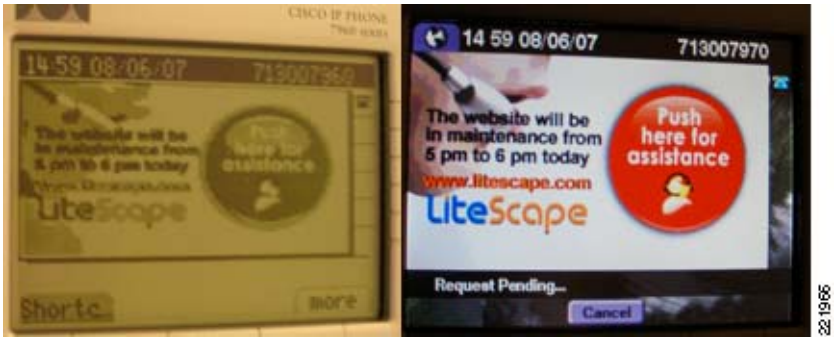
All sets sent using Film Strip were set to 30 seconds each and to loop for two minutes.

Summary and Recommendations

The Cisco Unified Communications Media Display solution successfully delivers a variety of capabilities, including the delivery of multimedia content (kiosk replacement), corporate messaging, and two-way communications.

The Cisco VoIP phones perform well as a substitute to a media kiosk for customer-facing deployments. The Cisco 7970 phone is the recommended phone to display images and messaging, because the color display provides a higher fidelity for photos and images. The monochrome 7960 and 7940 phone displays are not as clear when showing color source images (see Figure 32). Media content should be carefully reviewed before delivery to these phones.

Figure 32 Comparison of Phone Images



Surveys and voice communication enable immediate responses from end users. Survey results are easily collected through e-mail messages delivered from each phone.

A deployment model leveraging multicast and QoS are critical to the successful implementation of streaming media across a retail network. Because the media stream uses the G.711 codec, a substantial amount of bandwidth is consumed (over 100 kbps). If multicast is not used, several phones at a store could easily overwhelm the WAN link. For stores with a large number of phones, there is a significant value in deploying a distributed media server or some form of caching engine to reduce impact to the store WAN link.

The LiteScape OnCast application used in the Unified Communications Media Display solution demonstrates the additional value that can be achieved with an IP phone deployment in contrast to traditional PBX systems.

Appendix A—Configurations

QoS

Data Center

WAN Routers

```
ip access-list extended MISSION-CRITICAL-SERVERS
remark ---POS Applications---
permit ip 192.168.52.0 0.0.0.255 any
permit ip any 192.168.52.0 0.0.0.255
ip access-list extended TRANSACTIONAL-DATA-APPS
remark ---LiteScape Application---
permit ip host 192.168.46.82 any
permit ip 239.192.0.0 0.0.0.255 any
permit ip host 239.255.255.250 any
permit ip any host 192.168.46.82
permit ip any 239.192.0.0 0.0.0.255
permit ip any host 239.255.255.250
remark ---Remote Desktop---
permit tcp any any eq 3389
permit tcp any eq 3389 any
ip access-list extended BULK-DATA-APPS
    remark ---File Transfer---
permit tcp any eq ftp any
permit tcp any eq ftp-data any
permit tcp any any eq ftp
permit tcp any any eq ftp-data
remark ---E-mail traffic---
permit tcp any any eq smtp
permit tcp any any eq pop3
permit tcp any any eq 143
permit tcp any eq smtp any
permit tcp any eq pop3 any
permit tcp any eq 143 any
remark ---other EDM app protocols---
permit tcp any any range 3460 3466
permit tcp any range 3460 3466 any
remark ---messaging services---
permit tcp any any eq 2980
permit tcp any eq 2980 any
remark ---Microsoft file services---
permit tcp any any range 137 139
permit tcp any range 137 139 any

ip access-list extended NET-MGMT-APPS
remark - Router user Authentication - Identifies TACACS Control traffic
permit tcp any any eq tacacs
permit tcp any eq tacacs any



class-map match-any DATACENTER-MISSION-CRITICAL
match access-group name MISSION-CRITICAL-SERVERS

class-map match-any DATACENTER-BULK-DATA
match protocol tftp           ! Identifies TFTP traffic - Retailers
```

```
match protocol nfs            ! Identifies NFS traffic - Retailers
match access-group name BULK-DATA-APPS   ! ACL to reference

class-map match-any DATACENTER-TRANSACTIONAL-DATA  ! Must use "match-any"
match protocol citrix                    ! Identifies Citrix traffic
match protocol ldap                      ! Identifies LDAP traffic
match protocol telnet                    ! Identifies Telnet traffic
match protocol sqlnet                    ! Identifies Oracle SQL*NET traffic
match protocol http url "*SalesReport*"  ! Identifies "SalesReport" URLs
match access-group name TRANSACTIONAL-DATA-APPS  ! Other Apps

class-map match-any DATACENTER-NET-MGMT
match protocol snmp        ! Identifies SNMP traffic
match protocol syslog      ! Identifies Syslog traffic
match protocol dns         ! Identifies DNS traffic
match protocol icmp        ! Identifies ICMP traffic
match protocol ssh         ! Identifies SSH traffic
match access-group name NET-MGMT-APPS  ! Other Network Management Apps

class-map match-any DATACENTER-SCAVENGER
match protocol napster     ! Identifies Napster traffic
match protocol gnutella    ! Identifies Gnutella traffic
match protocol fasttrack   ! Identifies KaZaa (v1) traffic
match protocol kazaa2      ! Identifies KaZaa (v2) traffic
!
policy-map DATACENTER-LAN-EDGE-IN
class DATACENTER-MISSION-CRITICAL
set ip dscp 25
class DATACENTER-TRANSACTIONAL-DATA
set ip dscp af21     ! Transactional Data apps are marked to DSCP AF21
class DATACENTER-NET-MGMT
set ip dscp cs2      ! Network Management apps are marked to DSCP CS2
class DATACENTER-BULK-DATA
set ip dscp af11     ! Bulk data apps are marked to AF11
class DATACENTER-SCAVENGER
set ip dscp cs1      ! Scavenger apps are marked to DSCP CS1

class-map match-all VOICE
match ip dscp ef                  ! IP Phones mark Voice to EF
class-map match-all INTERACTIVE-VIDEO
match ip dscp af41 af42           ! Recommended markings for IP/VC
class-map match-all STREAMING-VIDEO
match ip dscp cs4     ! Recommended marking for Streaming-Video
class-map match-any CALL-SIGNALING
match ip dscp cs3                 ! Call-Signaling marking
class-map match-all ROUTING
match ip dscp cs6                 ! Routers mark Routing traffic to CS6
class-map match-all NET-MGMT
match ip dscp cs2                 ! Recommended marking for Network Management
class-map match-all MISSION-CRITICAL-DATA
match ip dscp 25                  ! Interim marking for Mission-Critical Data
class-map match-all TRANSACTIONAL-DATA
match ip dscp af21 af22           ! Recommended markings for Transactional Data
class-map match-all BULK-DATA
match ip dscp af11 af12           ! Recommended markings for Bulk Data
class-map match-all SCAVENGER
match ip dscp cs1                 ! Recommended marking for Scavenger traffic

policy-map WAN-EDGE
class VOICE
priority percent 18 ! Voice gets 552 kbps of LLQ
class INTERACTIVE-VIDEO
priority percent 15 ! 384 kbps IP/VC needs 460 kbps of LLQ
class CALL-SIGNALING
```

```
bandwidth percent 5 ! BW guarantee for Call-Signaling
class ROUTING
bandwidth percent 3 ! Routing class gets explicit BW guarantee
class NET-MGMT
bandwidth percent 2 ! Net-Mgmt class gets explicit BW guarantee
class MISSION-CRITICAL-DATA
bandwidth percent 10 ! Mission-Critical class gets 10% BW guarantee
random-detect ! Enables WRED for Mission-Critical Data class
class TRANSACTIONAL-DATA
bandwidth percent 7 ! Transactional-Data class gets 7% BW guarantee
random-detect dscp-based ! Enables DSCP-WRED for Transactional-Data class
class BULK-DATA
bandwidth percent 4 ! Bulk Data remains at 4% BW guarantee
random-detect dscp-based ! Enables DSCP-WRED for Bulk-Data class
class STREAMING-VIDEO
bandwidth percent 10 ! Streaming-Video class gets 10% BW guarantee
class SCAVENGER
bandwidth percent 1 ! Scavenger class is throttled
class class-default
bandwidth percent 25 ! Class-Default gets 25% min BW guarantee
random-detect ! Enables WRED on class-default
```

```
policy-map DATACENTER-LAN-EDGE-OUT
class class-default
set cos dscp

interface GigabitEthernet0/0
description ALL interfaces
service-policy input DATACENTER-LAN-EDGE-IN  ! Marks Data on ingress
interface GigabitEthernet0/1
description ALL interfaces
service-policy input DATACENTER-LAN-EDGE-IN  ! Marks Data on ingress
```

```
interface serial 1/0
description T3 to SERVICE PROVIDER
frame-relay traffic-shaping
max-reserved-bandwidth 100                ! overrides the default 75% BW limit

interface Serial1/0.3 point-to-point
description PVC to STORE
frame-relay interface-dlci 1003
class fr_qos

map-class frame-relay fr_qos
 frame-relay fragment 160
 frame-relay traffic-rate 1536000 1536000
 frame-relay adaptive-shaping becn
 service-policy output WAN-EDGE
```

All Stores

```
ip access-list extended MISSION-CRITICAL-SERVERS
remark ---POS Applications---
permit ip 192.168.52.0 0.0.0.255 any
permit ip any 192.168.52.0 0.0.0.255
ip access-list extended TRANSACTIONAL-DATA-APPS
```

```
remark ---LiteScape Application---
permit ip host 192.168.46.82 any
permit ip 239.192.0.0 0.0.0.255 any
permit ip host 239.255.255.250 any
permit ip any host 192.168.46.82
permit ip any 239.192.0.0 0.0.0.255
permit ip any host 239.255.255.250
remark ---Remote Desktop---
permit tcp any any eq 3389
permit tcp any eq 3389 any
ip access-list extended BULK-DATA-APPS
    remark ---File Transfer---
permit tcp any eq ftp any
permit tcp any eq ftp-data any
permit tcp any any eq ftp
permit tcp any any eq ftp-data
remark ---E-mail traffic---
permit tcp any any eq smtp
permit tcp any any eq pop3
permit tcp any any eq 143
permit tcp any eq smtp any
permit tcp any eq pop3 any
permit tcp any eq 143 any
remark ---other EDM app protocols---
permit tcp any any range 3460 3466
permit tcp any range 3460 3466 any
remark ---messaging services---
permit tcp any any eq 2980
permit tcp any eq 2980 any
remark ---Microsoft file services---
permit tcp any any range 137 139
permit tcp any range 137 139 any
ip access-list extended NET-MGMT-APPS
remark - Router user Authentication - Identifies TACACS Control traffic
permit tcp any any eq tacacs
permit tcp any eq tacacs any
```

```
class-map match-all VOICE
match ip dscp ef                  ! IP Phones mark Voice to EF
class-map match-all INTERACTIVE-VIDEO
match ip dscp af41 af42           ! Recommended markings for IP/VC
class-map match-any CALL-SIGNALING
match ip dscp cs3                 ! Call-Signaling marking
class-map match-all ROUTING
match ip dscp cs6                 ! Routers mark Routing traffic to CS6
class-map match-all NET-MGMT
match ip dscp cs2                 ! Recommended marking for Network Management
class-map match-all MISSION-CRITICAL-DATA
match ip dscp 25                  ! Interim marking for Mission-Critical Data
class-map match-all TRANSACTIONAL-DATA
match ip dscp af21 af22           ! Recommended markings for Transactional Data
class-map match-all BULK-DATA
match ip dscp af11 af12           ! Recommended markings for Bulk Data
class-map match-all SCAVENGER
match ip dscp cs1                 ! Recommended marking for Scavenger traffic

class-map match-all BRANCH-MISSION-CRITICAL
match access-group name MISSION-CRITICAL-SERVERS

class-map match-any BRANCH-BULK-DATA
match protocol tftp           ! Identifies TFTP traffic - Retailers
```

```
match protocol nfs            ! Identifies NFS traffic - Retailers
match access-group name BULK-DATA-APPS   ! ACL to reference

class-map match-any BRANCH-TRANSACTIONAL-DATA! Must use "match-any"
match protocol citrix                    ! Identifies Citrix traffic
match protocol ldap                      ! Identifies LDAP traffic
match protocol telnet                    ! Identifies Telnet traffic
match protocol sqlnet                    ! Identifies Oracle SQL*NET traffic
match protocol http url "*SalesReport*"  ! Identifies "SalesReport" URLs
match access-group name TRANSACTIONAL-DATA-APPS  ! Other Apps

class-map match-any BRANCH-NET-MGMT
match protocol snmp        ! Identifies SNMP traffic
match protocol syslog      ! Identifies Syslog traffic
match protocol dns         ! Identifies DNS traffic
match protocol icmp        ! Identifies ICMP traffic
match protocol ssh         ! Identifies SSH traffic
match access-group name NET-MGMT-APPS  ! Other Network Management Apps

class-map match-any BRANCH-SCAVENGER
match protocol napster     ! Identifies Napster traffic
match protocol gnutella    ! Identifies Gnutella traffic
match protocol fasttrack   ! Identifies KaZaa (v1) traffic
match protocol kazaa2      ! Identifies KaZaa (v2) traffic
!
policy-map BRANCH-LAN-EDGE-IN
class BRANCH-MISSION-CRITICAL
set ip dscp 25
class BRANCH-TRANSACTIONAL-DATA
set ip dscp af21     ! Transactional Data apps are marked to DSCP AF21
class BRANCH-NET-MGMT
set ip dscp cs2      ! Network Management apps are marked to DSCP CS2
class BRANCH-BULK-DATA
set ip dscp af11     ! Bulk data apps are marked to AF11
class BRANCH-SCAVENGER
set ip dscp cs1      ! Scavenger apps are marked to DSCP CS1

policy-map BRANCH-WAN-EDGE
class VOICE
priority percent 18  ! Voice gets 552 kbps of LLQ
class INTERACTIVE-VIDEO
priority percent 15  ! 384 kbps IP/VC needs 460 kbps of LLQ
class CALL-SIGNALING
bandwidth percent 5  ! Minimal BW guarantee for Call-Signaling
class ROUTING
bandwidth percent 3  ! Routing class gets 3% explicit BW guarantee
class NET-MGMT
bandwidth percent 2  ! Net-Mgmt class gets 2% explicit BW guarantee
class MISSION-CRITICAL-DATA
bandwidth percent 15 ! Mission-Critical class gets min 15% BW guarantee
random-detect        ! Enables WRED on Mission-Critical Data class
class TRANSACTIONAL-DATA
bandwidth percent 12 ! Transactional-Data class gets min 12% BW guarantee
random-detect dscp-based ! Enables DSCP-WRED on Transactional-Data class
class BULK-DATA
bandwidth percent 4  ! Bulk Data class gets 4% BW guarantee
random-detect dscp-based ! Enables DSCP-WRED on Bulk-Data class
class SCAVENGER
bandwidth percent 1  ! Scavenger class is throttled
class class-default
bandwidth percent 25 ! Default class gets min 25% BW guarantee
random-detect        ! Enables WRED on the default class

policy-map BRANCH-LAN-EDGE-OUT
```

```
class class-default

map-class frame-relay fr_qos
 frame-relay fragment 160
 frame-relay traffic-rate 1536000 1536000
 frame-relay adaptive-shaping becn
 service-policy output BRANCH-WAN-EDGE


interface Serial0/0/1:0
description T1 to SERVICE PROVIDER
frame-relay traffic-shaping
max-reserved-bandwidth 100                ! overrides the default 75% BW limit

interface Serial0/0/1:0.1 point-to-point
description PVC CONNECTION TO DATACENTER
frame-relay interface-dlci 201
  class fr_qos

interface VlanXX
 description POS
 no service-policy input set_priority
 service-policy output BRANCH-LAN-EDGE-OUT
 service-policy input BRANCH-LAN-EDGE-IN
```

Survivable Remote Site Telephony

RLRG-1

```
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
application
 global
  service alternate default
!
call fallback active
!
ccm-manager fallback-mgcp
ccm-manager mgcp
!
mgcp
mgcp call-agent 192.168.45.181 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode cisco
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp sdp simple
mgcp bind control source-interface loopback 0
mgcp bind media source-interface loopback 0
!
mgcp profile default
!
dial-peer cor custom
 name nr
!
```

```
dial-peer cor list nr
 member nr
!
dial-peer voice 1 voip
!
dial-peer voice 2 pots
!
dial-peer voice 18 pots
 service mgcpapp
 direct-inward-dial
 port 0/3/0
!
call-manager-fallback
 max-conferences 2 gain -6
 transfer-system full-consult
 ip source-address 10.10.50.2 port 2000 strict-match
 max-ephones 10
 max-dn 20
 cor incoming nr 1 8001 - 8999
!
```

RLRG-2

```
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
application
 global
  service alternate default
!
call fallback active
!
ccm-manager fallback-mgcp
ccm-manager mgcp
!
mgcp
mgcp call-agent 192.168.45.181 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode cisco
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp sdp simple
mgcp bind control source-interface loopback 0
mgcp bind media source-interface loopback 0
!
mgcp profile default
!
dial-peer cor custom
 name nr
!
dial-peer cor list nr
 member nr
!
dial-peer voice 1 voip
!
dial-peer voice 2 pots
!
dial-peer voice 18 pots
 service mgcpapp
 direct-inward-dial
```

```
 port 0/3/0
!
call-manager-fallback
 max-conferences 2 gain -6
 transfer-system full-consult
 ip source-address 10.10.50.2 port 2000 strict-match
 max-ephones 10
 max-dn 20
 cor incoming nr 1 8001 - 8999
!
```

Multicast

Data Center

RCORE-1

```
ip multicast-routing
ip pim bidir-enable
!
interface Loopback0
 ip pim sparse-dense-mode
!
interface Vlan42
 description
 ip pim sparse-dense-mode
!
interface Vlan45
 description Voice Services
 ip pim sparse-dense-mode
!
interface Vlan46
 description
ip pim sparse-dense-mode
!
interface Vlan101
description
 ip pim sparse-dense-mode
!
interface Vlan104
description
 ip pim sparse-dense-mode

ip pim bidir-enable
ip pim rp-address 192.168.1.10
```

RCORE-2

```
ip multicast-routing
!
interface Vlan102
 description
 ip pim sparse-dense-mode

!
interface Vlan103
 description
```

```
 ip pim sparse-dense-mode
!
ip pim rp-address 192.168.1.10

No active Sources on Core 2
```

WAN Routers

RWAN-1

```
    ip multicast-routing

    interface GigabitEthernet0/0
    ip pim sparse-dense-mode
    !
    interface GigabitEthernet0/1
    ip pim sparse-dense-mode

    interface Serial1/0.1 point-to-point
    ip pim sparse-dense-mode
    ip multicast boundary BlockMLocal
    !!
    interface Serial1/0.2 point-to-point
    ip pim sparse-dense-mode
    ip multicast boundary BlockMLocal
    !
    interface Serial1/0.3 point-to-point

    <none>

    ip pim rp-address 192.168.1.10

    ip access-list standard BlockMLocal
     permit 239.192.0.0 0.0.0.255
```

RWAN-2

```
ip multicast-routing

interface GigabitEthernet0/0
ip pim sparse-dense-mode
!
interface GigabitEthernet0/1
ip pim sparse-dense-mode

interface Serial1/0.1 point-to-point
ip pim sparse-dense-mode
ip multicast boundary BlockMLocal
!!
interface Serial1/0.2 point-to-point
ip pim sparse-dense-mode
ip multicast boundary BlockMLocal
!
interface Serial1/0.3 point-to-point

<none>

ip pim rp-address 192.168.1.10
```

```
ip access-list standard BlockMLocal
 permit 239.192.0.0 0.0.0.255
```

Small Store

RSMALL-1

```
ip multicast-routing
!
interface Serial0/0/0:0.1 point-to-point
description RSMALL-1 CONNECTION RSP-1
ip pim sparse-dense-mode
ip multicast boundary BlockMLocal
!
interface Serial0/0/1:0.1 point-to-point
description RSMALL-1 CONNECTION RSP-2
ip pim sparse-dense-mode
ip multicast boundary BlockMLocal
!
interface Vlan11
description POS
ip pim sparse-dense-mode
!
interface Vlan13
description VOICE
ip pim sparse-dense-mode
!

ip pim rp-address 192.168.1.10

ip access-list standard BlockMLocal
 permit 239.192.0.0 0.0.0.255
```

Medium Store

RMED-1

```
ip multicast-routing
!
interface GigabitEthernet0/0.11
 description POS
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/0.13
 description VOICE
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO RMED2 VIA SMED2
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/1.101
description ROUTER LINK TO RMED-2
ip pim sparse-dense-mode
!
interface Serial0/0/0:0.1 point-to-point
description CONNECTION TO RWAN-1
ip pim sparse-dense-mode
```

```
ip multicast boundary BlockMLocal
!
interface Vlan13
description VOICE
ip pim sparse-dense-mode
!

ip pim rp-address 192.168.1.10

ip access-list standard BlockMLocal
 permit 239.192.0.0 0.0.0.255
```

RMED-2

```
ip multicast-routing
!
interface GigabitEthernet0/0.11
 description POS
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/0.13
 description VOICE
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO RMED2 VIA SMED2
 ip pim sparse-dense-mode
!

interface GigabitEthernet0/1.101
 description ROUTER LINK TO RMED1 VIA SMED2
ip pim sparse-dense-mode
!
interface Serial0/0/0:0.1 point-to-point
description CONNECTION TO RWAN-1
ip pim sparse-dense-mode
ip multicast boundary BlockMLocal
!
interface Vlan13
description VOICE
ip pim sparse-dense-mode
!

ip pim rp-address 192.168.1.10

ip access-list standard BlockMLocal
 permit 239.192.0.0 0.0.0.255
```

Large Store

RLRG-1

```
ip multicast-routing

!
interface Loopback0
description RP for Multicast
 ip pim sparse-dense-mode
```

```
!
interface GigabitEthernet0/0.11
description POS
ip pim sparse-dense-mode
!
interface GigabitEthernet0/0.12
 description DATA
ip pim sparse-dense-mode
!
interface GigabitEthernet0/0.13
 description VOICE
ip pim sparse-dense-mode
!
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO RLRG-2 VIA SLRG-2
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/1.101
description ROUTER LINK TO RLRG-2 VIA SLRG-2
ip pim sparse-dense-mode
!
```

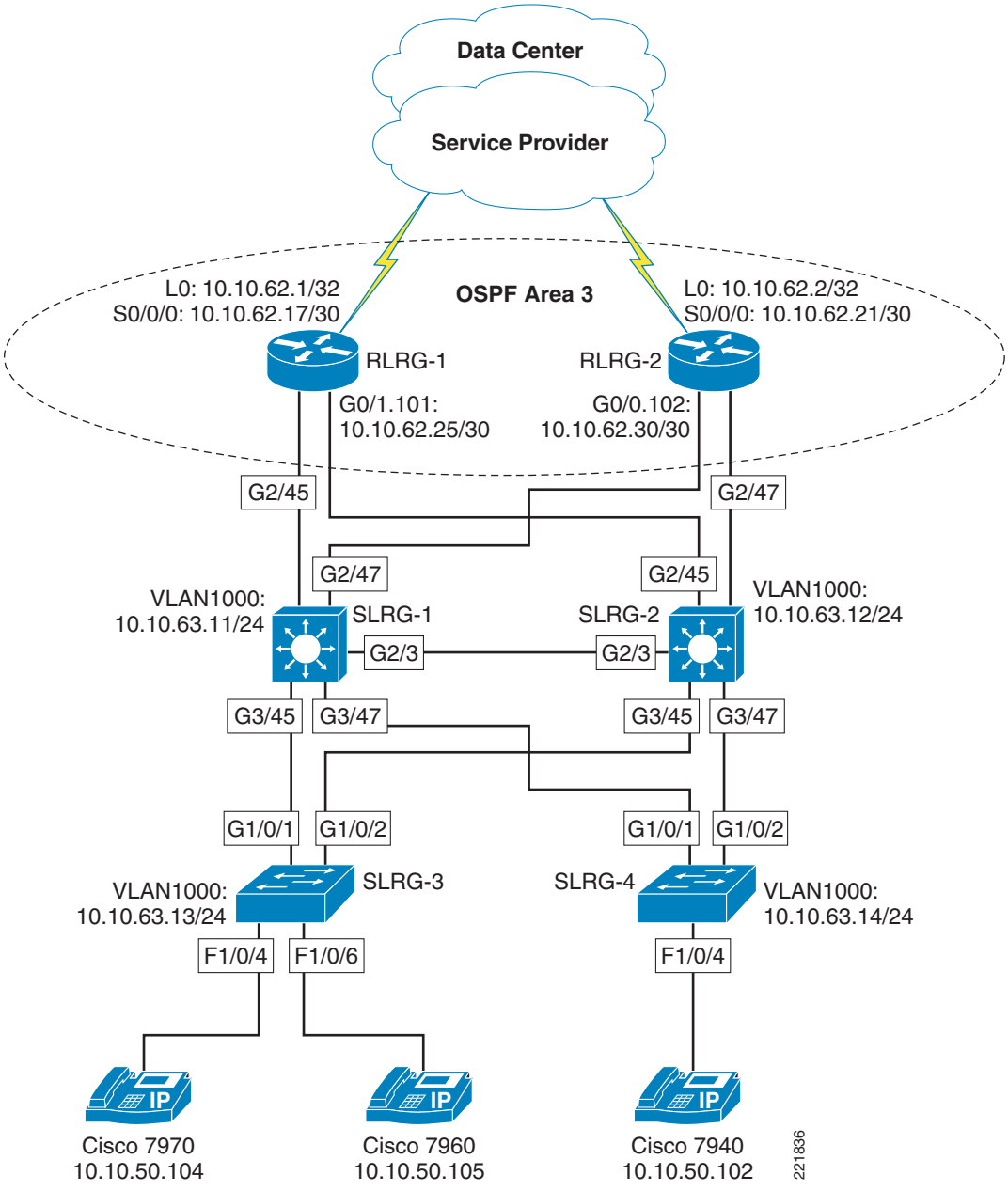
RLRG-2

```
ip multicast-routing
!
interface GigabitEthernet0/1.11
description POS
ip pim sparse-dense-mode
!
interface GigabitEthernet0/1.12
 description DATA
ip pim sparse-dense-mode
!
interface GigabitEthernet0/1.13
 description VOICE
ip pim sparse-dense-mode
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO RLRG-1 VIA SLRG-1
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/1.101
description ROUTER LINK TO RLRG-1 VIA SLRG-1
ip pim sparse-dense-mode
!
```

Appendix B—Network Diagrams

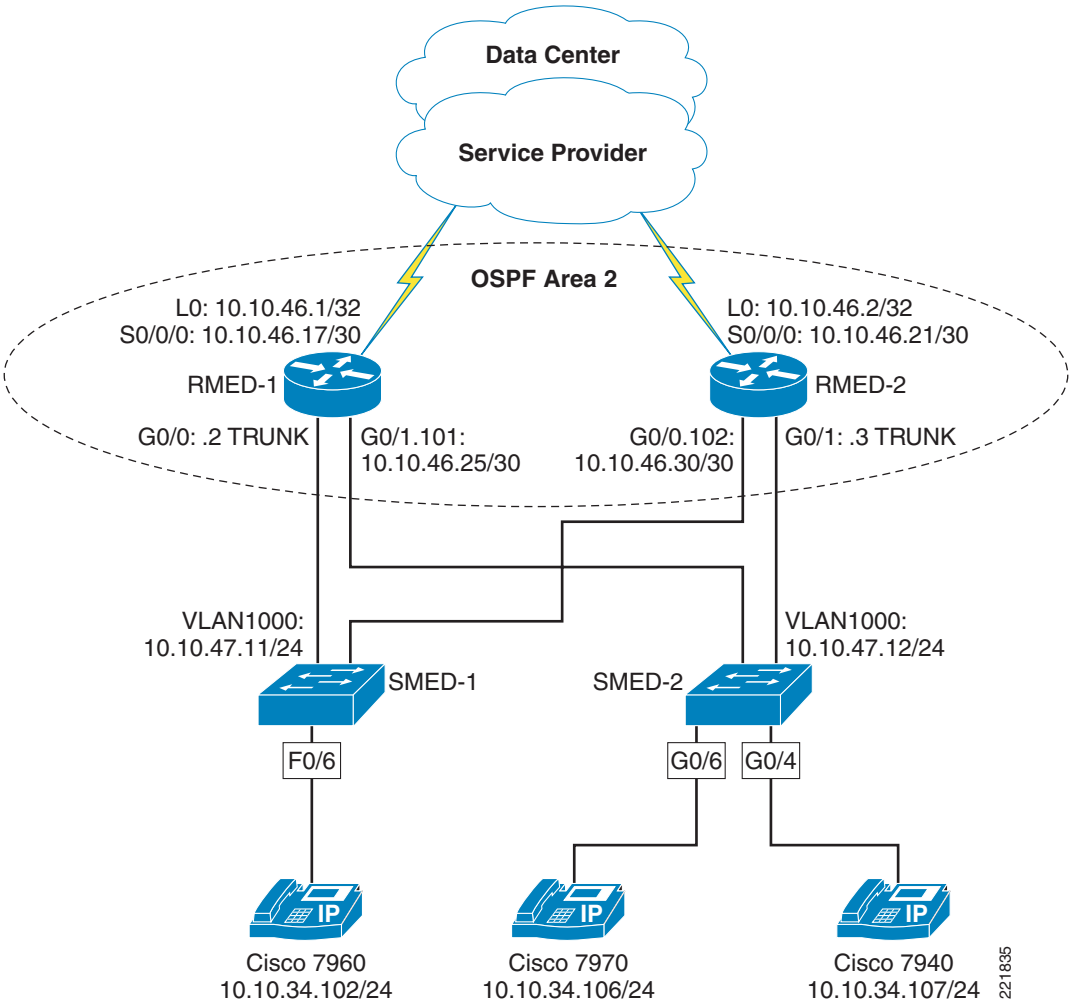
Large Store

Figure 33 Large Store Topology



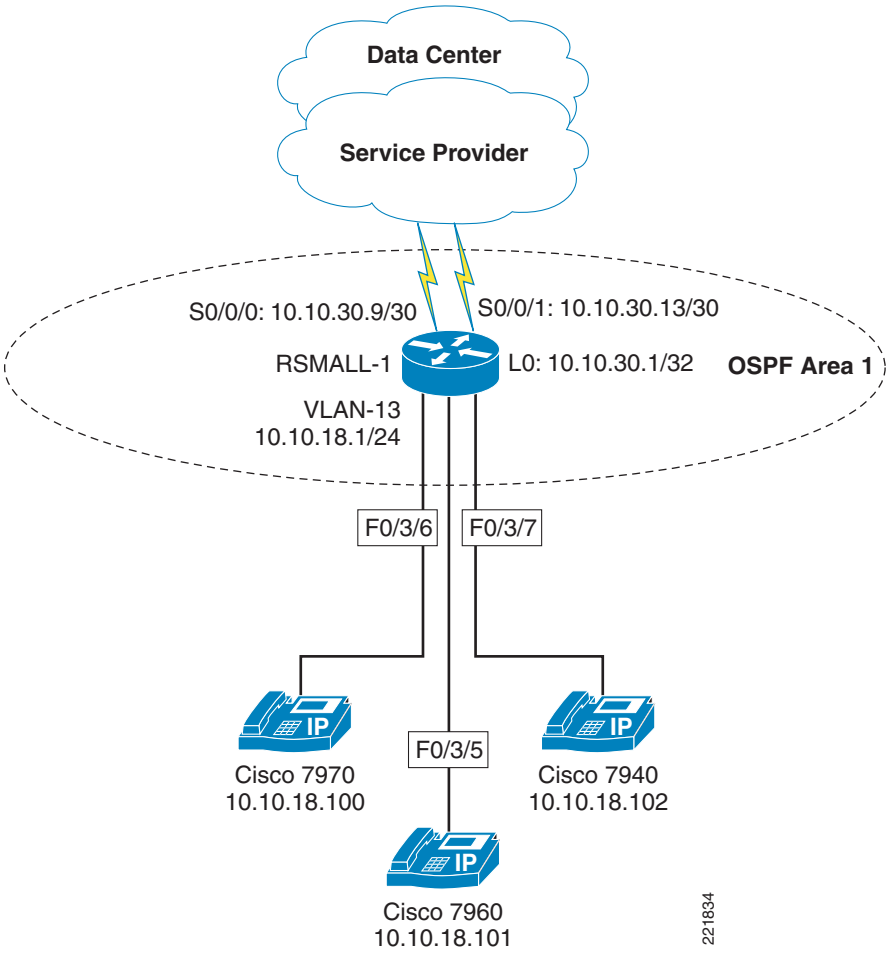
Medium Store

Figure 34 Medium Store Topology



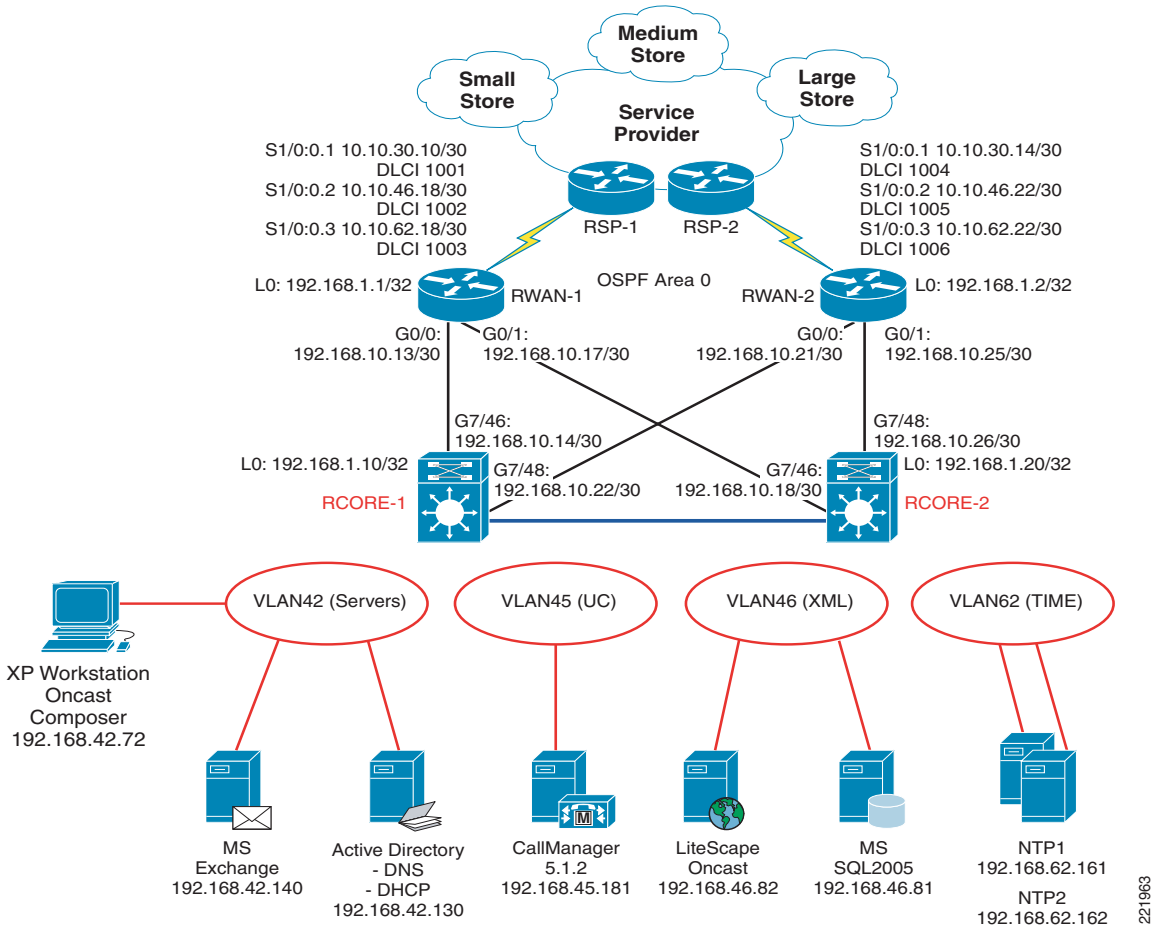
Small Store

Figure 35 Small Store Topology



Data Center

Figure 36 Data Center Topology



Service Provider

Figure 37 Service Provider Topology