



Cisco Imatis Mobile Care Solution Design Guide

Cisco Validated Design

February 20, 2008

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

Text Part Number:

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Cisco Imatis Mobile Care Solution Design Guide

© 2007 Cisco Systems, Inc. All rights reserved.

Copyright © 2008, Imatis AS

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior permission in writing by Imatis, or as expressly permitted by law.

IMATIS® is an Internationally registered trademark of Imatis. IMATIS ® is also registered in the U.S. Patent and Trademark Office.



CONTENTS

CHAPTER 1**Cisco Imatis Mobile Care Solution Overview 1-1**

- Executive Summary 1-1
- Solution Description 1-2
- Target Market 1-3
- Solution Benefits 1-3
- Scope of the Solution 1-4
- Imatis Overview 1-5

CHAPTER 2**Cisco Imatis Mobile Care Solution Services 2-1**

- Challenges Experienced in Hospitals 2-1
- Cisco Imatis Mobile Care Services 2-1
 - IMATIS Mobile Nurse Call Services Overview 2-2
 - IMATIS Order Entry Alerts Services Overview 2-4
 - Hospital Services Overview 2-5
 - IMATIS Mobile Alerts 2-6
 - IMATIS Hospital Orderly 2-7
 - Text Messaging 2-7
 - IMATIS Medical Team Assembly 2-8
- Summary 2-8

CHAPTER 3**Cisco Imatis Mobile Care Solution Architecture 3-1**

- Overview 3-1
- Deployment Model 3-2
- IMATIS Overview 3-3
 - IMATIS Hospital Communication Solutions 3-3
- Services Flow 3-5
 - IMATIS Mobile Nurse Call 3-5
 - RS-232-Based Nurse Call Interconnect 3-6
 - IMATIS Order Entry Alerts 3-7
 - IMATIS Medical Team Assembly 3-9
 - IMATIS Hospital Orderly 3-10
 - Text Paging (SMS) 3-11

Hospital Services—Building Alarms	3-13
Fire Systems	3-13
Security Systems	3-14

CHAPTER 4

Cisco Imatis Mobile Care Solution Features and Components 4-1

Solution Features List	4-1
Solution Components	4-1
Mobile Care Solution Prerequisites	4-2
Unified Communications Components	4-3
Infrastructure Components	4-3
Third Party Components	4-4
Reference Design Guides	4-4

CHAPTER 5

Designing the Cisco Imatis Mobile Care Solution 5-1

Quality of Service	5-1
Quality of Service Primer	5-1
Layer 2 802.1Q/p	5-2
Layer 3 Differentiated Services Code Point (DSCP)	5-2
Mapping between Layer 2 CoS and Layer 3 DSCP	5-3
Trusting QoS CoS/DSCP	5-4
Cisco IOS Voice Gateway QoS	5-4
Alert Generating Systems	5-5
IMATIS Mobile Nurse Call Systems	5-5
Clinical Systems	5-9
Fire and Security Systems	5-10
IMATIS Hospital Communication System	5-13
Cisco Security Agent (CSA) QoS Marking	5-13
IMATIS	5-14
QoS Summary and Checklist	5-15
Unified Communications Manager	5-16
Voice	5-18
Voice Port Utilization and Planning	5-18
Disconnect Supervision	5-20
VoWLAN	5-20
QoS Issues	5-22
High Availability (HA) Considerations	5-23
Unified Communications Component	5-23
Cisco Infrastructure	5-23

Network Components	5-24
IMATIS Hospital Communication System	5-24
IMATIS Components	5-25
Wireless Mobility Components	5-25
Access Points	5-26
Wireless LAN Controllers	5-26
Authentication	5-27
Encryption	5-28
Authentication Server (ACS)	5-29
1:1 WLC Redundancy	5-29
N+1 WLC Redundancy	5-30
Solution Component Interconnections	5-30
CUCM to IMATIS Connections	5-30
IP Phone to CUCM/IMATIS Connections	5-31
Hospital Equipment to IMATIS Adapters	5-31
Voice Gateway to Nurse Call System	5-31
Network Services Integration	5-32
Active Directory and Cisco Secure ACS	5-32
DNS (Domain Name Services)	5-32
DNS for XML High Availability	5-32
Network Time Protocol	5-33
CHAPTER 6	
Implementing the Cisco Imatis Mobile Care Solution	6-1
Network Topology	6-1
Configuration Task List	6-2
Cisco Unified Communications	6-4
Communications Manager Configuration	6-4
Creating System Users	6-4
SNMP Configuration	6-9
Creating XML Services	6-11
Creating XML Speed Dial Services	6-16
IMATIS Mobile Nurse Call Voice Callback Configuration	6-18
XML Services Redundancy on CUCM	6-22
User Management	6-24
IP Phone Configuration	6-25
Adding Services to the Phone	6-26
Creating Extension Mobility Users	6-27
Configuring Speed Dial Button for IMATIS Medical Team Assembly	6-30
Services Configuration	6-32

IMATIS System Configuration	6-33
User ID Management	6-34
IMATIS Portal for System Administrator	6-34
IMATIS Worklist and INBOX	6-35
IMATIS Mobile Nurse Call	6-35
IMATIS Mobile Nurse Call Integration	6-35
IMATIS Floor Plan and Bedroom Assignment	6-35
IMATIS Portal—System Administrator	6-36
IMATIS Portal for User Assignment—User	6-37
Alarm Types	6-38
IMATIS Order Entry Alerts	6-41
Ancillary System Integration	6-41
User Assignment	6-42
Text Messaging	6-42
Main Menu Screen and INBOX	6-42
Composing a Text Message	6-43
Receiving and Answering a Text Message	6-44
IMATIS Hospital Orderly Request	6-44
IMATIS Portal for System Administration	6-44
IMATIS Hospital Orderly Request Interface	6-45
IMATIS Dispatcher	6-46
Hospital Orderly Workflow	6-47
IMATIS Medical Team Assembly	6-49
IMATIS Portal for System Administration	6-49
IMATIS Medical Team Assembly Request	6-49
IMATIS Medical Team Assembly Workflow	6-50
IMATIS Mobile Alerts	6-51
User Assignment	6-52
IMATIS Scalability Considerations	6-53



CHAPTER 1

Cisco Imatis Mobile Care Solution Overview

Cisco Imatis Mobile Care is a solution for healthcare that improves the communication flow for hospital staff. By deploying Cisco Imatis Mobile Care, employees in a hospital can access, receive, and utilize information from numerous disparate hospital communication systems via the Cisco Unified Communications (UC) platform and Cisco Unified Wireless Network across a Cisco network infrastructure. Caregivers in a hospital see improved care, increased patient satisfaction, and reduced cost of care. Other hospital employees receive vital clinical information while not at their primary location, wherever and whenever they want it, greatly improving their effectiveness in providing patient care. Patients can make requests from the bedside, gather information about their condition, or order services that would have otherwise required staff interaction.

Cisco Imatis Mobile Care can be viewed as an extension to the Cisco Unified Communications system that currently supports hospital environments. This solution also addresses the important requirement to upgrade a hospital's legacy communication systems. In other cases, Cisco Imatis Mobile Care might be an adjunct to the hospital's legacy communication system. In all these cases, the underlying architecture leverages Cisco network designs for places in the network (PINs), such as the campus network or a wireless infrastructure to support voice. Key technologies that bring these new services to the hospital include Cisco Unified Communication, Cisco Unified Wireless Network, and Secure Mobility. Cisco's partner Imatis provides the gateway to hospital systems and Nurse Call systems and facilitates the delivery of critical information to mobile handsets.

Executive Summary

The challenges facing healthcare are well known and extend to many areas, including cost of care, regulations and compliance, lack of information, growing numbers of patients, etc. A common framework for interoperability, based on open standards, is needed to enable secure information sharing, simplify organizational processes, improve system performance, and reduce costs. Typical comments include:

- “Public health service is underfunded and unevenly distributed.”
- “Increases in health care spending have been attributed in part to an aging population.”
- “The cost of health care is one of the largest components of the U.S. economy and is rising faster than the rate of inflation.”
- “Healthcare companies today are faced with the daunting challenge of reducing costs while retooling systems and processes throughout their business to support electronic document exchange and comply with HIPAA”
- “Problems are embedded in the work processes and lack of adoption and use of technology, and patients, doctors, nurses, deserve and can build a better system.”

The goal of the Cisco Imatis Mobile Care solution enabled by key Cisco technologies and the partnership with Imatis is to return to staff and caregivers the time and resources that were lost because of poor communication flow. Improvements result when mobile staff can receive essential information anywhere in a hospital setting and when patients can retrieve information themselves without involving staff. The time and resources saved by hospital staff can then be directed back to their primary roles in the hospital.

Solution Description

The Cisco Imatis Mobile Care solution is an end-to-end system integration that provides hospital IT and system integrators with the information required to design and deploy a system that supports nurse call, stat alerts with HL7 ancillary systems, and hospital building systems. The primary focus is to facilitate a more efficient information flow from these systems to the caregivers, hospital staff, and patients. The three focus areas are:

- **Nurse Call Integration**—The Nurse Call component complements the primary notification system being used by a particular Nurse Call vendor. Nurse call alarms are typically those initiated by the patient, usually through the use of a pull station or bedside-attached nurse call device. These alarms are still delivered to the primary Nurse Call Station, while secondary messages are delivered to Cisco 7921G Wireless IP Phones for the mobile caregiver staff. The 7921G phone is then programmed with an option to call back the room that originated the alarm.
- **Ancillary System Integration**—The IMATIS Order Entry Alerts component provides mobile care givers with critical, results-oriented clinical information without regard for their physical location inside the healthcare enterprise. Through the use of Cisco 7921G phones, the caregivers responsible for the care of a patient are pushed updates critical to their care. These updates may be abnormal clinical results from a number of ancillary systems. Business rules are applied for formatting, scheduling, acknowledgment, and escalation mechanisms for these alerts.
- **Hospital Service Integration**—These integration points are examples, but each hospital may have unique integration points that should be addressed in conjunction with Imatis and Cisco. Some examples of hospital services that are requested by the care provider on an ad-hoc bases are:
 - Summons/team assembly
 - Building and fire alarms
 - Orderly requests (e.g., housekeeping, transportation, and dietary)
 - Text messaging

The foundational technology to support the delivery of this information to Cisco 7921G IP phones when staff are mobile include:

- **IMATIS Platform (Hospital Communication System)**—The foundation for an event-driven, service-oriented architecture including:
 - **Integration and Orchestration Server**—Combines messaging and connectivity to collect, transform, and distribute real-time events. Key performance indicators and metrics are established to help enterprise organizations continuously improve operational efficiencies, staff productivity, and decision-making.
 - **Adapters**—Imatis has designed and developed adapters to integrate third-party vendors throughout the enterprise to a standards-based, Web services format.
- **Cisco Unified Communications System**—Increases business agility by helping you integrate communications more closely with business processes, ensuring that information reaches recipients quickly through the most appropriate medium.

- Cisco Unified Wireless Network—Delivers secure connections, rich experiences, and intelligent services to help your organization.
- Cisco VoWLAN—Provides reliable voice communication anywhere in your facility.
- Cisco Campus and Data Center Designs—Deploy more robust business continuance and enhance data security for applications and servers.

Imatis should be contacted for specific information and considerations for integrating these medical devices and systems:

- Nurse Call System
- Ancillary systems (e.g., laboratory systems)
- Hospital Service systems (e.g., building and fire alarm systems)

Target Market

The Cisco Imatis Mobile Care solution is focused on solving communication bottlenecks within mid-size to large-size medical facilities. The benefits are even more amplified when large numbers of staff are involved and information flow between departments does not scale well. The solution is targeted at:

- Mid-size to large-size healthcare organizations (>150 beds)
- Hospitals with older voice and data technologies
- Hospitals with a very mobile work staff within the campus
- Hospitals with Point of Care system like Nurse Call Systems, Information Systems with HL-7 interfaces, building systems for fire or security alarms, and administrative systems such as dietary systems.

The healthcare provider's IT Infrastructure must adhere to the Cisco Medical-Grade Network architecture for recommendations on voice over wireless designs, Cisco's Unified Communications architecture for voice and security, and Campus/Data Center design practices.

Solution Benefits

The Cisco Imatis Mobile Care solution is focused on improving communication flow inside a hospital environment. The identified use cases focus on three main target groups. The first two target groups are employees of the hospital that are mobile. One group is focused on employees whose primary purpose is providing medical care, such as nurses, doctors, laboratories, etc. The second employee group covers the remainder of the hospital staff that need information and are mobile, such as security personnel, orderlies, and other facilities-related staff. The third group that receives immediate benefit from the solution are hospital patients. Patients are not typically mobile, but usually located in hospital rooms and potentially immobile. They frequently have requests or require information that they cannot obtain without the intervention of hospital staff.

- Caregiver benefits:
 - Receive all messages, alerts, and calls to one device so there is no need for additional devices when a user has an attending role (e.g., attending anaesthesiologist).
 - Voice and data communication anywhere in a hospital
 - Improved workflows

- Ability to receive alerts with information helpful in delivering timely and accurate patient care
- Allows the staff to be more mobile and not anchored to a particular location
- Gives time back to staff for their primary function
- Ability to rapidly assemble specialty teams
- Ability to escalate urgent issues when busy
- Flexibility to order services related to facilities or dietary
- Hospital staff benefits:
 - Receive all messages, alerts, and calls to one device so there is no need for additional devices when a user has an attending role (e.g., attending anaesthesiologist).
 - Voice and data communication anywhere in a hospital
 - Improved workflows
 - Allows the staff to be more mobile and not anchored to a particular location
 - Gives time back to staff for their primary function
 - Ability to receive information to provide accurate services
 - Ability to deal with urgent matters as they arise
 - Flexibility to order services related to facilities or dietary
- Patients:
 - Ability to retrieve information dynamically
 - Ability to request services that previously required manual intervention
 - Ability to order items within a hospital

Scope of the Solution

Deploying the Cisco Imatis Mobile Care solution involves a broad range of technologies and features. To ensure a successful deployment, you must keep in mind key design and implementation considerations that center around an infrastructure that is compliant with the Cisco Medical-Grade Network. These fundamental characteristics can be achieved by adhering to the set of Cisco best practices for each of the technologies being deployed and outlined in the Cisco Medical-Grade Network architecture.

This document focuses on system considerations across campus, Cisco Unified Communications for CUCM, IP Phones, and Cisco Unified Wireless Network in collaboration with the IMATIS Hospital Communication System. Key design considerations and specific implementations across key Cisco products and integration with the IMATIS gateway are covered to deploy Cisco Imatis Mobile Care. Integration concepts with nurse call systems, ancillary systems for HL7, and hospital service systems are also covered to provide a general understanding of the integration challenges.

This document does not cover the installation steps required by each product in the solution. For detailed configuration information we suggest you consult the individual product documentation. Because the solution spans a wide array of technologies and product sets from both Cisco and third parties, we recommend that a certified installation partner be consulted during the planning, configuration, installation, and training phases of a deployment for optimum results.

Imatis Overview

Headquartered in Porsgrunn, Norway, Imatis AS is the leader in innovative software solutions for the healthcare industry. Their products focus on connecting people, information, processes and systems within a healthcare organization. The Integration Engine, Messaging Service and clinical applications will help the customer in achieving their goal of becoming an Integrated Digital Hospital with focus on patient flow and lean thinking. The building blocks relies on the Cisco Medical-Grade Network and the Cisco Imatis Mobile Care solution.

The company was founded in 1991 by Morten Andresen and has its background from large-scale applications in the oil & gas and manufacturing industries as well as 7 years of experience from the healthcare industry. In 2007 the company was split into two separate organizations that will continue to be close technology partners. The oil & gas and manufacturing unit is now named CARDIAC Industry AS (<http://www.cardiac.no>) while the healthcare unit is now named Imatis AS (<http://www.imatis.com>). Imatis is also the name of our main product suite. Imatis has a good reputation and years of experience with implementing software as an integrated part of the hospital work flow and mobile care.

At Imatis AS they utilize their own software product family and have a large in-house product development department. The products included in the IMATIS Suite are standardized as a part of the Integrated Healthcare and Application Portfolio. Imatis work closely with National Instruments, Cisco, HP and Microsoft to embed their framework applications and modules into their products. Cisco Silver and Gold Partners is a part of the Imatis roadmap for delivering the solution portfolio in the international marketplace.

The IMATIS Suite is a service-based infrastructure and application framework. It includes several healthcare applications, like patient bedside terminals, nurse calling, electronic patient charts, vital sign/patient monitoring and notification, bed management, localization services, asset control and patient whiteboard. The platform also supports advanced and flexible services for hospital communication like notifications, team assembly, emergency medical communications, alarm management and voice.

Imatis applications provide an excellent platform for point-of-care as well as mobile services. The IMATIS role-based portal and applications run on Cisco wireless IP phones, mobile phones, patient bedside terminals, wireless computers and PDA's both inside and outside the hospital building to create a true mobile care environment. The Integration Engine can also connect to external applications and services such as a patient registry, birth registry, doctor's office or clinic, directory services, etc.

Contact information:

Head Office Europe

Imatis AS
Vipeveien 51
N-3917 Porsgrunn
Norway
Tel: +47 91 800 700

<http://www.imatis.com>

sales@imatis.com

Head Office North America

Imatis US, Inc.
133 Federal Street
Suite 901
Boston MA 02110, US
Tel: +1 (617) 515 5135



CHAPTER 2

Cisco Imatis Mobile Care Solution Services

Challenges Experienced in Hospitals

Care providers are faced with an ever-increasing number of challenges in global healthcare systems. Patient loads are increasing due to the shrinking numbers of medical professionals within the industry. To make their jobs even more challenging, they now face an increased number of clinical information sources, including nurse call, ancillary clinical systems, and building systems. In many healthcare organizations, for example, nurse calls are received at the central nursing station and require the duty nurse to overhead audio page or audio room page the responsible nurse in order to handle another patient request. Disruptions like these to an already stressed workflow result in clinical inefficiencies and overall lower patient safety and satisfaction.

With respect to increasing amount of clinical diagnostic results being generated, the responsibility of collating and acting upon these reports falls on nursing staff. More times than not, they are processed in a batch form and not as they arrive from the ancillary department. If the result is recognized as critical to the patient care, it must be communicated to the attending physician and/or assigned nurse. The problem, however, is that often these results are lost in a paper shuffle and sometimes time critical to patient treatment is lost in the process.

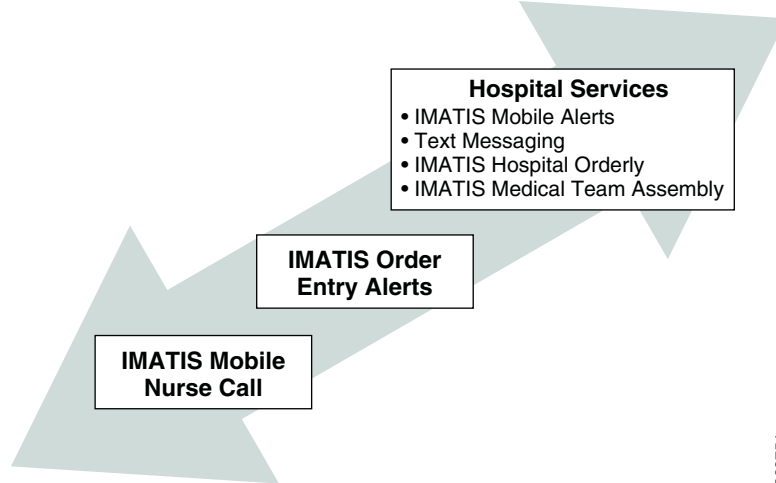
To streamline the care process, Cisco has developed the Cisco Imatis Mobile Care Solution. This solution provides the correct and most appropriate caregivers with the information that they need, where ever they are. Through the use of the Unified Wireless Mobility and Unified Communications technologies from Cisco, the caregiver can now be presented with timely and prioritized information they can more efficiently view and act upon. The IMATIS Order Entry Alerts component of the Cisco Imatis Mobile Care Solution interfaces the physician or nurse directly to the ancillary systems, which notifies them using a wireless phone as to the availability of a clinical test result. From this same device, a nurse can receive alerts from patients or entire Medical Emergency Teams, such as the Code, Cesarean, Respiratory, and Cardiac team, can now receive real-time alerts when requested. In addition, the solution provides voice communication directly between the patient and caregiver, further enhancing patient care while at the same time increasing efficiency.

Cisco Imatis Mobile Care Services

The Cisco Imatis Mobile Care solution is based on three main use cases or functions that address many of the common communication requirements within a healthcare environment. Each of these use cases is discussed in detail in the following sections and all utilize a Cisco Medical-Grade compliant infrastructure which supports both a Unified Communications and Unified Wireless Network Solution.

[Figure 2-1](#) shows a summary of the services enabled through the integration with Imatis.

Figure 2-1 Summary of Services Enabled Through the Integration with IMATIS



IMATIS Mobile Nurse Call Services Overview

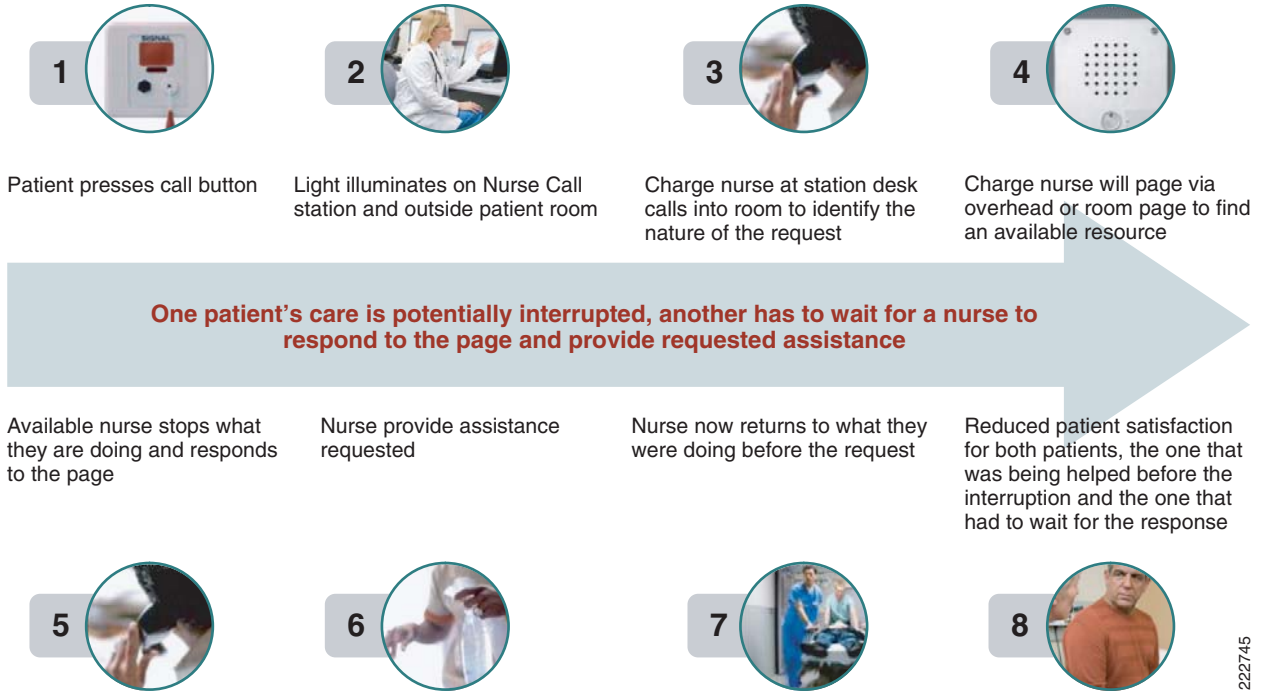
These services will greatly enhance the workflows of a hospital. Several services and integrations are described below. matis has other services and integrations points that are not covered in this document. Use the contact information provided in [Imatis Overview](#) to obtain more information.

In order to provide efficient patient care, communication among patients and nursing staff is critical for optimal patient outcomes. In any healthcare-related facility, whether it be acute, outpatient, or aged care facilities, a nurse call system is likely deployed. With the addition of IMATIS Mobile Nurse Call to an existing or yet-to-be-installed nurse call system, the communication system is augmented and optimized.

Interfacing directly with the nurse call system by using the IMATIS Hospital Communication System, both text- and audio-based alerts can be provided to the optimal caregiver where ever they are located within the healthcare facility. The solution employs a simple to use wireless handset that provides the care giver with a text-based workflow presenting prioritized alerts.

[Figure 2-2](#) shows a sample workflow through existing methods for nurse call.

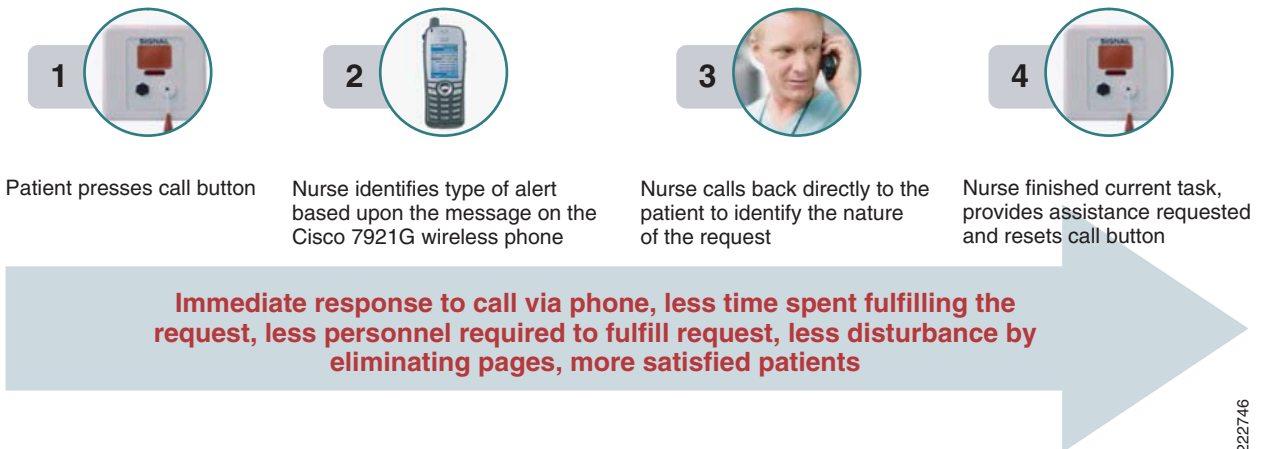
Figure 2-2 Sample Workflow for Nurse Call



222745

Figure 2-3 shows the efficiencies gained by all parties when using IMATIS Mobile Nurse Call.

Figure 2-3 Sample Workflow Using IMATIS Mobile Nurse Call



222746

By using the Cisco Imatis Mobile Care solution, patient safety and clinical efficiency are improved over that of a traditional nurse call system. Integration with the BEST Nurse Call System provides secondary alerts to Cisco IP phones in addition to the primary alerts sent to the Nurse Call stations provided by BEST.



For additional Nurse Call System integrations, contact Imatis.

IMATIS Order Entry Alerts Services Overview

Many times within a healthcare system, the availability of new patient diagnostic information is lost in the paper and work shuffle. By leveraging both mobility and VoIP technologies, the timely notification of test results can now be communicated in real time to one or more caregivers responsible for patient care. Through the use of IMATIS Hospital Communication System, the availability of diagnostic results can be communicated to caregivers through a standard HL7-based interface.

This HL7 interface allows any ancillary system to be instrumented such that clinical results or information about the availability of new results from systems such as lab, oncology, and radiology can be sent directly to the prescribing physician as well as the responsible nursing staff. The result is rapid turn around, allowing physicians and caregivers to act upon those results.

Figure 2-4 shows a sample of the delays and uncertainties around the readiness of lab results in current settings.

Figure 2-4 Delays and Uncertainties in Lab Readiness Results

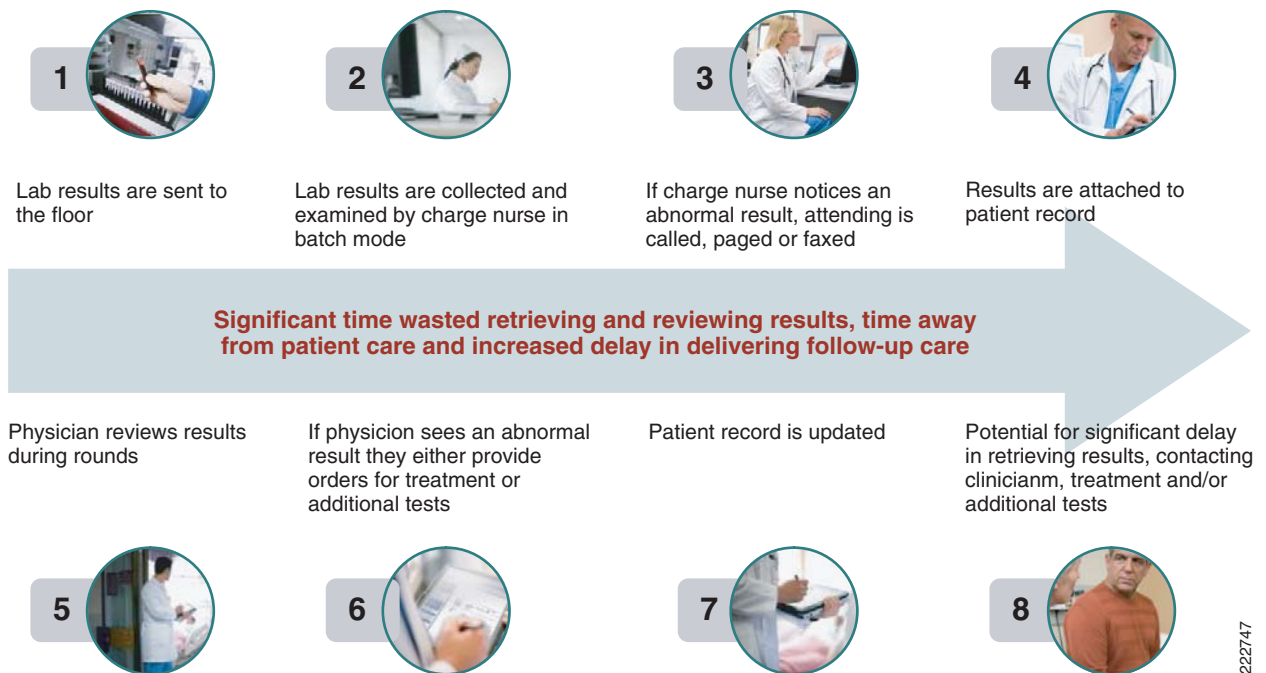
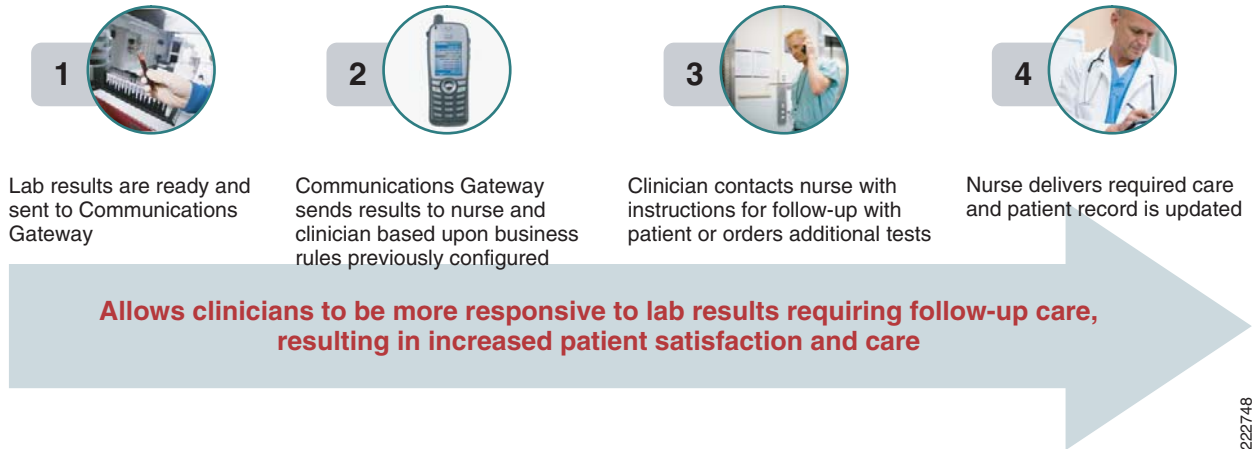


Figure 2-5 shows the benefits clinicians gain by using IMATIS Order Entry Alerts to support the alerts when a lab result is ready for review.

222747

Figure 2-5

Lab Result Availability Alerts Using IMATIS Order Entry Alerts

HL7 is used by various hospital system and may utilize a range of parameters. For detailed information on specific integration points, contact Imatis.

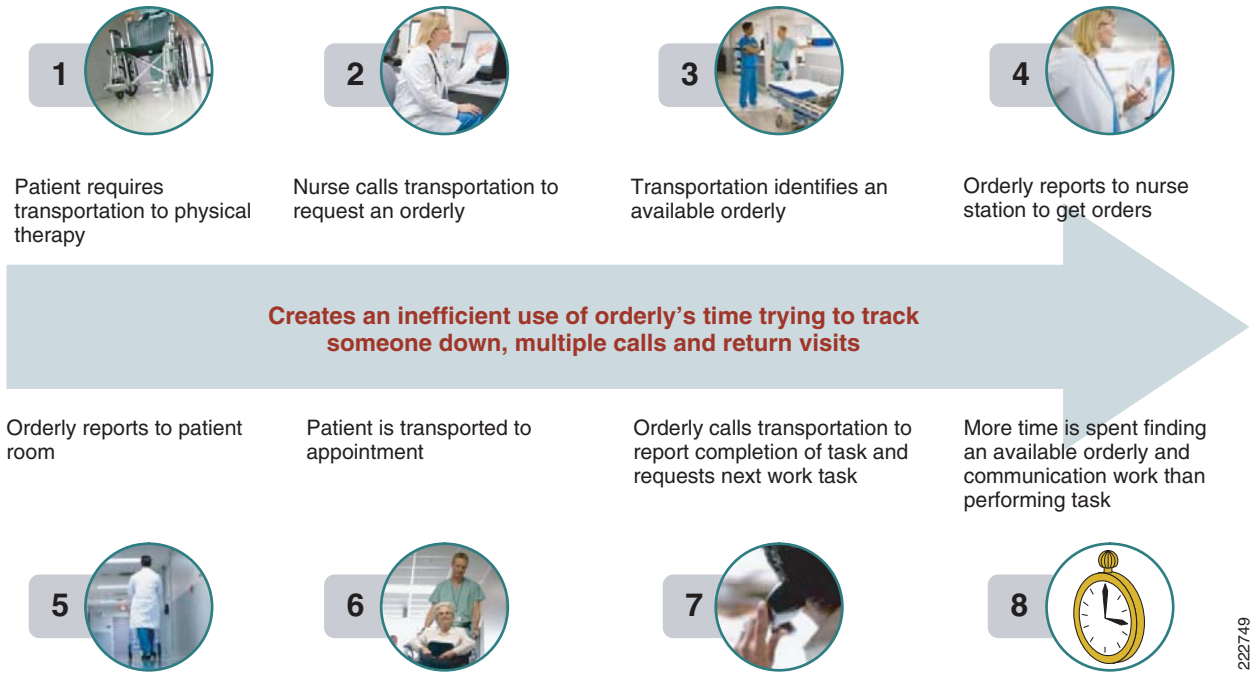
Hospital Services Overview

Hospital services is a general category of services that can help to improve the workflows of hospital staff employees. The four areas that Imatis focuses on to improve workflow are:

- IMATIS Mobile Alerts
- IMATIS Hospital Orderly
- Text messaging (within a hospital)
- IMATIS Medical Team Assembly

Figure 2-6 shows an example of hospital services without the benefits of the Cisco Imatis Mobile Care Solution.

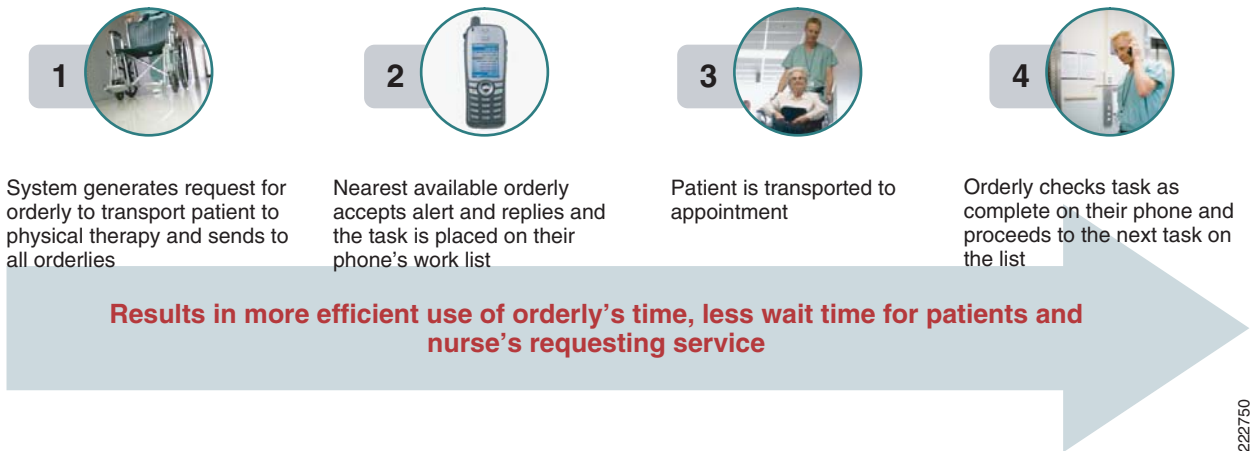
Figure 2-6 Hospital Services Without Cisco Imatis Mobile Care



222749

Figure 2-7 portrays the improved workflow gained through using the Cisco Imatis Mobile Care Solution for hospital services.

Figure 2-7 Improved Workflow Using Cisco Imatis Mobile Care for Hospital Services



222750

IMATIS Mobile Alerts

IMATIS Mobile Alerts is a general messaging service for routing messages from different producers to consumers.

Integrating with best-of-breed facilities systems and installations like Fire Alarm, Security Systems, HVAC systems, Elevators, Pneumatic tubing, Automated Guided vehicles, and so on, gives the opportunity to send alarms, maintenance and error messages to dedicated service personnel, as well as sending notifications on arrival of pneumatic tubes or AGV transport to the receiving person improving the overall transport efficiency.

Just as timely clinical information is critical in a healthcare environment, so is building safety. By interfacing directly with building systems, such as fire and security, caregivers are provided with accurate and timely information during an emergency. Security lock downs, fire alarms, additional alarms, etc. can be sent to users in a text-based message. This can include descriptive text about the location or nature of the emergency.

The result is that staff are better informed and can take appropriate action during such an event. Since the nature of the emergency is now known and tracked in real time, the care giver can provide patient and other staff with timely information as to the status of the emergency.



IMATIS Hospital Orderly

IMATIS Hospital Orderly is a system designed to improve hospital patient transport functions. This automated workflow solution enhances staff communication, reduces late pick-ups, distributes transport workload on the orderlies, and optimizes the use of transport resources.

IMATIS Hospital Orderly includes functions such as:

- Ordering transport from Web pages or IP phones
- Automatically assign service orders to service staff
- Provide work lists to service staff anywhere and anytime
- Generate invoice reports on orders
- Provide central overview on all orders, response times, etc.
- Centrally manage orders

Requests for patient movement inside a hospital or other facility-related requests are also commonly asked of caregivers. Often the request is initiated while next to the patient's bed. With a transportation service request issued from the bedside communication system, efficiencies can be gained and the request sent as soon as the caregiver is aware of it. Updates can be provided to the requester as well the employees responding to the request through the Cisco 7921G phone.

Text Messaging

Poor coverage may exist inside a hospital for typical text message devices. The Cisco Imatis Mobile Care Solution can rectify this and integration with existing directory systems for hospital staff can be customized by using the text message services offered through the solution. This service provides the ability for any hospital staff to text message another hospital staff through the integration with Cisco Unified Communications Manager and Cisco Unified Wireless Network. From any Cisco IP phone, one can text message another person using the Cisco IP phone whether it is wired or wireless. This flexibility provides the staff with a device that offers a wide range of service options through XML applications.

IMATIS Medical Team Assembly

IMATIS Medical Team Assembly provide the functionality in emergency situations to rapidly send out messages to potential members of a specialist team (for example cardiac arrest team, multi-trauma team, or a need for emergency expertise in the hospital) and keep track of acknowledged responses to make sure the team is fully casted and on their way. The solution provides the necessary escalation logic and logs to monitor the alarm activity. This includes dispatch software which allows the person handling incoming emergency calls to simultaneously send messages to stationary or hand held devices (pagers, IP phones, mobile phones) of the response team.

Often teams of individuals for a particular role, like a cardiac team, need to be rapidly assembled. Using methods for finding a particular person for a specific shift may require much manual searching, wasting critical time in the assembly of the team. Using the service created through the Cisco Imatis Mobile Care Solution for team assembly, specific roles can be assigned to staff for particular shifts, such that all roles are always covered. Alerts for a team assembly are as simple as selecting a speed dial button on a Cisco IP phone and the alert to form a team can be rapidly pushed to the right individuals.

Summary

The Cisco Imatis Mobile Care solution offers a variety of exciting workflow enhancements. A great benefit to the multi-purpose staff and employees in a hospital that may carry multiple roles, this range of services can be converged onto a signal device to further reduce the complexities of dealing with multiple interfaces to get information. For more information on this solution, contact your Cisco or Imatis representatives to learn more. The following sections cover the architecture, designs, and implementation around the services covered.



CHAPTER 3

Cisco Imatis Mobile Care Solution Architecture

Overview

The Cisco Imatis Mobile Care solution plays a critical part in providing information to caregivers reliably and in real time. To accomplish this, the solution is based on Cisco's Medical-Grade Network Architecture, providing high availability and scalability. It is beyond the scope of this document to discuss the Cisco Medical-Grade Network architecture in detail.

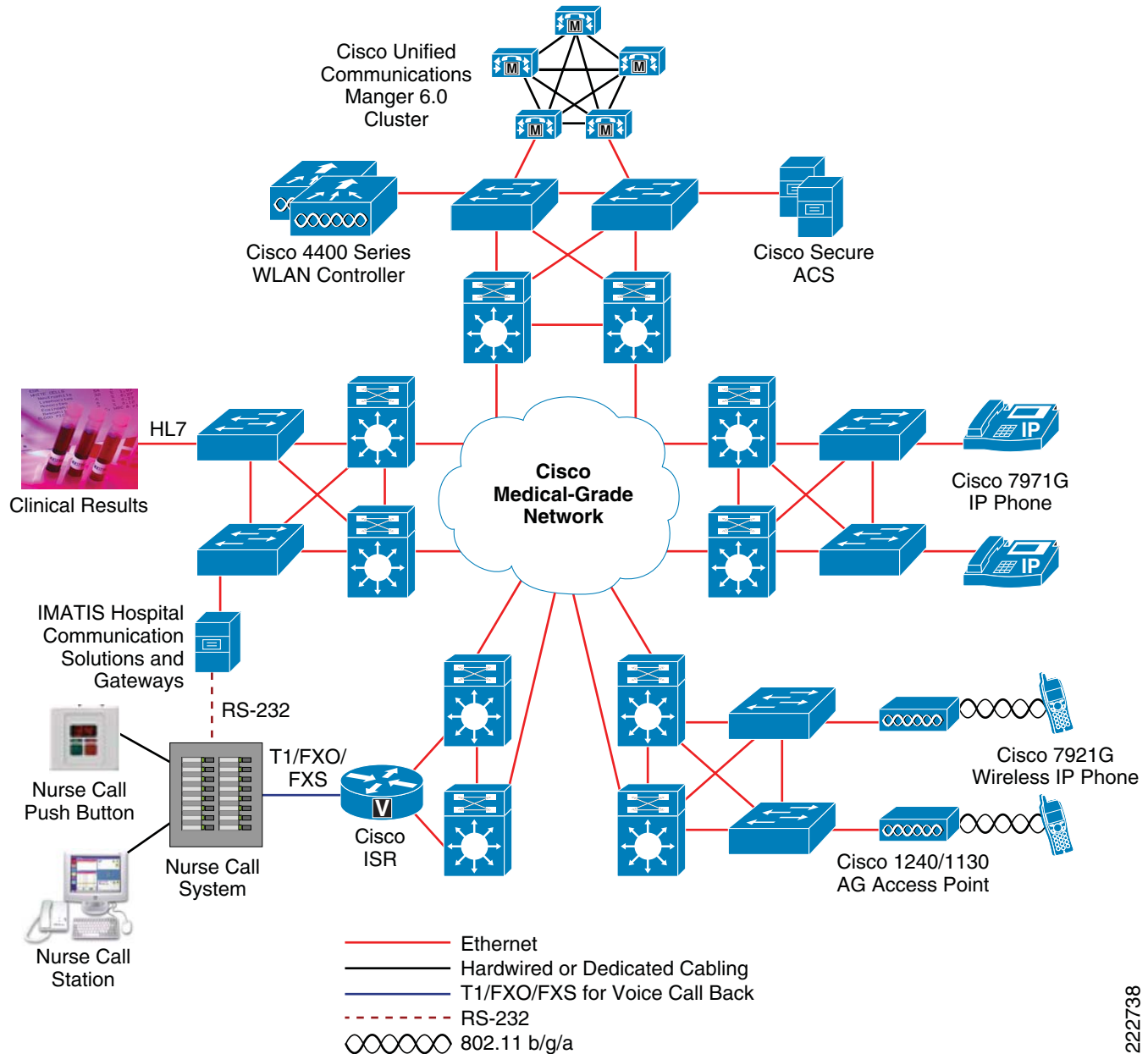
It is however important to point out that achieving a level of availability for such systems requires careful review and planning of the end-to-end network topology as it applies to:

- Redundancy
- Security
- Quality of Service
- Scalability
- Expandability

For information on Cisco's Medical-Grade Network architecture, refer to <http://www.cisco.com/go/healthcare>. These designs are based on the architectures that can be found at <http://www.cisco.com/go/srnd>. Information about the architectures that are relevant to Mobile Care can be found in the design guides for Campus, Data Center, Secure Mobility, and Voice over WLAN. The placement of the Wireless LAN Controller (WLC) as recommended should be either part of the distribution layer or service module. It is not recommended to place the WLC directly to the Data Center core switching fabric. In many deployments, a service module is created to host components that provide network services such as Content Switching Modules (CSM), FireWall Service Modules (FWSM), and Application Control Engine (ACE) modules.

[Figure 3-1](#) provides a high level overview of the network used to validate this design architecture.

Figure 3-1 High-Level Overview of Network Used to Validate Design Architecture



222738

Deployment Model

The deployment of Cisco Imatis Mobile Care is based on the Campus design. Each floor of a hospital should follow the access designs aggregating traffic up to the distribution and core components of the campus network. The application servers, such as the Cisco Unified Communications Manager and IMATIS server, should be placed in the server farm of the data center. For the deployment of the 7921G

phone, strict adherence to site surveys for wireless deployment should be followed. See the section for prerequisites for wireless voice deployment for details. To achieve the most optimal voice coverage, follow the design recommendations found in the voice over wireless LAN design guide.

IMATIS Overview

IMATIS Hospital Communication Solutions

The IMATIS platform connects together and manages a series of different input sources. Examples include alarms from medical equipment, patients' emergency pull cords, and alerts from ancillary clinical systems. The message event originating devices span a wide range of device types, from medical equipment, mechanical signal senders such as emergency pull cords, postal tube systems, and other technical systems, to clinical IT systems and telephony equipment. In addition, the system manages logical alarms, such as if a nurse leaves a department and that department is understaffed (based on predefined assumptions). Using rules which process in real time, an alarm for cardiac arrest triggers an alarm on the units the cardiac arrest team are currently using. The cardiac arrest team can be defined as the personnel nearest to the patient based on the system's location parameters. The solution can do more than just pass alarms and messages. Using IMATIS Hospital Communication System, which uses Web Services (.NET and MS-BizTalk), the patients' journals can be retrieved from the medical applications on the doctor's or nurse's PC or PDA. The system also manages patient terminals on which patients can choose entertainment or control technical systems in their room, such as light and temperature.

A core of Web Services has been produced that make it possible for the portals on the various units to retrieve the information needed. Using the message server IMATIS, PCs and Cisco IP telephones can be used for voice, dictation, e-mail, SMS, and other message exchanges, and alarms and remote control if they are equipped with these functions. For example, an alarm from a patient monitoring device can be routed to the nearest doctor and in a form suited to the doctor's unit, as an alert to an IP telephone, or as a spoken message to a telephone without a display.

The messaging server:

1. Functions as the server for routing of messages to personnel.
2. Is able to handle messages linked to stationary roles (permanently positioned functions and personnel) and dynamic roles (on-call doctors/nurses, trauma teams, on-call IT, technical operations, fire teams, etc.)
3. Is able to handle messages to groups of people. It also synchronises with or retrieves contact information about stationary roles, groups, and personnel from the catalogue service and provides solutions to maintain dynamic roles

In addition, message routing takes place both as a wired and wireless function using standardised protocols and interfaces and is routed from call devices in rooms (phones, work stations (PCs), and patient signal units) and information systems (e-mail, SMS, IM, etc.) to the message recipient via wireless phones and wireless message receiving devices (PCs, PDAs, etc.) or as e-mail.

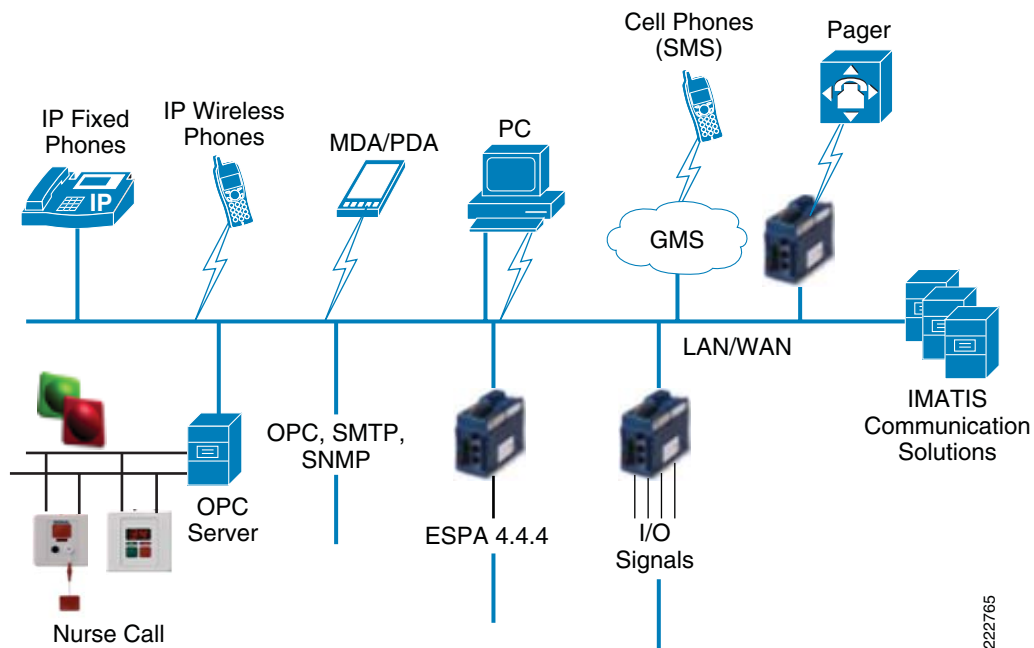
The system can be integrated with all described message routers and receivers using standard network technology (TCP/IP) and network-based standards such as XML, SMTP, SMNP, and OPC, including network connectors (gateways) to non-IP based standards such as SMS, ESPA 4.4.4, and potential free I/O signals, etc.

The patient signal unit itself collects and transfers various alarms from patients and nurses for calling assistance to bed rooms, toilets, examination and treatment rooms, and specialised rooms. Calls and alarms are routed to the specified ward and, via the messaging server, to the dedicated nurse. The patient

signal unit also allows the public and patients to call for assistance from individual rooms, such as handicap toilets (HC) in public areas. Alarms from these rooms are routed to the duty centre and security guards via the messaging server.

The system is installed as a distributed solution with positioning of redundant servers. An overview of the IMATIS Hospital Communication System, together with the patient signal system, is shown in Figure 3-2.

Figure 3-2 Overview of IMATIS Hospital Communication System with Patient Signal System



The main elements of the message router solution are:

- A complete, redundant server design that ensures availability
- Distributed services that, distributed on three servers, ensure performance and scalability
- Cost-effective solutions in which the message recipients are the same devices as for wireless IP telephony and with shared use of the network infrastructure
- System integration with the telephony system for a complete solution
- Use of existing SAN for databases/storage
- System integration with catalogue for mirroring stationary user information
- Dynamic role management and on-call team (“On-call surgeon,” “Cardiac arrest,” etc.)
- Message routing to text messaging and e-mail
- Message transmitter is connected via OPC
- Other described standards such as XML, SMTP, SNMP, IM, etc. are supported
- Assault alarms on wireless phones

The main elements in the patient signal solution are:

- Modern patient signal units from, for example, BEST Teleprodukter
- Cabling for patient signal units included in the delivery

- Intuitive and user-friendly IMATIS Web-based PC client on the ward
- Xtag Baby from Xtag is used as RFID based alarm units for babies
- IMATIS calling client for PC-based messages/summons and call-ins
- Service for positioning and location designation of units in the wireless network

Services Flow

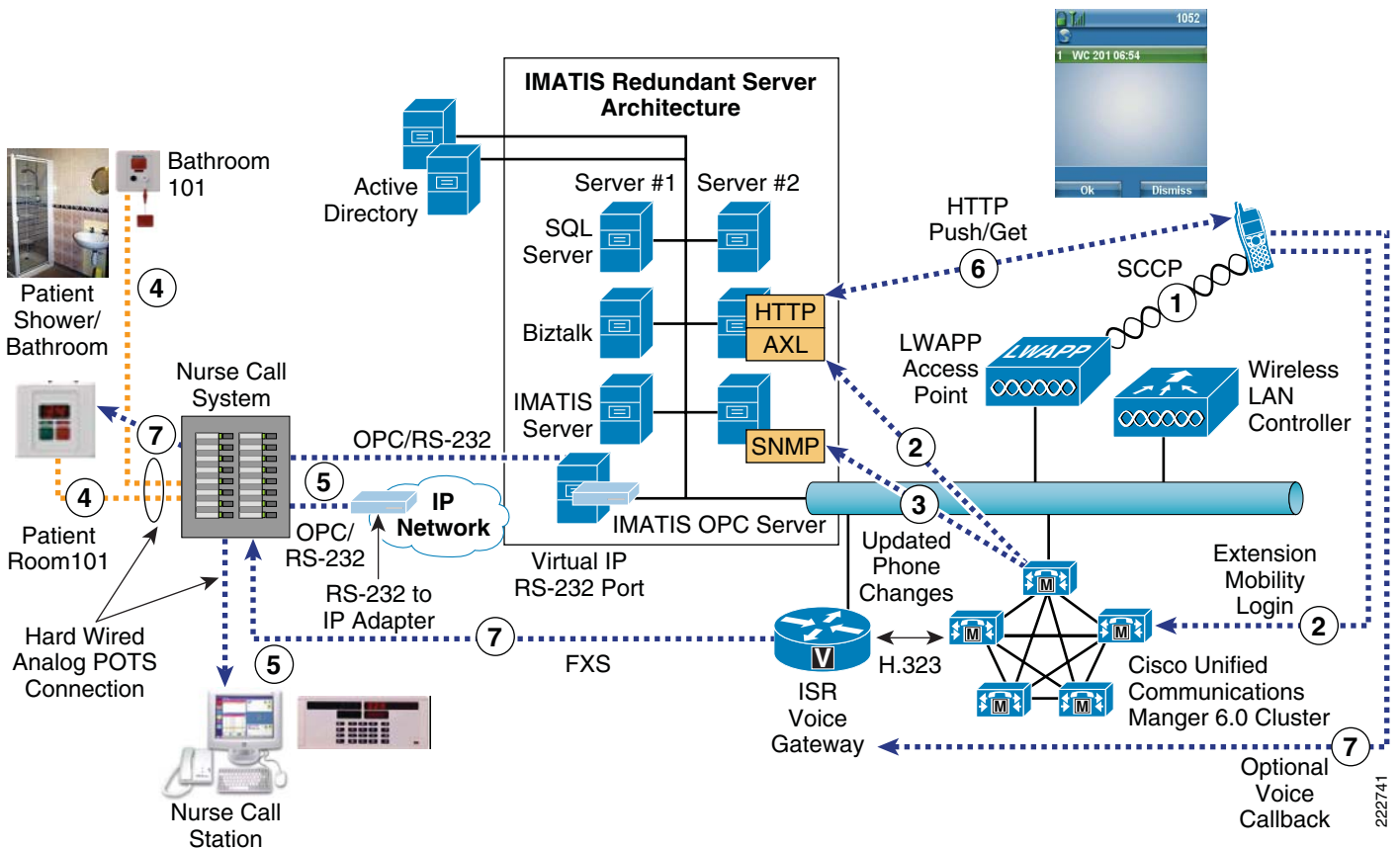
IMATIS Mobile Nurse Call

The IMATIS Nurse Call service is provided through integration with nurse call systems vendors, such as BEST in Sweden (<http://best.se/index.htm>). Imatis creates adapters to interface with nurse call systems using protocols like OPC or the protocol used by the nurse call vendor. The alarms created by the nurse call system are collected by the IMATIS server and delivered to the clinicians and nurses according to the defined business rules.

A high-level architectural diagram is shown in [Figure 3-3](#).

1. The Cisco 7921G phone registers with Cisco Communication Manager.
2. The user logs in through the IMATIS login and is automatically logged into CUCM using extension mobility.
3. Any phone state changes are updated to the IMATIS servers through SNMP updates.
4. A patient in the room rings the nurse call button.
5. The alert from the nurse call system is sent to the IMATIS servers as well as the any nurse call stations used by the nurse call system.
6. The IMATIS server relays the nurse call alarm to the assigned nurse based on the business rules defined for that patient.
7. The nurse receiving the nurse call alarm may call back with a single touch call back button from the Cisco 7921G phone.

Figure 3-3 High-Level Architecture—Nurse Call



Interfacing to the nurse call system can be accomplished through two primary methods. The most common method is the use of an RS-232 serial connection between the IMATIS server and the nurse call system. The second method, if supported by the nurse call vendor, is an IP connection where the nurse call system sends XML formatted messages directly to the IMATIS server over an IP-based network.

RS-232-Based Nurse Call Interconnect

The maximum distance for RS-232 is both dependent on the capacitance of the cabling used and the speed of the serial transmission. The RS-232 specification specifies that the cable length must not exceed 50 feet or a cable length whose capacitance does not exceed 2500 pF. Using Category 5 cabling, it may be possible in some circumstances to reach 150 feet at 9600 baud. The use of Cat 5 cabling however is implementation-dependant and such results may not be possible in all cases.

Since most nurse call systems use 9600 baud connections, the typical installation using non-specialized cabling, the 50 foot rule of thumb should be used. Since the IMATIS server is critical to the clinical workflow, both its availability and reliability must be considered. As such, it is strongly recommended that you install the IMATIS server in the hospital data center. Since the location of the data center is typically greater than 50 feet from the installed nurse call system, a method of converting RS-232 to IP must be employed. It is possible to extend RS-232 signal from remote nurse call systems by using an RS-232 to IP converter or by using the Cisco IOS feature BSTUN (Block Serial Tunneling).

IMATIS Order Entry Alerts

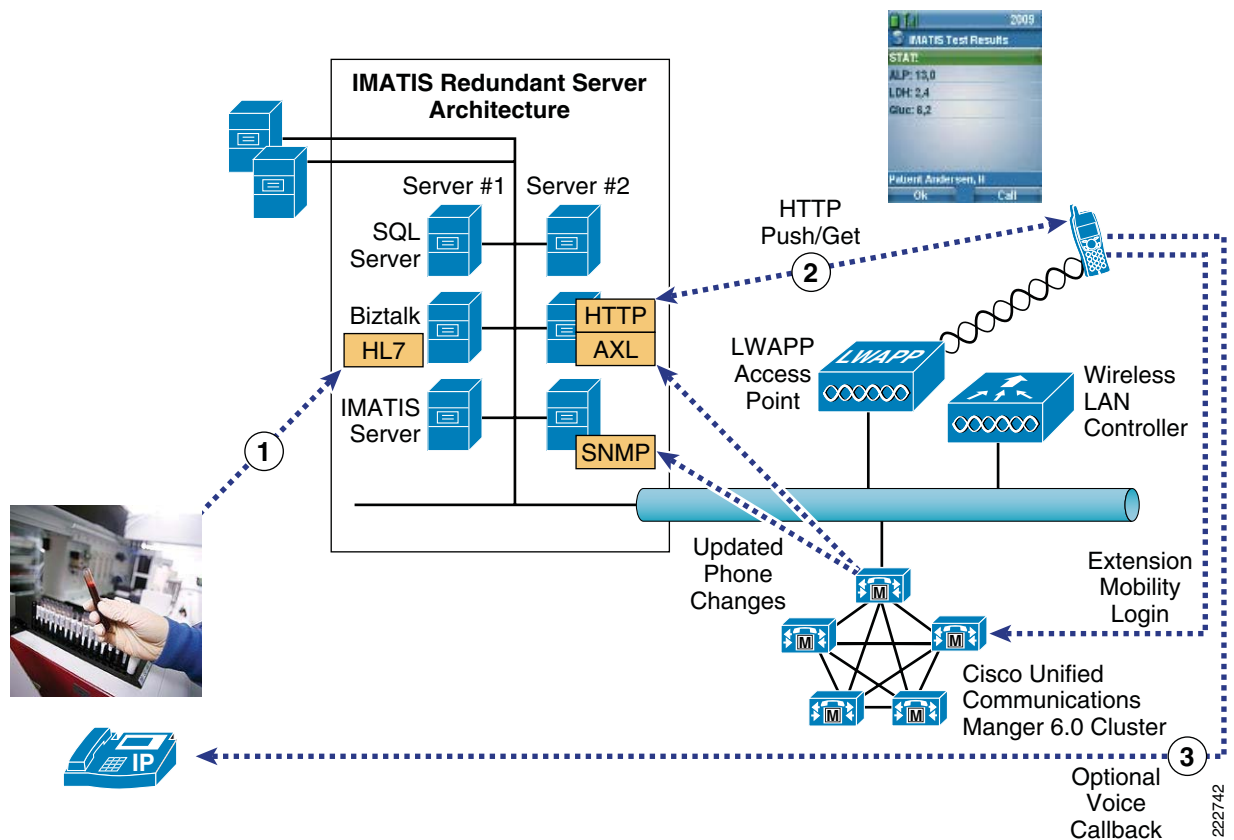
The IMATIS Order Entry Alerts solution provides care givers with real time alerts about the availability of clinical results specific to a patient under their care. The source of the alerting information can be any ancillary system that supports standard HL7-based results reporting. The ancillary system can originate the HL7 transaction directly to the IMATIS server or an HL7 interface engine can replicate a message and forward a copy to the IMATIS system.

Despite the mechanism used to deliver the message to the IMATIS server, a number of rules can be applied to the event and trigger the notification of the results to the appropriate care provider.

Figure 3-4 highlights the flow of the message content between the ancillary system and the care providers.

1. A laboratory results is ready and the information systems used by the labs send a message indicating that information to the IMATIS server through an HL7 interface.
2. The notification is sent to the appropriate receiver based on the HL7 message and the business rules defined on the IMATIS server.
3. The receive notification has an option to place a voice callback to the lab that provided the lab results through single touch dialling.

Figure 3-4 Message Content Flow



Communication between the ancillary system and the IMATIS server is IP/TCP based and can occur on any TCP port as configured on the IMATIS and ancillary HL7-based system.

Once the message is received by the IMATIS server, it is examined to determine if action must be taken against the message. If such an event requires notification to third parties, the message is sent to the BizTalk server where it is examined further to determine the parties to which the message should be sent. One of the critical business rules decides what type of data is passed onto the clinician. Due to patient sensitive data, a business rule decides if the results is sent along with the alert or if only the indication that a result is ready is sent to the clinician. Once this is determined, the IMATIS server forwards the message to the intended devices currently assigned to the care providers.

The screens shown here are seen by the clinician when a stat alert is received on their Cisco 7921G phone.

Figure 3-5 shows a normal lab result is ready for a patient and displays the test results.

Figure 3-5 *Result Ready and Results Shown*



Figure 3-6 shows a normal lab result is ready for review by the clinician, but the results are not shown.

Figure 3-6 *Result Ready and Results Not Shown*



Figure 3-7 shows an urgent lab result is ready for a patient and displays the test results.

Figure 3-7 Urgent Result Ready and Results Shown

Figure 3-8 shows an urgent lab result is ready for review by the clinician, but the results are not shown.

Figure 3-8 Urgent Result Ready and Results Not Shown

IMATIS Medical Team Assembly

IMATIS enables the ability to request a summon of a predefined team. This predefined team would enroll for a specific functional role as defined by the team. An example of a team may be the cardiac team that consists of a doctor and a nurse or it may be all nurses on floor 15. These rules are defined in the IMATIS server. These members enrolled in this group then receive alerts that belong to the team.

The request for this medical team can be achieved via several methods:

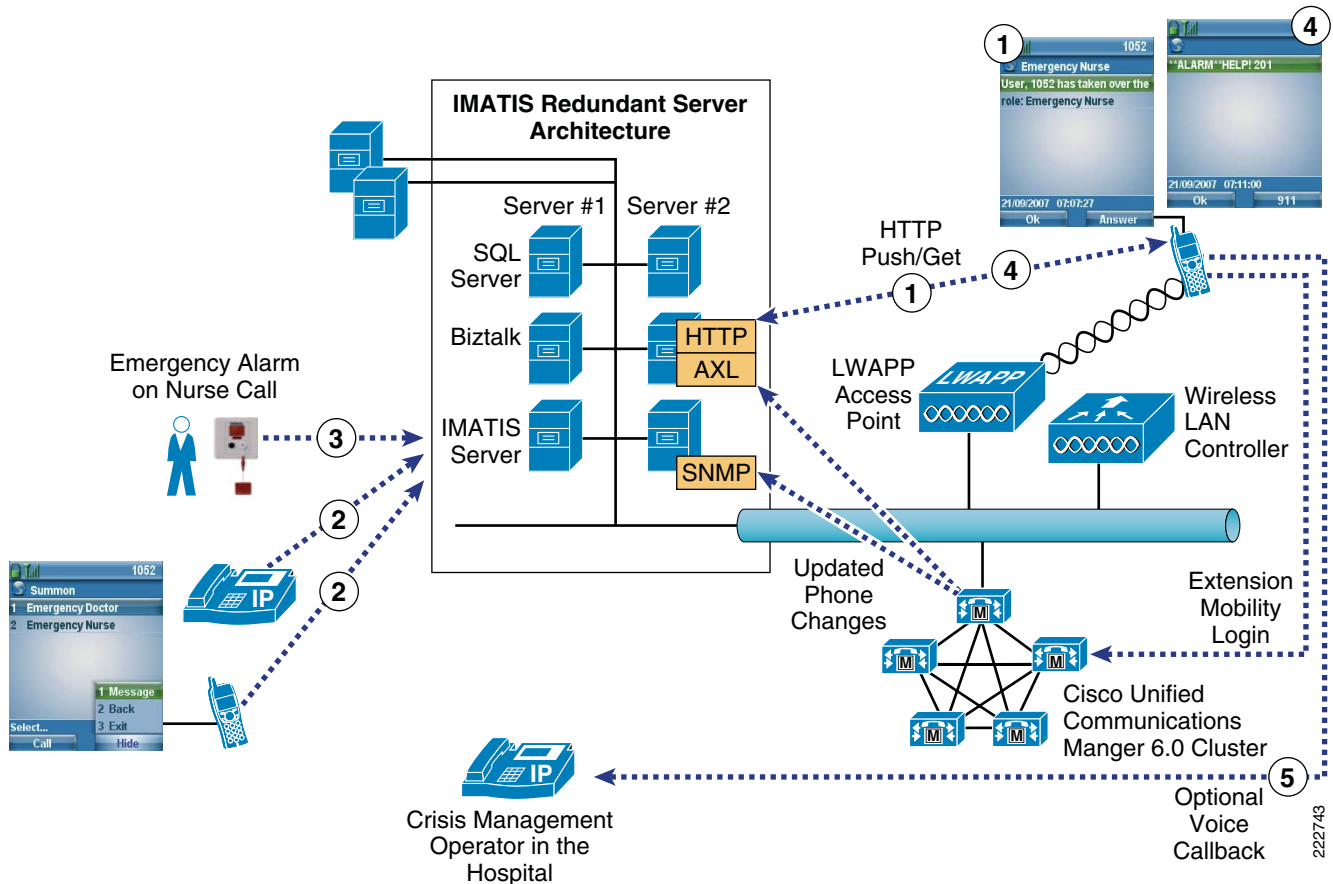
- Medical Team Assembly Request Tool by Imatis
- Speed dial on a Cisco IP phone
- XML menu on the Cisco IP phone

Figure 3-9 demonstrates the workflow for summons of a medical team.

1. The responsible party logs into a pre-defined role based on their job function. For example, a role may be the emergency nurse for that shift.
2. A request for medical team assembly is generated from a Cisco IP Phone.
3. Another method can be used to generate an emergency alarm for medical team assembly based on the integration with existing nurse call systems.

- The alert for the medical team assembly is sent to the assigned person for a particular role based on the business rules defined in IMATIS.

Figure 3-9 IMATIS Medical Team Assembly



IMATIS Hospital Orderly

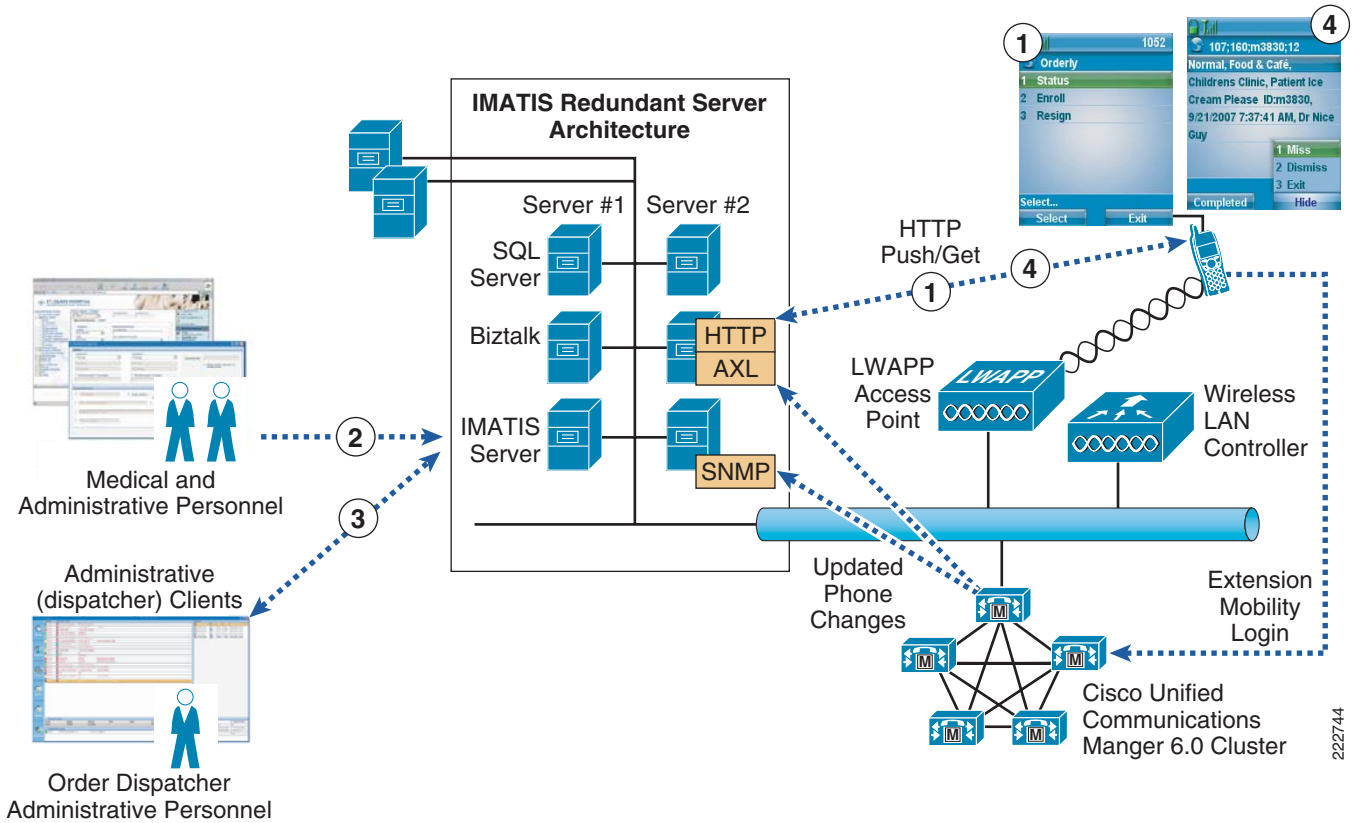
IMATIS provides greater efficiencies for the orderly staff in a hospital. Through the combination of Web applications enabled by IMATIS and the Cisco Unified Communications system to provide updated requests to orderly staff, the mobile staff can receive updated work requests in real time. Accomplished through an IMATIS interface, the work staff in a hospital can make a specific request for an orderly to perform a task. This task request is then sent to the hospital dispatcher to assign the request to a specific individual. The receiver of the message has the option to accept, miss, or dismiss the request. By accepting the task, the system acknowledges the dispatcher once the task is completed. To dismiss a request, such as when the orderly staff may be busy with an activity, the request is then rerouted back to the dispatcher for reassignment. In the miss scenario, the request may not be able to be serviced due to the inability to service the request, for example when a wheelchair transport being requested is not available at the specified location.

Figure 3-10 demonstrates the workflow of an orderly request.

- An orderly signs in and enrolls in their task to indicate availability to receive orderly tasks.

2. Administrative staff may place an order request and these requests are then forwarded to the dispatcher.
3. After receiving the order, the dispatcher assigns the task to an available orderly.
4. The orderly receives the request on their phone based on the business rules defined on the IMATIS server.

Figure 3-10 IMATIS Hospital Orderly



Text Paging (SMS)

Due to coverage issues of GSM phones inside a hospital or improved integration with hospital directory systems, a hospital may want to have a localized message system to facilitate communication from one individual to another individual inside a hospital facility. This can be enabled through the text message application enabled by IMATIS and delivered through the Cisco Unified Communications system. A few screens seen by the user are shown below.

Figure 3-11 shows the window to create the text message from a Cisco phone.

Figure 3-11 Window for Creating Text Message on Cisco Phone



Figure 3-12 shows the user receiving a message.

Figure 3-12 User Receiving Message



Figure 3-13 shows the options to answer the message, which are to answer with a predefined answer, call the originator back, or send them back a user-defined text message.

Figure 3-13 Options to Answer Message



Figure 3-14 shows the inbox for a text message for a particular user.

Figure 3-14 User Text Message Inbox

Hospital Services—Building Alarms

Integrating building alarm systems such as fire and security is critically important. Up until now, there has not been a focus on bringing such life-critical alerts directly to the clinician. Interfacing to such systems is similar in design to that of an RS-232-based nurse call system. Using the IMATIS server, it is possible to trigger on messages, and forward to groups of phones, both hard-wired XML-enabled Cisco phones as well as wireless 7921G phones. The integration to these systems uses the protocol European Selective Paging Association (ESPA) 4.4.4.

Fire Systems

Connectivity to most fire alarm systems is accomplished via an RS-232 serial interface or in some cases with older equipment a 20 mA (Milli-Amp) current loop. These outputs from the fire alarm system were typically connected to a line printer which was used as a notification mechanism for responding fire personnel.

The output includes the following information:

- Alarm location, including floor and room
- Alarm source such as fire pull station, smoke detector, heat detector, or optical detector
- Alarm type, such as alarm or equipment trouble
- Miscellaneous information such as the density of smoke or heat detected

Using this information, the IMATIS server can forward alerts to the most appropriate staff. The message can be both building/floor dependant. [Figure 3-15](#) shows two screenshot samples as seen by the facilities manager receiving the message.

Figure 3-15 Sample Screenshots for Received Messages

Security Systems

Similar to fire alarm systems, most security system control panels provide a serial interface to which alerts or system programming can be performed. Likewise, many card access systems also provide a mechanism to provide activity monitoring information via a standard RS-232 serial interface. The event monitoring data sent from a security system can be forwarded to the IMATIS server through either a direct connection or extended via IP through the use of an RS-232 to IP device.

A typical alarm message would include:

- Time/date
- System name
- System location
- Zone name
- Alert type (trouble or alarm)
- Device ID sending the alert (window 1, door 17)

Once these messages are received by the IMATIS server, they can easily be acted upon based on the configured business rules. [Figure 3-16](#) is a sample screen shot of a security alarm being received.

Figure 3-16 Sample Screen Shot of Security Alarm Being Received



CHAPTER 4

Cisco Imatis Mobile Care Solution Features and Components

Solution Features List

Some of the key features available in the Cisco Imatis Mobile Care Solution include:

- Voice over WLAN
- Secure WLAN
- Nurse call integration
- HL7 integration
- Ancillary system integration
- Alarm system integration
- Data alerts on wired and wireless IP Phones
- Service requests from IP phones
- Voice call back with dynamically programmable softkey
- Call escalations when acknowledgment times expire
- Summon an assembly of a pre-defined medical team
- Dynamic user login for shared devices using extension mobility
- End-to-end QoS for differentiated traffic types like voice and critical data alerts
- Single sign on for user login
- Text messaging between mobile care users
- Request orderly services to mobile workforce

Solution Components

The solution components required for Mobile Care span several key technologies. These technologies used in combination address the requirements to improve communication flow in a hospital:

- Call control—Provides the central intelligence to deploy IP voice- and data-enabled endpoints to generate or receive the information flow based on the services in the Cisco Imatis Mobile Care solution. Featuring Cisco Unified Communications Manager (CUCM) 6.0, this release provides a foundation with rich features to meet the communication requirements of both the solution and other

communication systems in the hospital. The key features of CUCM 6.0 provide resource and call control for wired and wireless IP endpoints and the ability to deliver XML applications to handsets for the various services in Cisco Imatis Mobile Care. CUCM interfaces with the IMATIS Hospital Communication System which then provides the interface to a variety of hospital systems.

- IP endpoints—The two endpoints highlighted in this solution are the Cisco 7921G and Cisco 7970G/7971G phones that provide, respectively, wireless and wired support. These phones are enabled with XML applications to serve as voice communication devices and also generate mobile care services and receive critical alerts from hospital systems.
- IMATIS Hospital Communication System—The hospital communication system is an essential middleware services layer that bridges the interfaces of various hospital systems with Cisco's infrastructure for voice and data. IMATIS adapts to the various protocol interfaces that range from nurse call systems to HL7 systems to a variety of other interface types. By applying a set of rules defined for a particular service type, actions are taken and essential data is then passed to the responsible party in real-time.
- Mobility—Through the Cisco Unified Wireless Network architecture, voice or data needs are delivered to the user anywhere in a hospital setting that has wireless coverage. Users are securely authenticated for access such that only users allowed on the system are provided services when and where they need it. Mobility is a key element in the Cisco Imatis Mobile Care solution.
- Campus and data Center infrastructure—Following Cisco design recommendations for campus and data center designs ensures that hospitals have a business-resilient and secure architecture to provide a variety of applications in a hospital setting, including being a foundational component for delivering Cisco Imatis Mobile Care.
- Hospital systems—Some limited testing was performed with available systems. Hospital systems describes a general grouping of the range of applications that are used in a hospital. These systems typically send information to static systems so the information is only received by the intended users when the user requests the information. These include systems used to request information, which can now be requested through XML-enabled applications from the bedside or mobile IP endpoints. Categories include:
 - Nurse call system
 - Ancillary system (HL7-based HIS systems)
 - Fire and building alarm systems
 - Hospital PBX systems

Mobile Care Solution Prerequisites

Healthcare has a high level of criticality with respect to wireless mobility. As such, Cisco has instituted a mandatory process for VoWLAN solutions to help ensure all deployments are reliable and highly available. This process requires the completion of the following steps before an order is released for shipment:

- Full VoWLAN site survey including RF spectrum analysis
- VoWLAN site survey and installation must be completed by a Cisco Certified Unified Communications Integration Partner and Wireless LAN Integrator
- Completed QoS assessment for both the wired and wireless network
- The Cisco Unified Wireless IP Phone 7921G Deployment Guide must be adhered to

- All orders for 7921G phones are placed on hold until Cisco receives an Assessment-to-Quality (A2Q) survey from the partner

Contact your sales representative for details on how to complete these steps.

For additional reference material that help ensure successful Cisco Imatis Mobile Care deployments, refer to:

- Proposal for Sales & Deployment of Unified Wireless IP Phone 792X in Healthcare:
http://www.cisco.com/en/US/partner/products/hw/phones/ps379/prod_bulletin0900aecd805df502.html
- 792x Sales Process for Healthcare:
http://www.cisco.com/en/US/partner/products/hw/phones/ps379/products_qanda_item0900aecd805df4e7.shtml
- Follow the VoWLAN Design Guide practices:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns656/c649/ccmigration_09186a0080923473.pdf
- Follow this assessment on Quality for Voice over Wireless LAN:
http://www.cisco.com/en/US/partner/products/hw/phones/ps379/prod_bulletin0900aecd804fb75c.html
- Follow the instructions outlined in this Site Survey FAQ:
http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_q_and_a_item09186a00805e9a96.shtml

Unified Communications Components

This section provides a complete list of the Cisco Unified Communications components that were used in the Cisco Imatis Mobile Care Solution.

Table 4-1 Unified Communications Components

Component	Functional Description	HW/SW Releases
Cisco Unified Communications Manager	Call control and resource management for voice- and XML data-enabled IP endpoints	6.0.1.2000-4
Cisco IP Phone 7921	802.11 a/b/g wireless enabled IP Phone	1.0.4
Cisco IP Phone 7970G/7971G	SCCP IP Phone	SCCP70.8-3-1S
Cisco IP Phone 7970G/7971G	SIP IP Phone	SIP70-8-3-1S
ISR Voice Gateway and Gatekeeper	H.323 Voice Gateway and Gatekeeper	c3845-ipvoice_ivs-mz.124-13b.bin

Infrastructure Components

Table 4-2 lists the infrastructure components used for mobility, user authentication, server load balancing, and QoS markings as part of the Cisco Imatis Mobile Care Solution.

Table 4-2 Infrastructure Components

Component	Functional Description	HW/SW Releases
Cisco 4402 / 4404	WLAN Controller	4.1.181.0
1240AG or 1130AG	LWAPP Wireless Access Point	12.3(7)JA1
Cisco Secure Access Control Server	Centralized RADIUS server or TACACS+ server	Release 4.1(3) Build 12
Cisco Security Agent	CSA Manager for QoS markings	Version 5.2
Cisco 6500-E Catalyst Switch	6509 with SUP-720 to provide IOS SLB (Server Load Balancing)	s72033-entservicesk9_wan-mz.122-18.SXF9.bin

Third Party Components

Table 4-3 lists the third-party products that were part of the Mobile Care solution.

Table 4-3 Third Party Components

Component	Functional Description	HW/SW Releases
IMATIS Message Server	Message Server	Version 1.1
IMATIS SQL Server	Database Server for IMATIS	Microsoft Sql Server 2000 SP3
IMATIS BizTalk Server	BizTalk Server for IMATIS	Microsoft BizTalk Server 2004 SP1

Reference Design Guides

Mobile care is layered on several foundational design guidelines which are often referred to as places in networks (PINS). The PINs that should be followed are:

PIN	Link
Voice over WLAN Design Guide	http://www.cisco.com/en/US/netsol/ns741/networking_solutions_products_generic_content0900aecdd80601e1d.html#mobility
Secure Mobility Design Guide	http://www.cisco.com/application/pdf/en/us/guest/netsol/ns386/c649/ccmigration_09186a0080871da5.pdf
Enterprise Mobility 3.0 Design Guide	http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808118de.pdf
Campus Network Multilayer Architecture and Design Guidelines	http://www.cisco.com/application/pdf/en/us/guest/netsol/ns656/c649/cdccont_0900aecdd804ab67d.pdf

PIN	Link
Unified Communications 6.x Design Guide	http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html
Server Farm Security in a Business Ready Data Center Architecture 2.1	http://www.cisco.com/application/pdf/en/us/guest/netsol/ns376/c649/ccmigration_09186a008078e021.pdf



CHAPTER 5

Designing the Cisco Imatis Mobile Care Solution

Quality of Service

The Cisco Imatis Mobile Care Solution includes a number of different services with varying levels of criticality. Since the solution optimizes the clinical workflow and provides a number of patient services, the overall reliability of the end-to-end solution is critical. This chapter describes the various mechanisms for assuring a high level of service from each of the components of the design. Careful consideration to the end-to-end Quality of Service (QoS) is mandatory for a Cisco Imatis Mobile Care deployment.

For an in-depth design guide on QoS, refer to <http://www.cisco.com/go/srnd>. This publicly available Web site provides excellent Solution Reference Network Design material.

- *Enterprise QoS Solution Reference Network Design Guide Version 3.3*

Quality of Service Primer

This document is not an in-depth guide to QoS, but a quick review may be helpful. QoS provides the services necessary to eliminate packet loss while at the same time minimizing jitter and delay in a converged IP network. It is only effective if implemented end-to-end between each of the systems in the Cisco Imatis Mobile Care solution.

There are three main areas of QoS that must be considered in any Cisco Imatis Mobile Care deployment are:

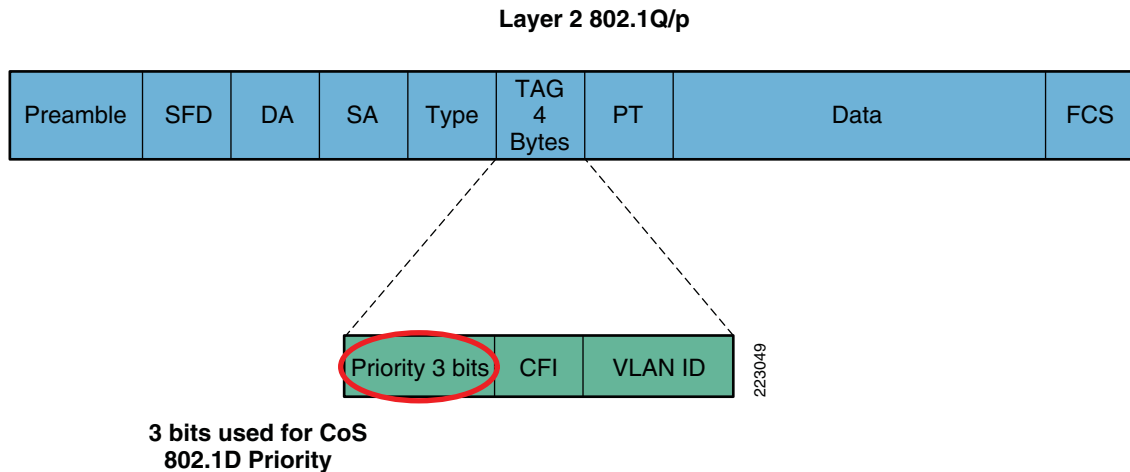
- **Classification**—Marking packets with a priority code that indicates the service requirements required by the network.
- **Scheduling**—Assigning marked packets into various queues for expedited processing if necessary.
- **Provisioning**—Calculating the required bandwidth for the solution along with the overall end-to-end delays caused by network overhead.

Typically an IP network is composed of a number of Layer 2 networks (VLANs) which are eventually interconnected using a Layer 3 router providing inter-VLAN routing services, and hence end-to-end connectivity. Marking a packet with a Layer 3 marking does not affect how that packet is handled through a Layer 2 network because the Layer 2 network switching fabric does not inspect Layer 3 header information. Likewise, packets marked at Layer 2 does not affect traffic as it is routed at Layer 3.

Layer 2 802.1Q/p

Frames marked at Layer 2 using Class of Service (CoS) are classified and subject to the queuing policy defined on the switch.

Figure 5-1 Layer 2 802.10p



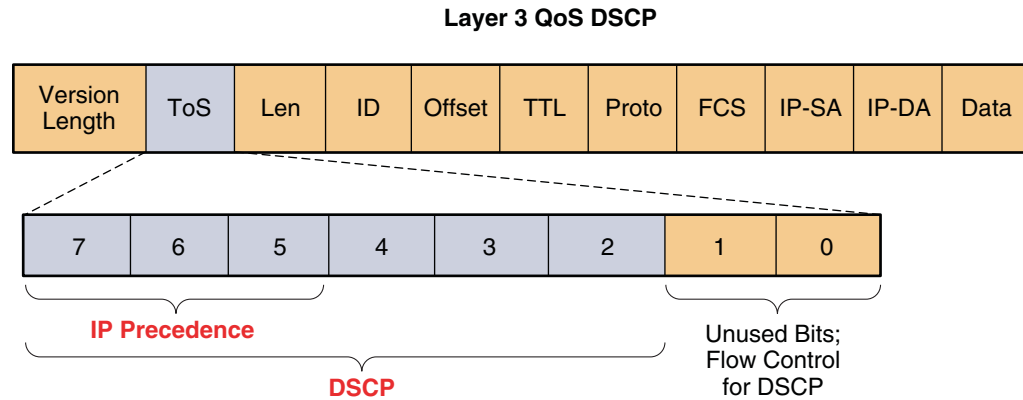
Within 802.1p, the precedence is a 3 bit field, allowing values between 0 and 7. The various bit patterns and their values are:

- 000 = 0—Best Effort (Scavenger)
- 001 = 1—Background
- 010 = 2—Standard
- 011 = 3—Business Critical
- 100 = 4—Streaming Multimedia
- 101 = 5—Voice and Video, less than 100ms latency and jitter
- 110 = 6—Layer 3 Network Control (reserved)
- 111 = 7—Layer 2 Network Control (reserved)

Layer 3 Differentiated Services Code Point (DSCP)

The ability to mark traffic at Layer 3 has existed long before the now more common DSCP mechanism. DSCP utilizes the 1 byte Type of Service (ToS) field and preserves it for backward compatibility to the IP Precedence ToS marking. The first three bits of the ToS field are commonly referred to as the IP Precedence and similar to that of CoS with values from 0 through 7, with 0 being the lowest priority and 7 being the highest. The next 5 bits are the DSCP bit indicators, but DSCP actually uses the ToS bits in the overall marking.

Figure 5-2 DSCP



First 3 MSBs define the IP Precedence or Type of Service (DiffServ May Use Six D.S. Bits Plus Two for Flow Control)

223050

DSCP uses these 6 bits as shown in Figure 5-3 to indicate the relative service level that should be provided to any traffic so tagged.

Figure 5-3 DSCP Service Levels

	Class	Low Drop Preference	Medium Drop Preference	High Drop Preference	Diff Service Code Point		
Expedite Forwarding		EF			101110		
Assured Forwarding	Class 1	AF11	AF12	AF13	001010	001100	001110
	Class 2	AF21	AF22	AF23	010010	010100	010110
	Class 3	AF31	AF32	AF33	011010	011100	011110
	Class 4	AF41	AF42	AF43	100010	100100	100110
Best Effort					000000		

223051

Mapping between Layer 2 CoS and Layer 3 DSCP

When a frame is marked with DSCP, for example, and it needs to traverse a series of Layer 2 switches or 802.1Q Trunks, how will it be queued in these Layer 2 devices? To accomplish this, there is a mapping that takes place between the Layer 3 mapping field (TOS) and the Layer 2 CoS fields. It is important to note that this mapping between Layer 3 and Layer 2 is set by default on various vendor hardware. On Cisco devices, this is taken care of for you through a mapping process that can be viewed via the **show mls qos maps** command. This command shows a number of tables, but for reference the default is shown below.

```
6509_R1#sh mls qos maps
```

```

Dscp-cos map:                                     (dscp= d1d2)
d1 : d2 0  1  2  3  4  5  6  7  8  9
-----
0 :   00 00 00 00 00 00 00 00 01 01
1 :   01 01 01 01 01 01 02 02 02 02
2 :   02 02 02 02 03 03 03 03 03 03
3 :   03 03 04 04 04 04 04 04 04 04
4 :   05 05 05 05 05 05 05 05 06 06
5 :   06 06 06 06 06 06 07 07 07 07
6 :   07 07 07 07

```

The mapping is shown in a more readable format in [Figure 5-4](#). These can be changed however using the **mls qos map cos-dscp 10 15 20 25 30 35 40 45** command. In this case, it would map each of the 8 CoS values to the DSCP values shown in the command from lowest CoS priority to highest.

Figure 5-4 Mapping Between Layer 3 Mapping field (TOS) and Layer 2 CoS Fields

DSCP	CoS
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

223052

Trusting QoS CoS/DSCP

When a packet arrives on an inbound port of a switch, should the switch trust these markings? In the case of a service provider delivering broadband to the home, for example, it may not be wise to trust frames marked with a high priority. Each switch has the ability to either trust CoS, DSCP, or IP Precedence. By default, the switch rewrites the QoS values to 0, effectively nullifying the QoS markings previously marked upstream. Many times this fact is missed during the configuration steps and as such the marked traffic is reclassified to best-effort. To configure the switch to trust the QoS markings received on a port, you must enter the **mls qos trust** command. This command allows the network administrator to set, on a port-by-port basis, the default trust behavior, allowing DSCP, COS, or IP Precedence to be trusted.

```

6509-R1(config-if)#mls qos trust ?
cos          cos keyword
dscp        dscp keyword
extend      extend keyword
ip-precedence ip-precedence keyword
<cr>

```

Cisco IOS Voice Gateway QoS

In order to interface to a nurse call system for voice call back, a voice gateway (GW) may be necessary. This device is typically an Integrated Services Router such as Cisco 2800 series or 3800 series, for example, which is configured with FXO, FXS, E&M, T1, or E1 voice interfaces. In some deployments

where voice connectivity is required directly to the IMATIS Mobile Nurse Call system, the voice GW physically resides at the access layer in the network, typically on a nursing floor and often co-located in the same wiring closet as the IMATIS Mobile Nurse Call system.

The voice GW uses Cisco IOS to digitize analogue voice signals or protocol translate digitized voice traffic and map it to H.232 RAS traffic. Once this traffic is mapped, the DSCP bits are set to CS3, typically through a policy-map. This policy-map is one example of how to mark the H.323 signaling traffic at the edge switch. Once the policy map is configured, it is applied to the voice GW's outbound interface to police all H.323 RAS traffic to ensure the proper DSCP is set. By default, the RTP (audio) stream being sent by the voice GW is marked Expedite Forwarding (EF) and complies to the recommended Cisco campus QoS policy.

```
class-map match-all ras_signaling
description class map for H.323 RAS traffic
match access-group 100
!
!
policy-map set-qos
class ras_signaling
set dscp cs3
!
!
interface GigabitEthernet0/0
description To access layer switch in Nursing floor 4 North
ip address 172.21.52.101 255.255.255.240
duplex auto
speed auto
media-type rj45
no keepalive
service-policy output set-qos
```

Alert Generating Systems

Alert generating systems for Cisco Imatis Mobile Care are nurse call, ancillary clinical systems, and fire and security systems. Some of the systems utilize the same physical transport mechanisms (RS-232, IP using ESPA, TAP, etc.), but may require additional configuration when deployed within a healthcare environment.

IMATIS Mobile Nurse Call Systems

Many of the nurse call systems available today provide an RS-232 interface to external systems. The protocol from each of these systems varies across vendors and in some cases across models within the same vendor product portfolio. The common protocols are TAP (Telocator Alphanumeric Protocol), used heavily in North America, and ESPA (European Selective Paging Association), which is widely used in Europe. Despite the protocol used, it is critical that the serial data generated by these systems reliably reach the IMATIS Hospital Communication System for processing.

It is highly recommended that the IMATIS servers be located in a data center environment in order to provide a physically secure environment for this critical component. As such, it may not typically be the case that the data center is within the maximum distance allowable for a serial interface operating at 9600 bps. Long-haul modems may provide a solution to the cable length problem, but at the same time introduce multiple single points of failure and are therefore not recommend.

Conversion of RS-232 serial output to TCP/IP provides a mechanism to extend the reach of the serial interface on a nurse call system to a remote data center. In addition, it is possible to mark this TCP/IP traffic with an appropriate QoS value. In the case of Cisco Imatis Mobile Care, Cisco recommends

marking the traffic with AF31 (Assured Forwarding, Mission-Critical data). Most 3rd party RS-232 to IP converters are not capable of marking the traffic themselves and therefore require edge marking at the access layer.

Two examples of third-party RS-232 to TCP/IP converters are provided for reference.

- Digi—Digi One SP
- Precidia Technologies—iPocket232

The Digi One SP device generates TCP traffic on TCP port 771. The device communicates with a software applet installed on the IMATIS Hospital Communication System and appears as an external virtual serial port. In the sniffer trace in [Figure 5-5](#), we can see that the traffic generated by the Digi One SP is not marked with any DSCP QoS as indicated with a DSCP value of 0x00 (Best Effort).

Figure 5-5 Sniffer Trace

8	5.71842	0.205639	5.718426	10.2.2.82	10.2.2.11	TCP	771 > 4278 [PSH, ACK] Seq=0 Ack=0 win=32768 Len=1
9	5.82004	0.101623	5.820049	10.2.2.82	10.2.2.11	TCP	[TCP keep-alive] 771 > 4278 [PSH, ACK] Seq=0 Ack=0 win=32768 Len=1
10	5.82007	0.000028	5.820077	10.2.2.11	10.2.2.82	TCP	4278 > 771 [ACK] Seq=0 Ack=1 win=65254 Len=0
11	6.09961	0.279537	6.099614	10.2.2.11	10.2.2.82	TCP	4278 > 771 [PSH, ACK] Seq=0 Ack=1 win=65254 Len=1
13	6.30611	0.043366	6.306115	10.2.2.82	10.2.2.11	TCP	771 > 4278 [ACK] Seq=1 Ack=1 win=32768 Len=0
14	6.53826	0.232153	6.538268	10.2.2.82	10.2.2.11	TCP	771 > 4278 [PSH, ACK] Seq=1 Ack=1 win=32768 Len=2
15	6.53842	0.000154	6.538422	10.2.2.11	10.2.2.82	TCP	4278 > 771 [PSH, ACK] Seq=1 Ack=3 win=65252 Len=3
16	6.54118	0.002763	6.541185	10.2.2.82	10.2.2.11	TCP	771 > 4278 [PSH, ACK] Seq=3 Ack=4 win=32768 Len=3
17	6.54129	0.000111	6.541296	10.2.2.11	10.2.2.82	TCP	4278 > 771 [PSH, ACK] Seq=4 Ack=6 win=65249 Len=3

```

Frame 13 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: DigiBoar_2f:88:de (00:40:9d:2f:88:de), Dst: HewlettP_25:d6:4d (00:19:bb:25:d6:4d)
Internet Protocol, Src: 10.2.2.82 (10.2.2.82), Dst: 10.2.2.11 (10.2.2.11)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 40
  Identification: 0x5070 (20592)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
0000  00 19 bb 25 d6 4d 00 40 9d 2f 88 de 08 00 45 00  ...%.M.@./....E.
0010  00 28 50 70 00 00 40 06 12 00 0a 02 02 52 0a 02  .(Pp..@. ....R..
0020  02 06 03 03 10 b6 00 01 24 17 2c 10 4c f0 50 10  .....$.L.P.
0030  80 00 66 a2 00 00 00 00 00 00 00 00  ..F.....

```

223053

In order to mark the traffic generated from the Digi One SP, the following configuration at the edge switch is required.

```

ip access-list extended Digi_One_SP { Classify Data to be marked with Access-List }
  permit tcp any eq 771 any { Matches any source IP address with TCP 771 as
  the source port to any destination IP address }
!
class-map match-all Digi_One_SP_Class_Map {Associate Access-List to the Class Map }
  match access-group name Digi_One_SP
!
policy-map Digi_One_SP_Policy_Map {Mark all traffic matching Class Map as DSCP AF31}
  class Digi_One_SP_Class_Map
    set dscp af31
!
interface FastEthernet1/0/33
  description Digi-One-SP
  switchport access vlan 10
  spanning-tree portfast
  service-policy input Digi_One_SP_Policy_Map {Apply the policy map to the port where the
  Digi One SP is connected}
!

```

After the marking has been applied to the port to which the Digi One SP is connected, we can see that the traffic is now marked accordingly, AF31.

Figure 5-6 Traffic Flow Marked AF31

4	2.02984	0.000029	2.029846	10.2.2.11	10.2.2.82	TCP	4278 > 771	[ACK]	Seq=0 Ack=1 win=65042 Len=0
6	4.16015	1.541434	4.160155	10.2.2.82	10.2.2.11	TCP	771 > 4278	[PSH, ACK]	Seq=1 Ack=0 win=32768 Len=2
7	4.16020	0.000049	4.160204	10.2.2.11	10.2.2.82	TCP	4278 > 771	[PSH, ACK]	Seq=0 Ack=3 win=65040 Len=1
8	4.16205	0.001855	4.162059	10.2.2.82	10.2.2.11	TCP	771 > 4278	[PSH, ACK]	Seq=3 Ack=0 win=32768 Len=3
9	4.16211	0.000052	4.162111	10.2.2.11	10.2.2.82	TCP	4278 > 771	[PSH, ACK]	Seq=1 Ack=6 win=65037 Len=3
10	4.16506	0.002952	4.165063	10.2.2.82	10.2.2.11	TCP	771 > 4278	[ACK]	Seq=6 Ack=4 win=32768 Len=0
11	4.16511	0.000055	4.165118	10.2.2.11	10.2.2.82	TCP	4278 > 771	[PSH, ACK]	Seq=4 Ack=6 win=65037 Len=6
12	4.16527	0.000158	4.165276	10.2.2.82	10.2.2.11	TCP	771 > 4278	[PSH, ACK]	Seq=6 Ack=4 win=32768 Len=3
13	4.16596	0.000690	4.165966	10.2.2.82	10.2.2.11	TCP	771 > 4278	[PSH, ACK]	Seq=9 Ack=4 win=32768 Len=3

Frame 13 (60 bytes on wire, 60 bytes captured)
 Ethernet II, Src: Digiboar_2f:88:de (00:40:9d:2f:88:de), Dst: HewlettP_25:d6:4d (00:19:bb:25:d6:4d)
 Internet Protocol, Src: 10.2.2.82 (10.2.2.82), Dst: 10.2.2.11 (10.2.2.11)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x68 (DSCP 0x1a: Assured Forwarding 31; ECN: 0x00)
 Total Length: 43
 Identification: 0x51ff (20991)
 Flags: 0x00
 Fragment offset: 0
 Time to live: 64
 Protocol: TCP (0x06)

```

0000  00 19 bb 25 d6 4d 00 40 9d 2f 88 de 08 00 45 88  ...%.M.@./...E
0010  00 2b 51 ff 00 00 40 06 10 06 0a 02 02 52 0a 02  ..+Q...@.....R..
0020  02 0b 03 03 10 b6 00 01 24 f3 2c 10 4e 28 50 18  .....$.N(P.
0030  80 00 34 63 00 00 10 20 20 00 00 00  ..4c...  ...
  
```

223054

Likewise, the Precidia iPocket232 generates TCP traffic on TCP port 9999. In order to mark the traffic generated from the Precidia iPocket232, the following configuration at the edge switch is required.

```

ip access-list extended iPocket232_ACL { Classify Data to be marked with Access-List }
  permit tcp any eq 9999 any { Matches any source IP address with TCP 771
  as the source port to any destination IP address }
!
class-map match-all iPocket232_Class_Map {Associate Access-List to the Class Map }
  match access-group name iPocket232_ACL
!
policy-map iPocket232_Policy_Map {Mark all traffic matching Class Map as DSCP AF31}
  class iPocket232_Class_Map
    set dscp af31
!
interface FastEthernet1/0/34
  description iPocket232
  switchport access vlan 10
  spanning-tree portfast
  service-policy input iPocket232_Policy_Map {Apply the policy map to the port where the
  iPocket232 is connected}
  
```

For other devices that convert RS232 transports to TCP/IP, a similar marking configuration should be used to provide the necessary QoS service levels to the mission-critical data. In the event that the IMATIS Mobile Nurse Call system generates IP-based messages, these can be marked at the edge using a similar marking policy as shown above.

Cisco BSTUN Serial Tunneling

It is possible to utilize a pair of Cisco routers to convert from RS232 to IP and back to RS232. Through the use of Block Serial Tunneling (BSTUN), a serial interface on a Cisco router can be configured to encapsulate the serial traffic into IP. The advantages of using this approach is that some Cisco ISR platforms provide a higher level of redundancy features when compared to lower end point devices. Some examples are dual power and the ability for the router to be multihomed to separate switching fabrics.

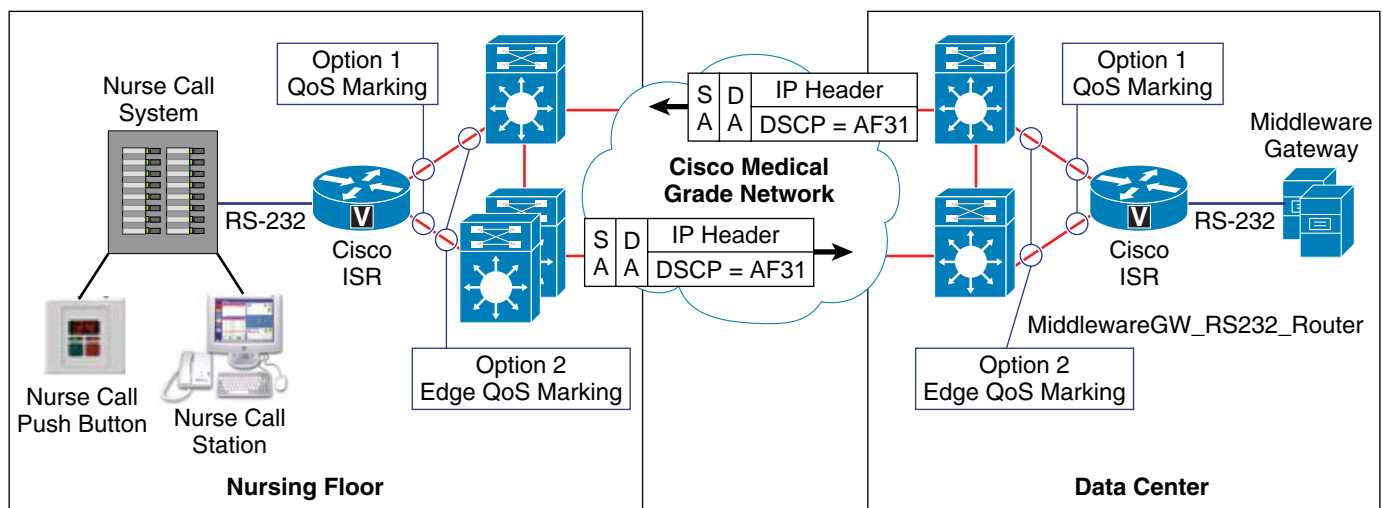
It may also be possible to leverage the router to service other traffic types. Examples of healthcare-specific legacy protocols still in wide use include serial printers, bisync printers, SNA, LAT, IPX, and DECnet. Since many of these legacy protocols are still found in many healthcare organizations, providing a dual use for a wiring closet based Cisco router can help offset the cost differential to that of point systems.

BSTUN is supported on the following platforms using IOS version 12.4(17):

1701, 1712, 1721, 1751, 1751-V, 1760, 1841, 2610XM-2611XM, 2620XM-2621XM, 2650XM-2651XM, 2691, 2801, 2811, 2821, 2851, 3631, 3640, 3640A, 3660, 3725, 3745, 3825, 3845, 7200, 7301, 7500, AS5350, AS5350XM, AS5400, AS5400HPX, AS5400XM, and CAT-4500-AGM.

The configuration in [Figure 5-7](#) shows systems connected via an end-to-end QoS-enabled IP network.

Figure 5-7 Block Serial Tunneling (BSTUN) With QoS Marking



```

hostname NursingFloor4N
!
bstun peer-name 10.1.1.1
!
bstun protocol-group 1 async-generic
!
interface loopback0
 ip address 10.1.1.1 255.255.255.252
!
interface serial0
 description To Nurse Call System 4North
 physical-layer async
 encapsulation bstun
 asp role secondary
 bstun group 1
 bstun route all tcp 10.1.1.5
!
interface FastEthernet0
 ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet1
 ip address 2.2.2.2 255.255.255.0
!
line 1
 speed 9600
 databits 8

```



```
parity none
stopbits 1

hostname MiddlewareGW_RS232_Router
!
bstun peer-name 10.1.1.1
!
bstun protocol-group 1 async-generic
!
interface loopback 0
 ip address 10.1.1.5 255.255.255.252
!
interface serial0
 description To NurseFloor 4North Nurse Call System
 physical-layer async
 encapsulation bstun
 asp role primary
 bstun group 1
 bstun route all tcp 10.1.1.1
!
interface FastEthernet0
 ip address 3.3.3.3 255.255.255.0
!
interface FastEthernet0
 ip address 4.4.4.4 255.255.255.0
!
line 1
 speed 9600
 parity none
 databits 8
 stopbits 1
```

For more information on BSTUN, refer to:

http://www.cisco.com/en/US/tech/tk827/tk369/technologies_configuration_example09186a00801dbe33.shtml

<http://cisco.com/univercd/cc/td/doc/product/software/ios112/asp.htm>

Clinical Systems

Most if not all clinical systems on the market have the ability to forward transactions in HL7 format to various ancillary systems over an IP network. As such, it is common to utilize an HL7 interface engine to apply business rules to these clinical or financial transactions, replicating and forwarding them to appropriate ancillary system(s). So for example, an ADT (Admit Discharge Transfer) system may in fact populate the database of ancillary systems (lab, radiology, etc.) with the patient name, ID, and other necessary information. Likewise, a lab system would send lab results or notifications of such results to the clinical results reporting system (EMR).

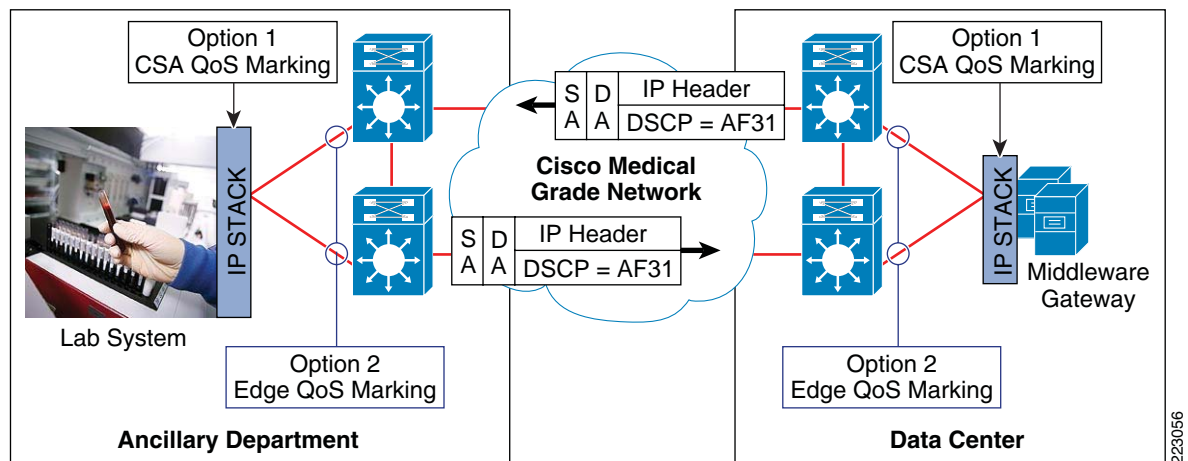
This transfer of information may occur directly between the ancillary systems or as stated previously may utilize the services of a HL7 interface engine. Some examples of such products include CloverLeaf, Egate, and Siemens Openlink.

Applying QoS markings to such systems can be accomplished using a marking technique similar to that outlined above or can optionally can be marked on the server itself using the Cisco Security Agent (CSA). In the event that the clinical system or HL7 is not able to mark the mission-critical data that it

generates with DSCP AF31, CSA has the ability to mark the traffic. In order to implement CSA on these systems, there must be careful planning with the hospital's IT security group and the systems manufacturer.

When it is not possible to mark on the server itself, either through the system's controls or the CSA, edge marking similar to our IMATIS Mobile Nurse Call marking approach must be used. Keep in mind that marking traffic must be performed on **both sides** of the connection. That is, if marked at a port level on the access layer edge switch from say an HL7 interface engine, the responses from the target system, in this case the IMATIS Hospital Communication System, must also be correspondingly marked.

Figure 5-8 Clinical Results Example with QoS Marking



Fire and Security Systems

Many fire and security systems utilize a similar mechanism as IMATIS Mobile Nurse Call systems to communicate externally as to the status of alarms and other events. This mechanism in many cases is a simple RS-232 connection or in some cases a 20mA current loop. In either case, a device that converts from such physical interface types into IP is strongly recommended, allowing the IMATIS Hospital Communication System to be located within the data center.

Marking the traffic in both directions is again critical and cannot be underestimated. Edge QoS marking at the switch port for the RS-232 to IP side is most likely the best option for third-party RS-232 to IP converters. As directed in the QoS best practices, it is best to perform QoS marking as close to the source of the traffic as possible. In this case, if the RS-232 converter device is not capable, the next location is on the switch port itself. The example below marks TCP traffic for the Precidia iPocket232 protocol converter provided that the default TCP port setting on the device is not changed.

The example below can be used to mark iPocket232 traffic on an access layer switch such as the Cisco 3750G.

```
ip access-list extended iPocket232_ACL { Classify Data to be marked with Access-List }
  permit tcp any eq 9999 any { Matches any source IP address with TCP 771
  as the source port to any destination IP address }
!
class-map match-all iPocket232_Class_Map {Associate Access-List to the Class Map }
  match access-group name iPocket232_ACL
!
policy-map iPocket232_Policy_Map {Mark all traffic matching Class Map as DSCP AF31}
  class iPocket232_Class_Map
    set dscp af31
```

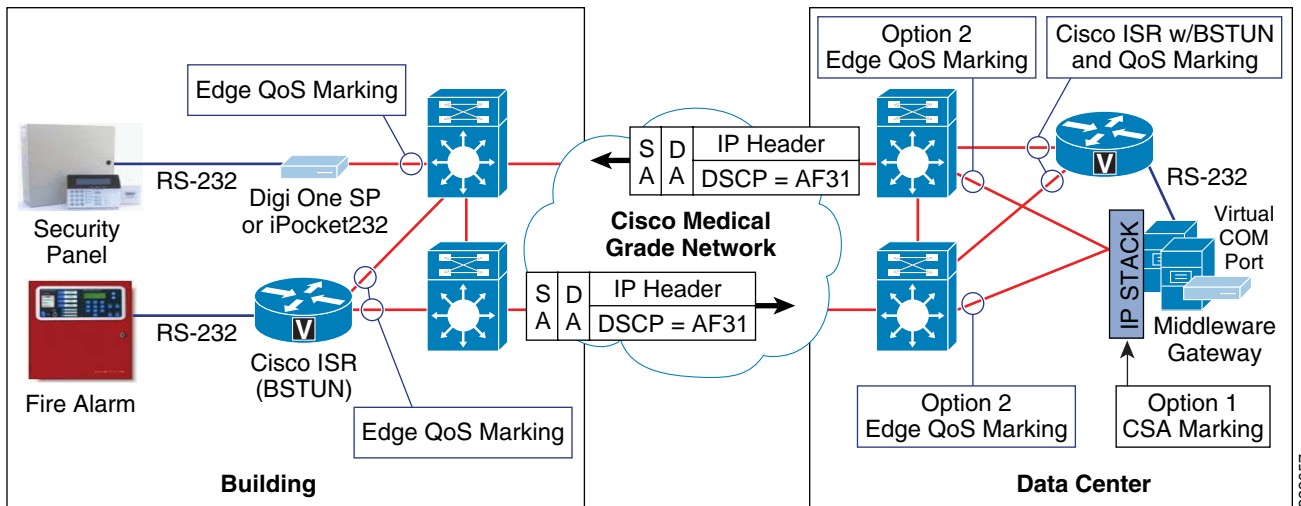
```

!
interface FastEthernet1/0/34
  description iPocket232
  switchport access vlan 10
  spanning-tree portfast
  service-policy input iPocket232_Policy_Map {Apply the policy map to the port where the
iPocket232 is connected}

```

For BSTUN configurations, a configuration similar to the one shown below can be used to establish a BSTUN connection between two ISR routers and mark the traffic accordingly. This configuration has not been validated as part of Cisco Imatis Mobile Care, but is documented here only to provide you with an example.

Figure 5-9 Fire and Security Integration with QoS Marking



```

hostname Bldg17-BSTUN-Router
!
bstun peer-name 10.10.17.1
!
bstun protocol-group 1 async-generic
!
interface loopback0
  ip address 10.10.17.1 255.255.255.252
!
interface serial0
  description To Fire Alarm Building 17
  physical-layer async
  encapsulation bstun
  asp role secondary
  bstun group 1
  bstun route all tcp 10.1.1.5
!
interface FasteEthernet0
  ip address 5.5.5.5 255.255.255.0
  service-policy output BSTUN_Policy_Map {Apply the policy map to the outgoing port }
!
interface FasteEthernet1
  ip address 6.6.6.6 255.255.255.0
  service-policy output BSTUN_Policy_Map {Apply the policy map to the outgoing port }
!
ip access-list extended BSTUN_ACL
  permit tcp any range 1976 1979 any {BSTUN TCP Ports 1976, 1977, 1978 and 1979}

```

```

!
class-map match-all BSTUN_ALL_Class_Map
  match access-group name BSTUN_ACL
!
policy-map BSTUN_Policy_Map
  class BSTUN_ALL_Class_Map
    set dscp af31
    {Set traffic matching Class-Map & ACL to af31 }
!
line 1
  speed 19200
  parity Even
  databits 7
  stopbits 1

hostname MiddlewareGW_RS232_Router
!
bstun peer-name 10.1.1.5
!
bstun protocol-group 1 async-generic
!
interface loopback 0
  ip address 10.1.1.5 255.255.255.252
!
interface serial1
  description To Fire Alarm Building 17
  physical-layer async
  encapsulation bstun
  asp role primary
  bstun group 1
  bstun route all tcp 10.10.17.1
!
ip access-list extended BSTUN_ACL
  permit tcp any range 1976 1979 any
  {BSTUN TCP Ports 1976, 1977, 1978 and 1979}
!
class-map match-all BSTUN_ALL_Class_Map
  match access-group name BSTUN_ACL
!
policy-map BSTUN_Policy_Map
  class BSTUN_ALL_Class_Map
    set dscp af31
!
interface FastEthernet0
  ip address 3.3.3.3 255.255.255.0
  service-policy output BSTUN_Policy_Map {Apply the policy map to the outgoing port }
!
interface FastEthernet0
  ip address 4.4.4.4 255.255.255.0
  service-policy output BSTUN_Policy_Map {Apply the policy map to the outgoing port }
!
line 2
  speed 19200
  parity Even
  databits 7
  stopbits 1

```

IMATIS Hospital Communication System

The IMATIS Hospital Communication System with regard to QoS is critical to the overall reliability and message delivery assurances needed for a clinical system. Again, there are a few approaches for marking the traffic using DSCP AF31 (Mission-Critical Data). As the focal point used to apply business rules and make forwarding decision, it is critical that traffic is marked in both directions for all protocol flows.

Using IMATIS Order Entry Results reporting as an example, typically these data flows are from the external ancillary system to the IMATIS Hospital Communication System and are TCP/IP port specific. Traffic generated by the lab system can be marked through a number of different techniques as previously discussed. It is critical that the TCP acknowledgments and TCP keep alive traffic from the IMATIS Hospital Communication System back to originating ancillary system is also marked AF31. Without the traffic being marked in both directions, the potential exists for the TCP connection between these two systems to become one way in an over-subscribed network, resulting in a TCP connection failure. This is a result of the acknowledgements and keep-alives being dropped as if they are not marked; they are classified as best-effort. While such events are rare, proper marking of this mission-critical data provides a level of reliability needed in the event of a virus or worm outbreak.

Cisco Security Agent (CSA) QoS Marking

Following best practices for QoS marking and traffic classification, marking the traffic before it exits the host is the most desirable method. This eliminates the effects of a host being moved from its properly-configured port to one that is not configured to provide edge QoS marking. Furthermore, providing the ability to secure the host from vulnerability found in the operating system is an added benefit of using CSA.

The Cisco Secure Agent can provide all of the security benefits to the host machine, but also has the ability to set the DSCP marking of traffic based on a policy. Assigning a DSCP marking to a class of traffic is typically performed at a TCP port level. It can however be classified as any type of IP traffic (TCP/UDP or other IP protocol traffic) that is generated by a specific application or executable running on the host machine. This could, for example, prioritize clinical information flows between a specific application on a well-known TCP port, but not prioritize similar TCP traffic based on the same TCP port but generated by a non-clinical application. Once again, during virus outbreaks or misbehaving applications, having the ability to prioritize critical clinical data flows over scavenger traffic is an obvious advantage to the Medical Grade Network design.

Configuration of the Cisco Security Agent is performed through the use of the CSA Management Console. [Figure 5-10](#) highlights the key traffic marking capabilities found within the CSA Management console. Note how the classification being performed can be applied to a specific application on a specific TCP/IP Port (1720 in this case) or can be applied to all applications as shown.

Figure 5-10 Management Center for Cisco Security Agent V5.2

The screenshot displays the configuration page for a QoS rule in the Management Center for Cisco Security Agents V5.2. The rule is titled "Trusted QoS Rule for Mobile Care" and is currently enabled. The configuration is as follows:

- Description:** Trusted QoS Rule for Mobile Care
- Enabled:**
- Take the following action:**
 - Action: **Set**
 - Attribute: **Differentiated Service** to Value: **Mission Critical Data (26,AF31)**
 - and** **Log**
- when**
 - An enforcement action of the following type: Terminate Deny Allow occurs
 - and** Applications in any of the following selected classes:
 - <All Applications>
 - <*Processes Executing Untrusted Content>
 - <*Suspected Virus Applications>
 - <First Time Application Execute>
 - <Processes Created by Network Applications>
 - But not in the following class: **<none>**
 - Attempt to act as a **client or server** for network services:
 - \$TCP Ephemeral server ports [V5.2 r203]
 - \$TCP [V5.2 r203]
 - \$HTTP [V5.2 r203]
 - \$ALT-HTTP [V5.2 r203]
 - TCP/1720
 - Communicating with host addresses: **<all>**
 - Using these local interfaces: **<all>**

Once the traffic is marked as DSCP AF31, the traffic is policed according to the end-to-end QoS policy which is configured throughout the network.

IMATIS

The Cisco Imatis Mobile Care solution has a number of Windows-based servers that provide the overall IMATIS solution. As discussed previously, in order to achieve a highly-reliable message delivery system suitable for the healthcare industry, the use of QoS marking for all message-based traffic is mandatory. The following list shows traffic types generated for the solution. On the IMATIS servers, running Cisco Security Agent in order to mark the traffic generated is one method. An alternate method is access-layer edge marking through the use of a route map.

- TCP 80—XML services on phone, between phones and IMATIS server, both directions
- TCP 80—Extension mobility, between CCM and IMATIS server, both directions
- TCP 443—AXL Soap, between CCM and IMATIS server, both directions

- UDP 161—SNMP, between CCM and IMATIS server, both directions
- UDP 162—SNMPTRAP, from CCM to IMATIS server

The following configuration marks traffic generated by an IMATIS server. Your implementation and deployment may vary as services and functions may be separated and deployed on different servers. The configuration below is only intended to provide a framework that can be customized for a given implementation strategy.

```
ip access-list extended Imatis_ACL    { Classify Data to be marked with Access-List }
  permit tcp any eq 80 any           { Matches any source IP address with TCP 80 as
  the source port to any destination IP address }
  permit tcp any eq 443 any          { Matches any source IP address with TCP 443 as
  the source port to any destination IP address }
  permit udp any eq 161any           { Matches any source IP address with UDP 161 as the
  source port to any destination IP address }

!
class-map match-all Imatis_Class_Map {Associate Access-List to the Class Map }
  match access-group name Imatis_ACL
!
policy-map Imatis_Policy_Map {Mark all traffic matching Class Map as DSCP AF31}
  class Imatis_Class_Map
    set dscp af31
!
interface FastEthernet1/0/40
  description Imatis Server
  switchport access vlan 10
  spanning-tree portfast
  service-policy input Imatis_Policy_Map {Apply the policy map to the port where the Imatis
  Server is connected}
!
```

QoS Summary and Checklist

To design a Cisco Imatis Mobile Care solution that provides an assurance level for message delivery that meets the demands of the healthcare environment, QoS must be designed into the solution from the start. Voice or mission-critical data traffic should be marked as close to the traffic source as possible. If the generating host is capable of marking the traffic, then this feature should be enabled if not enabled by default. If the originating host is not capable of marking the traffic, the use of the Cisco Security Agent is the next best step where appropriate. If this is not possible, then the traffic should be marked at the edge switch.

Once the traffic generated by both the sending and receiving hosts has been marked, the next step is to enable QoS policies on each network component in the end-to-end network, including wired Layer 2/Layer 3 switches as well as the wireless components, namely the Wireless LAN Controller (WLC).

1. Mark traffic generated by sending host.
 - a. CSA Marking within the originating host.
 - b. Edge marking via route map.
2. Mark traffic response from receiving host.
 - a. CSA Marking within the originating host.
 - b. Edge marking via route map.
3. Verify that QoS trust is appropriately configured end-to-end.
4. Verify that Layer 3 to Layer 2 and vice versa mapping is configured correctly.
5. Configure a QoS policy on each network device end-to-end.

- a. Use Auto-QoS if available.
 - b. Manually configure QoS policy.
6. Apply QoS policy to all ports necessary.
7. Verify at each endpoint that traffic being sent to it from remote systems is appropriately QoS marked.
 - a. If not, recheck traffic flow at network midpoint until reclassification location is determined.
8. Verify that Wireless LAN Controller is configured to support VoWLAN traffic priority.
9. For LWAPP Access points, ports need to trust DSCP not CoS as traffic is sent at Layer 3 via LWAPP and not bridged at Layer 2.

Unified Communications Manager

The Cisco Unified Communications Manager provides a number of services for a typical installation of Cisco Imatis Mobile Care. First, it provides signaling and control to all handsets registered to it. Second, it must interact with the IMATIS servers using a number of different protocols, which include SNMP, AXL, Syslog, and TAPI. Lastly, it can provide XML services to the phone or, at a minimum, provide the end user with a menu of subscribed services which may include the middleware application and in some deployments Extension Mobility. Some of these traffic flows by standard telephony standards are considered critical for voice delivery and are automatically marked by both the handset and Unified Call Manager. Others are not classified as mission-critical and are therefore not marked accordingly. Because of the nature of the message content as it relates to patient care, it is imperative that all traffic types originating from Unified Call Manager which comprise the Cisco Imatis Mobile Care solution be properly marked as mission-critical data (AF31).

Talking a logical approach, we examine each of the different protocols in the solution and reserve the discussion of the unique protocols respectively in each section for the IMATIS servers.

Endpoint devices generate two primary traffic flows for voice traffic that must be QoS marked and by default Unified Call Manager performs the marking. These can be summarized as the signaling channel and the bearer channel.

The signaling channel is responsible for the control of an endpoint, from collecting digits to signaling an inbound or outbound call. There are three types of signaling traffic in Cisco Imatis Mobile Care:

- SCCP (Skinny)—Typically used for endpoint signaling
- SIP (Session Initiated Protocol)—Typically used for endpoint signaling
- H.323—Used for Voice Gateway Call Control

The second is the bearer channel, which carries the audio or video traffic between endpoints. Again, this is automatically marked by both the endpoints and Unified Call Manager. More specifically, the protocol used to carry the packetized voice traffic is Real Time Protocol (RTP). RTP uses UDP and is dynamically assigned a UDP port number in the range of 16384-32767. The port selection is coordinated and communicated by the endpoints using the signaling protocol configured for the specific endpoint device.

The third protocol used is Trivial File Transfer Protocol (TFTP). This protocol (UDP 69) is used to transfer the configuration to the phone during each registration performed with Unified Call Manager. In addition to the configuration file, ring tones are transferred to the phone when instructed to do so by the IMATIS Hospital Communication System. This enables the phone to have dynamic ring tones that can correspond to various levels of message importance. Since the ring tone in some cases may be signal a critical event requiring immediate attention, TFTP must also be marked as mission-critical AF31.

Since Unified Call Manager automatically marks both signaling and bearer traffic, as well as instructs the registered endpoints as to which DSCP classification to use, there is little or no configuration necessary. Validating that the traffic is marked accordingly should be done during the implementation phase of all Cisco Imatis Mobile Care deployments.

In order to mark XML traffic generated by XML applications running on the phone, the DSCP for Phone-based Services field needs to be configured. This field is accessed on Call Manager and by default is valued at 0x00 for DSCP. When a phone boots up and downloads its configuration file from Call Manager, this setting is pushed to the phone. The field can be found in Unified Call Manager under System > Enterprise Parameters and is shown below.

- DSCP for Phone-based Services—This parameter specifies the Differentiated Service Code Point (DSCP) IP classification for IP phone services on phones, including any HTTP traffic.



Note You must restart phones for the parameter change to take effect. The default DSCP is (000000).

- DSCP for Phone Configuration—This parameter specifies the Differentiated Service Code Point (DSCP) IP classification for any phone configuration, including any TFTP, DNS, or DHCP access that is necessary for phone configuration.

The DSCP setting for phone configuration protocols is by default valued to CS3 (Call Signaling 3). Since this conforms to Cisco's recommended QoS Policy for IP telephony, no changes are required. It is however recommended that you verify that this field has been configured accordingly.



Note You must restart phones for the parameter change to take effect. The default is CS3 (precedence 3) DSCP (011000).

Figure 5-11 Cisco Unified CM Administration—Enterprise Parameters Configuration

Parameter Name	Parameter Value	Suggested Value
Synchronization Between Auto Device Profile and Phone Configuration *	True	True
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	AF31 DSCP (011010)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)

Likewise, the definition of the field found in Unified Call Manager under System > Enterprise Parameters are shown below.

- DSCP for Audio Calls—This parameter specifies the Differentiated Service Code Point (DSCP) value for audio calls. The default is EF DSCP (101110).

Figure 5-12 Cisco Unified CM Administration—Service Parameters Configuration

The screenshot shows the Cisco Unified CM Administration interface for Service Parameter Configuration. The page title is "Service Parameter Configuration" and it includes a navigation menu with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the navigation, there are buttons for Save, Set to Default, and Advanced. The main content area is titled "Clusterwide Parameters (System - QoS)" and contains a table of parameters with dropdown menus for selection.

Parameter Name	Current Value	Target Value
Priority Class *	Normal Priority	Normal Priority
DSCP for Audio Calls *	EF DSCP (101110)	EF DSCP (101110)
DSCP for Priority Audio Calls *	EF DSCP (101101)	EF DSCP (101101)
DSCP for Immediate Audio Calls *	EF DSCP (101100)	EF DSCP (101100)
DSCP for Flash Audio Calls *	EF DSCP (101001)	EF DSCP (101001)
DSCP for Flash Override Audio Calls *	EF DSCP (101010)	EF DSCP (101010)
DSCP for Executive Override Audio Calls *	EF DSCP (101010)	EF DSCP (101010)
DSCP for Video Calls *	AF41 DSCP (100010)	AF41 DSCP (100010)
DSCP for Audio Calls when RSVP Fails *	default DSCP (000000)	default DSCP (000000)
DSCP for Video Calls when RSVP Fails *	default DSCP (000000)	default DSCP (000000)
DSCP for ICCP Protocol Links *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)

Voice

Cisco Imatis Mobile Care lets care providers initiate voice calls in response to events sent to their handsets. This capability is exploited in the following IMATIS services:

- IMATIS Mobile Nurse Call
- IMATIS Order Entry Alerts
- IMATIS Medical Team Assembly
- IMATIS Hospital Orderly

As a vital part of the overall solution, careful planning and adherence to the related design guides is strongly encouraged for successful deployment.

Voice Port Utilization and Planning

It is important to the overall availability of the system from an end users perspective that there are ample voice ports available to handle any voice call back or offnet calling that is being generated by the clinical staff and patient community. Using the typical voice engineering capacity planning based on the Erlang B protocol, it is possible to determine a recommended number of lines/ports that are needed to achieve a desired level of service. An Erlang is the total number of call seconds generated in one hour during the busiest time during a 24 hour period divided by the number of calls in that same hour. If, for example, the busiest hour generates 3976 seconds in 23 calls, the number of Erlangs can be calculated as:

$$3976/3600 = 1.104 \text{ Erlangs}$$

Next we need to utilize the Erlang B formula shown in [Figure 5-13](#).

Figure 5-13 Erlang B Formula

$$B(c,a) = \frac{\frac{a^c}{c!}}{\sum_{k=0}^c \frac{a^k}{k!}}$$

Where:

- B(c,a) is the probability of blocking the call.
- c is the number of circuits.
- a is the traffic load.

To quickly determine the number of lines needed, it may be useful to use the Erlang B calculator found at <http://www.erlang.com/calculator/erlb/>.

As a working example, let us assume that we have a 40 bed floor that generates, during the busiest hour in 24 hours, 80 calls (each patient calls two times in one hour) and each call lasts 60 seconds. This would generate 80 calls * 60 seconds each or 4800 total call seconds. To determine the number of Erlangs this represents, we divide (80 * 60)/3600, which results in 1.333 erlangs. Next, using the Erlang B calculator found at <http://www.erlang.com/calculator/erlb/>, we enter 1.333 as the Erlang value. Next we need to determine the number of calls that we can tolerate being blocked per 100 calls. We would therefore enter 0.01 into the Erlang B calculator for the number of blocked calls. Since our goal is not to have any blocked calls, instead of using 0.01, representing one blocked call for every 100 calls, we will use a value of 0.001, which represents one blocked call in every 1000 calls—well above our call volume for the busiest hour encountered. The Erlang B calculator, using these values, tells us that for this floor and call load we need seven lines available.

Figure 5-14 Erlang B Calculator

What this does not take into account, however, is a nursing floor that may have 15 on-duty clinicians along with a dynamic number of transient users, such as physicians on rounds, orderlies, transportation, housekeeping, and so on. If these users utilize the same Voice Gateway for outbound calls, additional capacity may be required. If during the planning process these additional users were not considered and only nurse call bed count was taken into consideration, it may be likely that the voice port capacity has been under-provisioned.

In order to fully understand the voice port capacity engineering, its recommended that the Cisco Imatis Mobile Care design and implementation partner consult the IP Telephony/Voice over IP (VoIP) Traffic Analysis white paper available on CCO at:

http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800d6b74.shtml

Disconnect Supervision

With digital voice interfaces such as T1/E1 PRI, T1 CAS, or T1/E1 BRI, disconnect supervision is provided through signaling on the D channel, or in the case of Channel Associated Signaling (CAS), via the robbed bit signaling protocol. In most instances, disconnect supervision on these interfaces is not a problem. For analog interfaces such as FXO, FXS, and E&M interface, the process of signaling a disconnect or end-of-call can sometimes be troublesome depending on the mechanism used.

It is therefore recommended to validate that disconnect supervision is being properly handled between the voice gateway and the legacy system. This validation should be performed for each port that is in use and not just for 1 port. It has been found that some versions of firmware running on the legacy line cards found in some PBXs and nurse call systems do not properly implement the disconnect supervision as required. In some deployments, it may be possible that one line card is running an updated firmware revision that provides the correct disconnect supervision, while another card in the same system is running older code. This is why each port needs to be separately validated for proper call disconnect functionality.



Note

It has been discovered that some earlier versions of Dukane Nurse Call systems, now a GE Medical company, have disconnect supervision problems.

This can be corrected by upgrading the version of firmware on the Dukane station to version 4.01 or higher. The problem on older versions of firmware is that the Dukane system does not recognize a Power Denial-based Supervisory Disconnect, which by default lasts for at least 350ms.

GE/Dukane Disconnect Signaling

```
* DTMF enter "###"           all versions (clinician must enter ## before disconnecting
the call)
* 40-90 second timeout       all versions (Port remains in use for 40-90 seconds
then automatically resets)
* 300 - 500 ms loop drop     GE phone port firmware version <= 4.00 (GE/Dukane
Recognizes a power denial in this range)
* 250 - 1500 ms loop drop    GE phone port firmware version >= 4.01 (GE/Dukane
Recognizes a power denial in this range)
```

To assist in troubleshooting disconnect supervision problems, it is recommended that the document called “Understanding FXO Disconnect Problem” which can be found on CCO at the following URL be consulted.

http://www.cisco.com/en/US/tech/tk652/tk653/tsd_technology_support_troubleshooting_technotes_list.ht

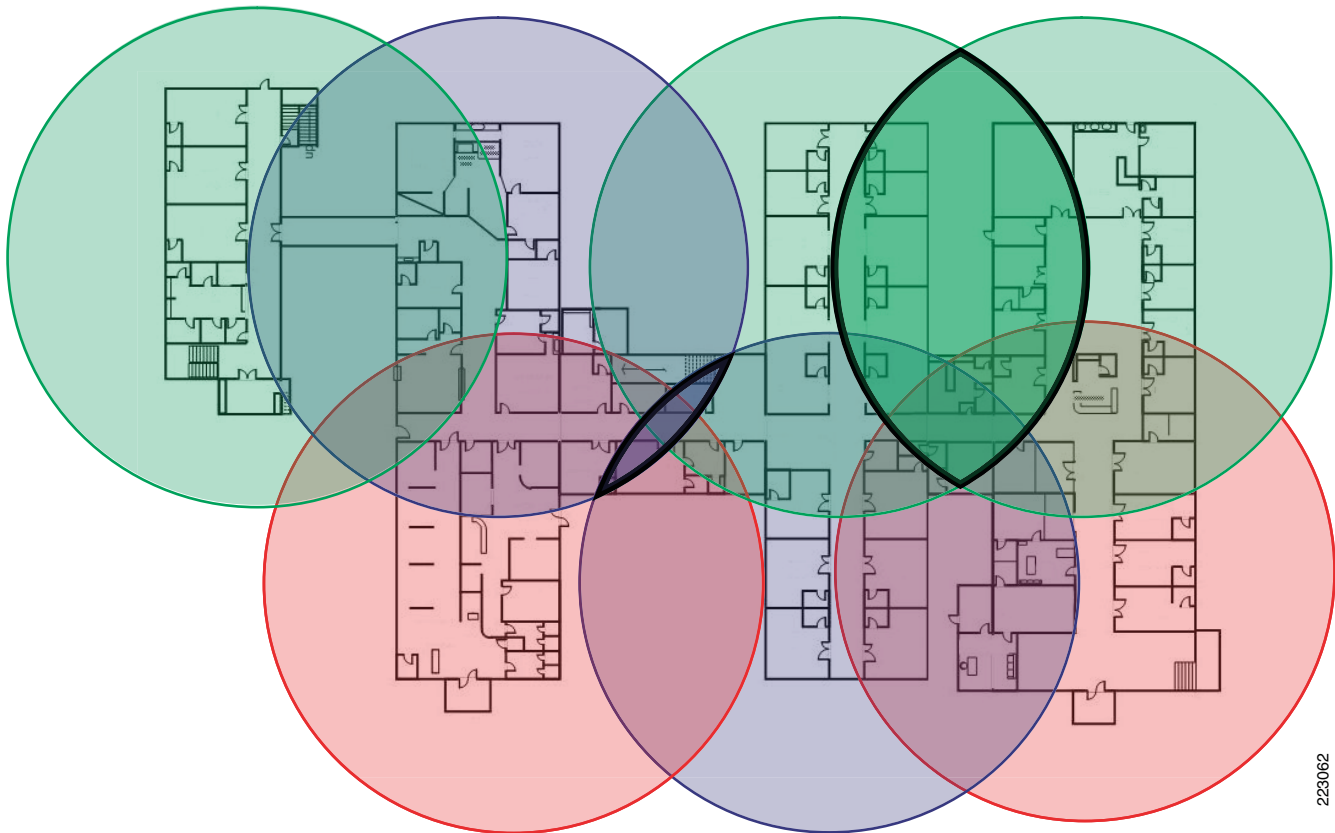
VoWLAN

The Cisco Imatis Mobile Care solution comprises a number of different horizontal technologies such as VoIP and wireless. As such, each of these technologies, as well as other best practices, are not discussed in detail in this guide. Instead, this document provides a high-level overview of design guidance and references the supporting horizontal design guides. Customer and implementation partners are strongly urged to review each of the design guides for best practices in order to design and implement a robust, scalable, and secure solution deployment. The design guides can be found on Cisco’s web site at <http://www.cisco.com/go/srnd>.

Because of the critical nature of the healthcare industry, it is critical that the underlying and supporting infrastructure for VoWLAN, namely Unified Mobility, is designed and implemented to support the unique demands of VoWLAN within a healthcare enterprise.

Many healthcare environments have sources of RF interference and these sources are not generally limited to the typical microwave oven or 2.4Ghz cordless phones. Other sources can include 2.4Ghz video cameras, bluetooth devices, as well as patient and visitor devices, such as Wi-Fi-enabled PCs and dual-mode phones. Multipath interference, caused by reflected signals as well as co-channel interference from adjacent hospital wings, must also be considered. Figure 5-15 shows an exaggerated incorrect deployment strategy for a 2.4Ghz, but highlights the increased possibility of co-channel interference found in a typical healthcare environment due in part to poor design and building floor plan.

Figure 5-15 Exaggerated Incorrect Deployment Strategy



223062

Due to the rise in consumer devices within the 2.4Ghz ISM band and the limited number of non-overlapping channels, it is recommended to migrate voice traffic as well as critical data-based services into the 5Ghz band. On the 5GHz (802.11a) band, all 23 channels (depending on geographic area) are non-overlapping channels. This results in an increased network capacity, improved scalability, and the ability to deploy with less likelihood of co-channel interference.

It is therefore recommended to migrate all critical data and voice services to the 5Ghz band whenever possible to reduce the likelihood of interference from a number of sources.

QoS Issues

There are a number of QoS-related issues that should be considered during the Cisco Imatis Mobile Care design and implementation phases. First, let us look at how QoS is handled as it relates to VoWLAN. The handsets are configured during the registration process with Call Manager for the QoS settings that are to be used. By default, both the RTP and SCCP/SIP control channels are Layer 3 marked as DSCP EF and CS3, respectively. At Layer 2, the CoS is 3 for call signaling and 5 for voice. For LWAPP-enabled wireless networks, however, the AP is connected directly to an access-layer switch port. The wireless traffic generated by wireless hosts associated to the AP is encapsulated in LWAPP frames and sent to the controller, typically over a Layer 3 network. So trusting the Layer 2 CoS is not necessary at the switch to which the APs are connected. Instead, DSCP should be trusted in LWAPP configurations.

So switch ports to which LWAPP-enabled access points are connected to should trust DSCP and can be configured using the commands shown below. For Layer 3 uplinks from the access layer to the distribution layer, DSCP should also be trusted.

```
interface GigabitEthernet1/0/1
  description LWAPP Access Point
  auto qos voip trust
  mls qos trust dscp
<SNIP>

interface GigabitEthernet1/0/48
  description L3 uplink to distribution
  mls qos trust dscp
  auto qos voip trust
  no switchport                                     {enables port as an L3 routed port,
not an L2 based VLAN access port}
  ip address 10.6.1.1 255.255.255.252
  srr-queue bandwidth share 10 10 60 20 {configured as part of auto qos voip trust
command}
  srr-queue bandwidth shape 10 0 0 0 {configured as part of auto qos voip trust
command}
  queue-set 2                                       {configured as part of auto qos voip
trust command}
<SNIP>
```

Since the Wireless LAN Controller trunks multiple VLANs and maps these to specific SSIDs, the WLC therefore connects to the network at Layer 2. As such, trusting CoS as opposed to DSCP is necessary and is shown in the configuration below.

```
interface GigabitEthernet1/0/1
  description Connection to Wireless LAN Controller
  auto qos voip trust
  mls qos trust cos { Note that due to bug CSCsi78368, the CoS is not being set properly
form the WLC. It is therefore necessary to trust DSCP until WLC release 4.2 }
<SNIP>
```

7921G QoS Issue

During the validation phase, it was discovered that the 7921G phone, when running firmware 1.0.4, fails to implement the QoS setting directed by Call Manager for XML/CTI services. The workaround is to view the QoS setting on the phone which causes the value to be written to non-volatile memory, where it is used from this point on, even across phone reboots and power cycles. This fix, CSCsk79795, is scheduled to be included in firmware 1.0.5.

To verify if you are experience this problem, a sniffer trace taken of the traffic being generated by the 7921G when executing XML-based services shows that the DSCP value is configured as 0 or best effort. When viewing the QoS settings on the 7921G handset directly, if configured in Call Manager for AF31

(mission critical data), AF31 is displayed as the value to be used for XML/CTI-based traffic. After viewing this setting on the handset, another sniffer trace should show that the XML/CTI traffic is now marked AF31 as required.

Figure 5-16 XML/CTI Traffic is Now Marked AF31



High Availability (HA) Considerations

The goal of a highly-available system is to eliminate and automate as much as possible all aspects of the solution. A signal point of failure anywhere in the system can lead to unscheduled outages as well as possibly sporadic availability. Monitoring of the overall system end-to-end is also a critical component to determine just how available the system is. Since there are a number of different technologies used in the solution, we break down each component part to identify possible HA architectures. For each major grouping of components, we also include suggested monitoring systems and techniques that can be employed in order to validate the availability.

Unified Communications Component

Cisco Infrastructure

The Cisco infrastructure required to deliver the Cisco Imatis Mobile Care solution can be broken down into a number of horizontal technologies which are described in the subsections below. It is beyond the scope of this document to describe in detail the various high availability aspects of each technology used. For an in-depth discussion, it is recommended that the Solution Reference Network Designs and Cisco Validated Designs (CVDs) be referenced. The SRND and CVDs can be downloaded from <http://www.cisco.com/go/srnd> and <http://www.cisco.com/go/cvd> respectively.

In summary, the overall availability of Cisco Imatis Mobile Care depends upon the infrastructure on which it is deployed. Items that should be considered in the high availability planning process include:

- Network core, distribution, and access
- Diverse power sources for each component comprising a pair of redundant devices or servers
- Redundant Active Directory, DNS, and DHCP servers

- Redundant wireless components
 - Wireless LAN Controllers (WLC)
 - Access point density sufficient to support fault tolerant design
 - ACS servers used for wireless user authentication
- Redundant Unified Communications components
 - Call Manager Clusters with redundant TFTP servers activated
 - ISR Voice Gateways
 - Server Load Balancing SLB for XML service redundancy
- Redundant paths between core, distribution, access, and wireless layers
- Validated Layer 2 and Layer 3 routing protocols for rapid convergence
- Dual-homed servers utilizing Fast Etherchannel on separate switch fabrics (IMATIS, ACS, DNS, DHCP, Active Directory, etc.)
- Cold spared hardware for core, distribution, access, wireless controllers, access points, servers, etc.
- Each redundant component should be on a separate maintenance, upgrade, and outage schedule.

Although only a summary, this lists items that must be considered during the GAP analysis phase.

Network Components

The network components include the Layer 2 and Layer 3 devices that compose the campus network and specifically include access, distribution, and core layers. There are a number of Solution Reference Network Design guides (SRNDs) available. The key documentation that is recommended for Cisco Imatis Mobile Care include:

- Designing a Campus Network for High Availability
- Campus Network Multilayer Architecture and Design Guidelines
- Deploying a Fully Routed Enterprise Campus Network
- Campus Design: Analyzing the Impact of Emerging Technologies on Campus Design

After reviewing these SRNDs, it is recommended that a GAP analysis or readiness check be performed. To help facilitate this step, it may be helpful to engage a third-party Cisco Certified implementation partner for each of the areas where a GAP was identified. In general, and in line with eliminating all single points of failure in the design, the following are mandatory for achieving a highly available network architecture which is capable of delivering between 99.99% and 99.999% availability. These levels of availability represent between 52.33 and 5.35 minutes of downtime per year, a goal that is highly desirable for any network delivering critical services such as those found in Cisco Imatis Mobile Care.

IMATIS Hospital Communication System

The IMATIS system is built around high availability mechanisms provided through Windows and BizTalk. The system can be configured in a redundant manner, where the IMATIS server and Database Server use Windows clustering and the Message Server uses BizTalk group for redundancy. Through this design, there is always a server available to any components that need to communicate with IMATIS, such as Nurse Call Systems, Hospital Information Systems, or CUCM. To these outside components, a IMATIS server is available. Internally, the redundant servers ensure a server is always available to process new requests.

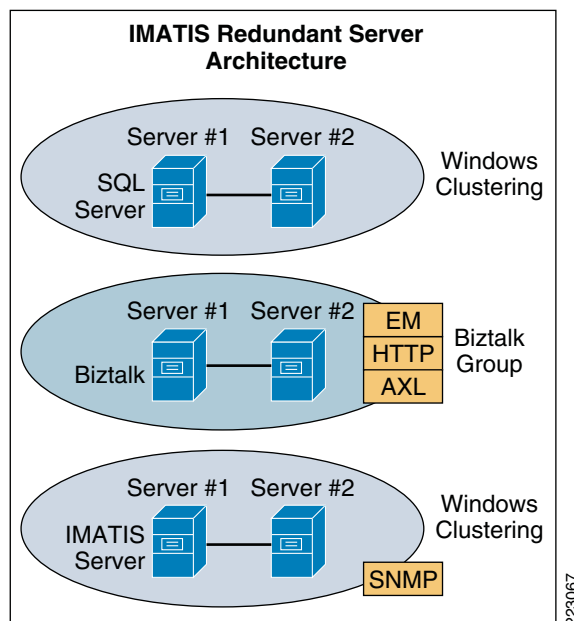
IMATIS Components

IMATIS is comprised of three server types:

- IMATIS server
- BizTalk server
- SQL server

To form a redundant architecture for these servers, the IMATIS server and SQL server use Windows Clustering and the BizTalk server uses BizTalk Groups to create redundancy. The BizTalk server and the IMATIS server have interfaces to CUCM or adapters to hospital equipment. To ensure that the active server is always available to serve any request, these servers should always be accessed through a virtual IP address. Using Windows Clustering or BizTalk Groups, the actual servers are always reachable through the virtual IP address.

Figure 5-17 IMATIS Redundant Server Architecture



Wireless Mobility Components

As is the case with any healthcare-related solution, a wireless design must consider and implement solid end-to-end security. It is therefore important to review some of the solution reference guides that provide detailed guidance on security as it relates to this solution. As is always the case, adherence to current best practices is always recommended for any healthcare IT-related engagement. With respect to mobility, which provides much of the service delivery for Cisco Imatis Mobile Care, reference the Secure Wireless 1.0 Design guide at <http://www.cisco.com/go/srnd>.

To address many of the security requirements with wireless mobility technologies as they relate to Cisco Imatis Mobile Care, this is the list of components in the end-to-end solution:

- Wireless LAN Controller (WLC)
- Access Control Server (ACS)

- Access Points (AP)
- Wireless Clients (7921G for IMATIS Mobile Care)

High availability for wireless mobility spans a number of different network infrastructure components. It is assumed for this discussion that the existing wired infrastructure has been designed to provide high availability end-to-end.

Access Points

The recommended 20% overlap is not a recommendation that applies to engineering a highly-redundant network. Rather, the 20% overlap rule is an RF engineering recommendation that attempts to provide seamless roaming by providing the wireless client with enough time to select a new access point onto which it can roam. To achieve High Availability, it is recommended to increase this overlap while paying close attention to the potential for co-channel interference. In order to provide hardware level redundancy for a centralized wireless deployment, the Wireless LAN Controller (WLC) dynamically adjusts the power output of APs adjacent to one that is no longer available. This capability, and the design aspects of achieving a High Availability wireless design, is discussed in the VoWLAN design guide located on Cisco's Web site:

http://www.cisco.com/en/US/netsol/ns741/networking_solutions_products_generic_content0900aecd80601e1d.html#mobility

Wireless LAN Controllers

The Wireless LAN Controllers (WLCs) provide configuration and management for the access-points in the wireless network. Much of this management is both automatic and dynamic in nature and as such requires a redundant design if high availability is to be achieved. It is not only necessary that there are redundant WLCs, but in addition the failure of any single WLC must not over subscribe the surviving WLCs.

If we take, for example, a wireless network consisting of the following, with each controller at 50% of its licensed capacity:

- 4402 which supports 12 APs (supporting 6 APs)
- 4402 which supports 50 APs (supporting 25 APs)
- A single WiSM in a 6509 which supports 150 APs (supporting 75 APs)

In the above example, the failure of the WiSM would result in 75 APs requiring WLC services. The 4402-12 and 4402-50 only have spare capacity to support 31 APs (6 + 25). It is therefore critical that ample WLC resources are available to support any possible WLC failure scenario.

Security for the WLC should include basic appliance security, which prevents unauthorized user access to the administrative and configuration sections of the WLC. After this, configuration of the wireless network takes into account a few items such as VLAN creation, SSID assignment, RADIUS authentication servers, and of course the encryption and authentication mechanisms used for each SSID.

Authentication

The recommended configuration is to use 802.1X authentication. This mandates the use of an external RADIUS server to authenticate end user devices. By using Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), the entire authentication stream is encrypted end-to-end. This approach provides a high level of security across the wireless network during the authentication process.

On the 7921G, configuration of EAP-FAST is found under Settings > Network Profiles > [Your Profile Name] > WLAN Configuration > Security Mode. Selecting EAP-FAST and configuring a unique userid and password on the device that conforms to strong security standards is all that must be done. This userid/password combination can be a locally-defined userid/password combination that is located on the ACS server directly. Optionally, the userid/password account can exist within the Active Directory domain which ACS can use as an external authentication database to validate userid/password as configured.

Once the userid/password is authenticated by one of the two means described above, a dynamically created WPA key is generated by the ACS server and effectively pushed to the 7921G to encrypt traffic generated by the device. This includes voice, call control, and XML services. To an observer using a wireless sniffer, all traffic generated by the device is encrypted with dynamically changing keys as provided by the TKIP protocol.

Figure 5-18 Traffic Encrypted with Dynamically Changing Key



Another item that must be completed in order to enable EAP-FAST against the WLC controller is to adjust the 802.1x timeout value. In ACS, the default is 20 seconds, but on the Wireless LAN Controller, the default is two seconds. In order for the client to obtain the PAC used for encryption via automatic provisioning on the 7921G, the value must be changed on the WLC to a higher value. The suggested timeout is 20 seconds on the WLC as indicated on page 25 of the 7921G Deployment Guide found on Cisco's Web site. To change the 802.1x timeout on the WLC, telnet or SSH to the controller and enter the following command:

```
(Cisco Controller) >config advanced eap request-timeout 20
```

```
(Cisco Controller) >show advanced eap
```

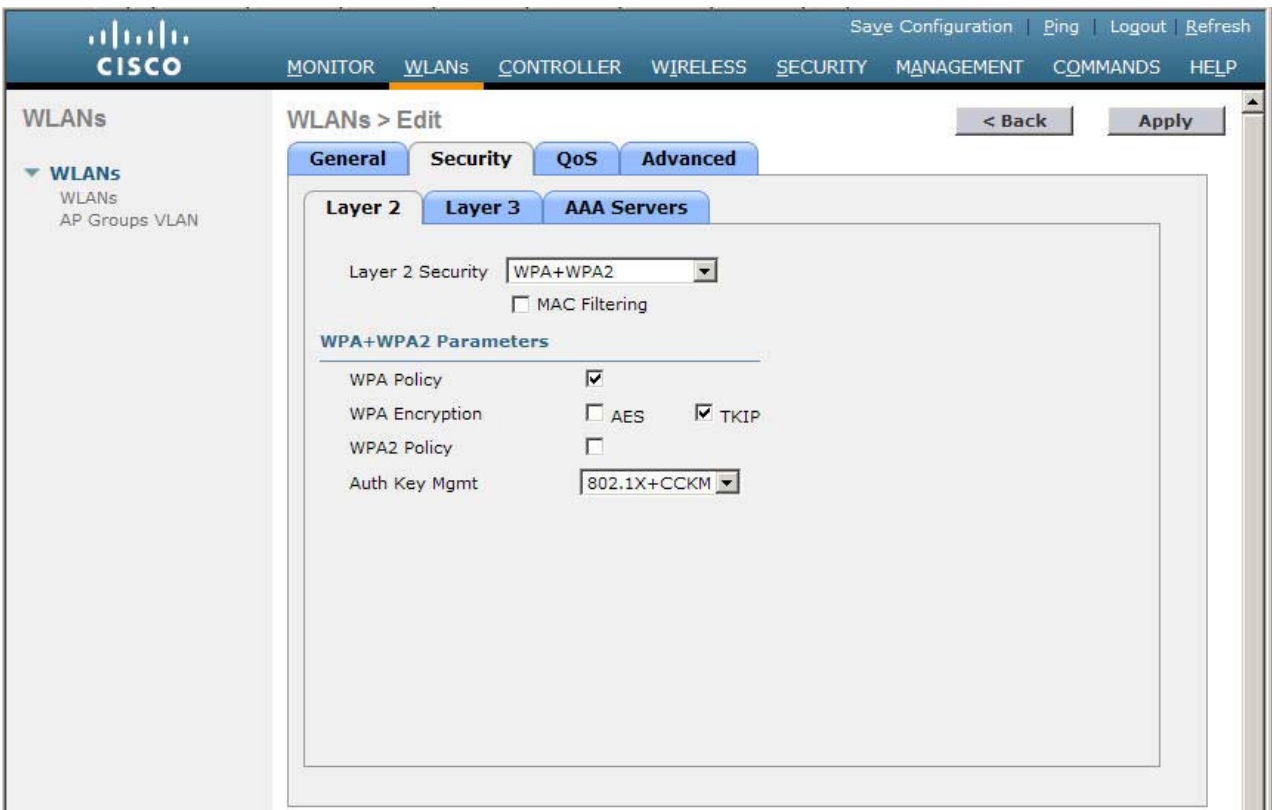
```
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 20
```

EAP-Request Max Retries..... 2

Encryption

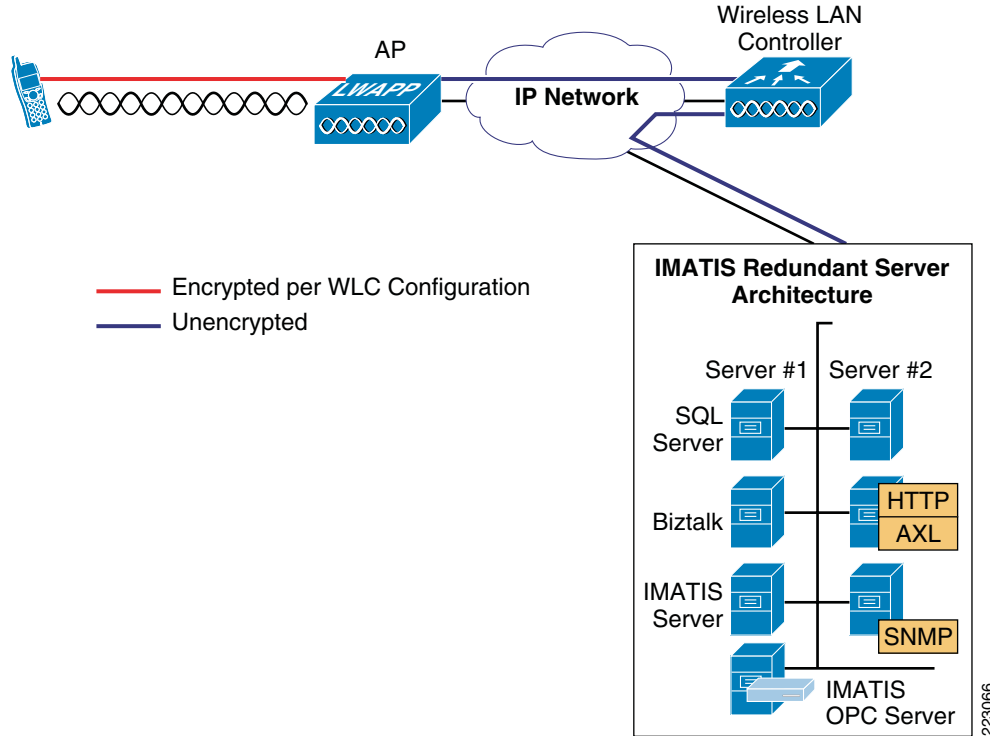
Between the wireless client (7921G) and the Wireless LAN Controller, it is recommended to use the WPA security protocol with TKIP encryption and 802.1x-with-CCKM key management. This is necessary as WPA2 does not provide predictable fast roaming. [Figure 5-19](#) shows the recommended encryption settings as configured on the Wireless LAN Controller.

Figure 5-19 Recommended Encryption Settings



It is important to understand the scope of the encryption as shown in [Figure 5-20](#) as it pertains to XML services. XML traffic between the 7921G phone and the Wireless LAN Controller (WLC) is encrypted as configured on the WLC. After the XML traffic is decrypted on the WLC, it is sent unencrypted as standard http XML flows. Secure HTTP (https) is not currently supported by the 7921G.

Figure 5-20 Scope of Encryption



Authentication Server (ACS)

The Cisco Secure Access Control Server (ACS) provides authentication, authorization, and accounting (AAA) services for users of the wireless network. The ACS server extends the integration of the user database to a number of external user databases. These external user databases can be Microsoft Active Directory or other LDAP-based user directories. In addition to providing authentication services to wireless users, it can also be used to provide administrative access to various network components, such as Integrated Services Routers (ISR) and switches. Restricting access to these systems can not only provide the security necessary for the overall security policy of the healthcare provider, but can also increase availability of the Cisco Imatis Mobile Care solution by preventing unauthorized access.



Note

As part of Cisco Imatis Mobile Care validation, EAP-FAST was tested with Cisco Secure ACS version 4.1.3 build 12.

1:1 WLC Redundancy

Using the example from above, in the event of either 4402 failing, the surviving WiSM LC has additional spare capacity to support the 6 or 25 APs from the failed 4402. If however the WiSM or 6509 in which it is installed fails or has a disruption of connectivity, the surviving 4402s do not have spare capacity to service the additional APs. When employing a 1:1 redundancy strategy, it is critical to perform a case-by-case failure analysis and determine if the design is able to provide a high level of availability as required for Cisco Imatis Mobile Care.

N+1 WLC Redundancy

It is also possible to employ a WLC controller strategy that uses an N+1 approach. When using N+1 architecture, each WLC is configured with a WLC that is designated as a backup WLC in the event of a failure. This controller is not used until there is a failure event upon which all APs using the failed controller switch to the backup WLC. This cost-effective approach provides a high level of availability in the event of a single WLC failure scenario.

The wireless controllers validated as part of the Cisco Imatis Mobile Care solution include the 4400-based controllers running version 4.1.181.0. As such, a few bugs have been discovered as part of the VoWLAN testing and are described in detail in the VoWLAN design guide. To summarize, the mapping between DSCP and CoS is not being performed properly and as such the end-to-end QoS mapping between DSCP and CoS may be lost depending upon what trust model is being used on the switch that is providing connectivity to the WLC. To work around this bug (CSCsi78368—found in 4.1.181 WLC code), it is necessary to trust the DSCP information as it is marked correctly from the WLC. This has been addressed and corrected in version 4.2 of the WLC code. Information about this bug and possible workarounds are discussed in the VoWLAN design guide at the following URL:

http://www.cisco.com/en/US/netsol/ns741/networking_solutions_products_generic_content0900aec80601e1d.html#mobility

Solution Component Interconnections

In this solution, several interconnections between components are required. This section outlines some of the design principles to consider for those interconnections. These interconnections may connect equipment that spans across a hospital campus and data center. As such, the QoS and high availability designs are critical as these interconnections are implemented.

CUCM to IMATIS Connections

Communication between CUCM and IMATIS uses three interface types:

- AXL for initial phone login and logoff
- SNMP for any state changes to phones
- EM for proxy extension mobility login over HTTP

A system user defined on the BizTalk server will be authorized to use the AXL interface. Each of the BizTalk servers is configured as a primary and backup interface. With two BizTalk servers or more in the BizTalk group, CUCM has more than one BizTalk server to connect in case one BizTalk server fails.

The SNMP interface connects between CUCM and the IMATIS server. When configuring the SNMP interface on the CUCM publisher, an option to “Apply to all nodes” is available and should be configured. Each CUCM server in the cluster is configured with the IMATIS server as the receiver for the SNMP messages. With multiple IMATIS servers in a windows cluster, an IMATIS server should always be available.

The EM proxy interfaces runs through the BizTalk server. The BizTalk server should be configured as a phone would be configured for XML Service Redundancy as outlined in [Chapter 6, “Implementing the Cisco Imatis Mobile Care Solution.”](#) The CUCM has a virtual IP address defined to access the available CUCM server to serve the request. When the BizTalk server sends the proxy EM request, the request is sent to the virtual IP address for CUCM.

IP Phone to CUCM/IMATIS Connections

IP phones should always be configured with the virtual IP address for CUCM and the IMATIS servers for an XML request. Using this virtual IP address ensures that the available CUCM or IMATIS server always serves the request from the IP phone. On the IMATIS server, both the Windows clustering and BizTalk group ensure that the application is always available to the phone. For the CUCM server, the XML services redundancy configuration ensures XML services are always available from one of the CUCM servers in the cluster.

IP phone redundancy to CUCM clusters for services other than XML services, such as call signaling, should use the design guidelines as outlined in the CUCM 6.0 SRND.

Hospital Equipment to IMATIS Adapters

Connections between the IMATIS adapters and the hospital equipment, such as nurse call systems, ancillary systems, and building and fire alarm systems, needs to be evaluated. As each hospital's equipment may have unique product capabilities, the analysis should be performed during the integration. For RS-232 interfaces, there are active/passive splitters that allow for a faster switch to the active connection from a server that uses RS-232 connections.

Voice Gateway to Nurse Call System

In order to provide voice access to legacy nurse call and PBX systems, the use of a Voice Gateway may be required. The most common use case as it relates to nurse call is a voice call back to the patient room or ancillary department. In addition, offnet communication can also be accomplished from any of the Cisco Imatis Mobile Care endpoints through the very nature of Unified Communication. To provide this connectivity, the use of an Integrated Services Router with an appropriate voice interface is one possible solution. The other alternatives include various voice-capable line cards available for the Cisco Catalyst 6500 series platform.

As part of the Cisco Imatis Mobile Care validation process, a 3875 ISR was used with FXS ports which provide connectivity to nurse call and PBX-based systems. From a high availability perspective, it is recommended that redundant voice gateways be used within the Cisco Imatis Mobile Care solution. To utilize redundant voice gateways, a route group can be defined that specifies the order in which trunks or voice gateways are utilized for any given route pattern. In the event that a Voice Gateway fails or is no longer reachable, Call Manager automatically removes that gateway from the list of configured gateways and continues routing calls through the surviving configured gateways.

When connecting redundant voice gateways to PBXs, it is recommended that each voice gateway be connected to PBX ports that are contained on separate PBX shelves in order to provide a level of fault tolerance in the event of a failure or scheduled maintenance of the shelf.

Network Services Integration

Active Directory and Cisco Secure ACS

The Cisco Imatis Mobile Care solution interfaces with and uses a number of different network services. Active Directory integration is supported as a means to authenticate wireless users through the use of the Cisco Secure ACS solution. The IMATIS suite of applications also takes advantage of Active Directory to provide user assignment. This greatly simplifies the assignment of roles to users, as once the user is defined to Active Directory, the userid appears within the IMATIS User Manager application.

DNS (Domain Name Services)

Both redundancy and completeness of domain naming information should be included in the overall design of the network. Many hosts depend upon the ability to correctly resolve the host name of a server. In the case of the Cisco Imatis Mobile Care solution, both the 7921G and 7971G phones require that the hostname of the middleware XML-based service host be resolvable. Each time the services key is pressed, for example, the URL configured for that key on the phone is referenced. If the URL contains a hostname-based URL, a DNS query is performed by the phone in order to resolve the supplied name to its corresponding IP address.

If during this time DNS services are inhibited or unavailable for some reason, the overall availability and end user perceived reliability of the solution deteriorates. In order to provide a high level of service availability, redundant DNS servers should be employed and connected to the network using diverse switching fabric. Similar to that of the DHCP servers, each DNS server should be placed on separate maintenance windows to prevent issues arising due to hardware or software updates. Both the 7921G and 7971G do not cache DNS queries which relate to a DNS query for each XML service selected from the phones menu.

DNS for XML High Availability

In order to increase the availability of the XML services as accessed from a Cisco handset, it is recommended that either Server Load Balancing (SLB) be utilized or an appliance-based load balancing solution be implemented, such as the ACE appliance or Content Services Switch (CSS). Alternatively, it is possible to use round robin DNS to provide round robin IP address resolution for each of the configured Call Managers in the Unified Communications cluster. With round robin DNS, each successive DNS request made issues the next IP address for a given hostname in a circular fashion. In the event of a failed Call Manager, or a Call Manager which no longer has access to the network, this IP address is still resolved. While this is a disadvantage to round robin DNS, it does provide the end user with the ability to press the services button, for example, and have a possibility of receiving an IP address for one of the surviving Call Managers in the cluster. Equally, however, it is possible that during the time that user A experienced the address of the failed Call Manager, another user B may have obtained the address for the surviving Call Manager. The next time that user A requests services, they would again receive the failed server IP address until such time that their request results in one of the surviving Call Manager IP address being returned. For this reason, round robin DNS is not recommended for a high availability-based solution for Cisco Imatis Mobile Care over that of SLB or an appliance-based approach. It is included here to discuss its capabilities and limitations on the overall user experience.

Network Time Protocol

While availability is not typically affected by Network Time Protocol (NTP), it can provide valuable assistance in determining the sequence of events that lead to a disruption of service. In addition, having the time synchronized between the phone, middleware vendor servers, network infrastructure, and ancillary systems can become important when tracing the delivery of messages as they traverse the overall solution. Implementing a redundant and hierarchal NTP design can provide valuable information during troubleshooting, hopefully resulting in the reduction of service interruptions.



CHAPTER 6

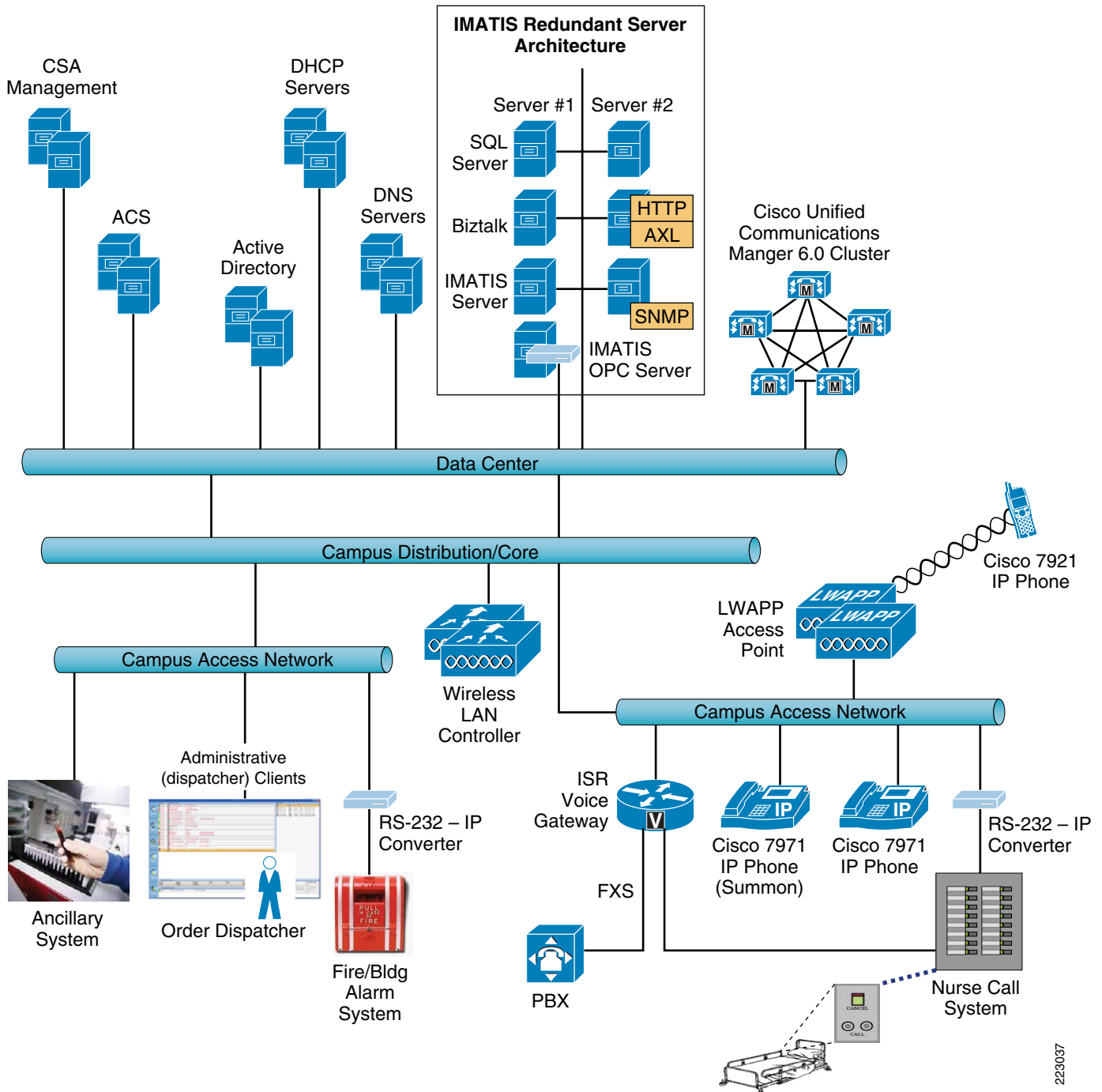
Implementing the Cisco Imatis Mobile Care Solution

This chapter provides implementation details for the services enabled by Cisco Unified Communications, Cisco Unified Wireless Network, and IMATIS for the Mobile Care services. This section describes the steps required to configure features across the components to enable the services. Some design concepts and limitations are provided that you should keep in mind during implementation.

Network Topology

[Figure 6-1](#) provides a frame of reference as you implement the solution. [Figure 6-1](#) should be referred to as you implement the infrastructure steps outlined in [Chapter 5, “Designing the Cisco Imatis Mobile Care Solution”](#) and the application components in this chapter. There are many components in this solution and the placement of these components as it pertains to the places in the network helps to ensure better performance, availability, and security for the solution.

Figure 6-1 Network Topology



223037

Configuration Task List

Configuration of the Cisco Imatis Mobile Care solution is a multi-step process that involves components across the network infrastructure, Cisco Unified Communications, Cisco Unified Wireless, the IMATIS servers, and a range of hospital equipment. The goal of this implementation checklist is to provide a list

of key areas to cover to achieve a successful implementation. The checklist outlines the key steps to enable Cisco Imatis Mobile Care services, in addition to pointers to several foundational design guides that should be leveraged.

1. Unified Communications
 - a. Communications Manager
 - SNMP Configuration
 - Creating System Users
 - Creating XML Services
 - Creating XML URL Speed Dials
 - b. Nurse Call Voice Callback Configuration
2. XML Services Redundant Configuration
3. User Management
 - a. IP Phone Configuration
 - b. Adding Services to the IP Phone
 - c. Creating Extension Mobility Users
 - d. Configuring Speed Dials for Medical Team Assembly
4. Services Configuration
 - a. IMATIS System Configuration
 - b. IMATIS Worklist and INBOX
 - c. IMATIS Mobile Nurse Call
 - d. IMATIS Order Entry Alerts
 - e. Text Messaging
 - f. IMATIS Hospital Orderly
 - g. IMATIS Medical Team Assembly
 - h. IMATIS Mobile Alerts

**Note**

Refer to [Chapter 4, “Cisco Imatis Mobile Care Solution Features and Components”](#) for a list of all the components and software revisions that have been validated.

**Note**

These configuration steps provide detailed configurations for Cisco products. Configuration details for partner products, such as the IMATIS server or the IMATIS Mobile Nurse Call system, are not described in this document. Some general guidance is provided for the IMATIS server, but for detailed configurations refer to the implementation guides from the partners. For customers deploying Cisco Imatis Mobile Care, work with Imatis and system integrators identified by Cisco and Imatis.

Cisco Unified Communications

Communications Manager Configuration

Configuration of the Communications Manager is outlined in this section. The following provides a detailed checklist of key items to configure to enable Cisco Imatis Mobile Care services.

Summary of CUCM Configurations

1. Creating System Users
 - a. Extension Mobility proxy user for EM login via IMATIS server
 - b. Cardiac user to control all the phones associated with the service to send XML services to the phone and interface to the AXL interface from CUCM.
2. SNMP configuration
3. Creating XML services
 - a. IMATIS Login/Logout
 - b. Text Messaging
 - c. IMATIS Medical Team Assembly
 - d. IMATIS Hospital Orderly service
 - e. Main Menu
4. Creating XML Service Speed Dial
 - a. Cardiac Arrest Team
 - b. Emergency Doctor



Note

IMATIS Mobile Nurse Call, IMATIS Order Entry Alert, and IMATIS Mobile Alert services do not require a unique XML service to be defined. Once the user is logged into IMATIS and that phone user is then associated with the service in IMATIS, the user is then able to receive mobile nurse call alerts, order entry alerts, or mobile alerts from building or fire alarm systems.

Creating System Users

Creating users for predefined functions is required for system-level functions. This configuration only needs to be performed during the initial installation. These users provide IMATIS the user permission to perform the following two functions. Configuring individual users for Cisco Imatis Mobile Care services is outlined in [Services Configuration](#).

- Communications Manager User—This user is defined to authorize IMATIS to control the physical phone devices that are used for Cisco Imatis Mobile Care. All phones used for Cisco Imatis Mobile Care should be associated with this user to allow the IMATIS server to post XML messages to these phones.

- Extension Mobility User—This user is defined to authorize IMATIS to login using Extension Mobility for the IMATIS user defined for the Cisco Imatis Mobile Care service. This user is defined in IMATIS and initiates a proxy login for the corresponding EM user in CUCM. By allowing this proxy login, the mobile care user can have a single logon and therefore is not required to login via IMATIS and then again for Extension Mobility in CUCM.

To add a Communications Manager User:

-
- Step 1** Select User Management -> End User.
- Step 2** Select Add New.
- Step 3** End User Configuration.

Figure 6-2 Adding a Communications Manager User

The screenshot shows the Cisco Unified CM Administration interface for End User Configuration. The 'User Information' section is highlighted with a red box. The fields and their values are as follows:

Field	Value
User ID*	cardiac
Password	12345
Confirm Password	12345
PIN	12345
Confirm PIN	12345
Last name*	cardiac
Middle name	
First name	
Telephone Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC	
Digest Credentials	
Confirm Digest Credentials	

A text box to the right of the highlighted fields contains the following information:

```
User ID = cardiac
Password = 12345
PIN = 12345
Last Name = cardiac
```

- Step 4** Enter information in the highlighted fields.



Note These entries should match the IMATIS configuration files BtImatisLogInOutSettings.xml and BtIpPhoneAdapterSettings.xml

- Step 5** Save the configuration.
- Step 6** Select Device Association.

Figure 6-3 Device Association Configuration

The screenshot shows the Cisco Unified CM Administration interface for User Device Association. The page title is "User Device Association" and it shows 7 records found. The table below lists the associated devices:

<input type="checkbox"/>	Device Name	Directory Number	Description
<input checked="" type="checkbox"/>	SEP00179406EB92	1003	SEP00179406EB92
<input checked="" type="checkbox"/>	SEP001AA1928FE9	2003	SEP001AA1928FE9
<input checked="" type="checkbox"/>	SEP001AA192971B	2002	SEP001AA192971B
<input checked="" type="checkbox"/>	SEP001AA192A13B	2004	SEP001AA192A13B
<input checked="" type="checkbox"/>	SEP001AA192A22B	2001	SEP001AA192A22B
<input checked="" type="checkbox"/>	SEP001B2AC681D6	1001	SEP001B2AC681D6
<input checked="" type="checkbox"/>	SEP001B2AC681E6	1002	SEP001B2AC681E6

Step 7 Select the devices that belong to the Cisco Imatis Mobile Care Service.

Step 8 Click the Save Selected/Changes button.



Note Any new phones that are added later that also require the Cisco Imatis Mobile Care service should be added to this user.

To add an Extension Mobility User and AXL interface system user:

Step 1 Select User Management -> Application User.

Step 2 Select Add New.

Figure 6-4 Application User Configuration

The screenshot displays the 'Application User Configuration' page in Cisco Unified CM Administration. The page is divided into several sections:

- Status:** Shows 'Status: Ready'.
- Application User Information:** Contains fields for 'User ID*' (emcardiac), 'Password' (12345), and 'Confirm Password' (12345). A red box highlights these fields, and a callout box states 'User ID = emcardiac Password = 12345'. Other fields include Digest Credentials, Confirm Digest Credentials, Presence Group* (Standard Presence group), and several checkboxes for subscription and notification options.
- Device Information:** Shows a list of 'Available Devices' (SEP00179406EB92, SEP001AA1928FE9, SEP001AA192971B, SEP001AA192A13B, SEP001AA192A22B) and buttons for 'Find more Phones', 'Find more Route Points', and 'Find more Pilot Points'. There is also a 'Controlled Devices' section.
- CAPF Information:** Shows 'Associated CAPF Profiles' with a 'View Details' link.
- Permissions Information:** Shows 'Groups' and 'Roles' sections, each with a 'View Details' link. A red box highlights the 'Add to User Group' button, with a 'Remove from User Group' button below it.

Step 3 Enter information in the highlighted fields.



Note These entries should match the IMATIS configuration file BtImatisLogInOutSettings.xml.

Step 4 Select Add to User Group.

Figure 6-5 Adding User Groups

Find and List User Groups

Select All Clear All Add Selected Close

Status
21 records found

User Group (1 - 21 of 21) Rows per Page 50

Find User Group where Name begins with Find Clear Filter

<input type="checkbox"/>	Name ^	Roles	Copy
<input type="checkbox"/>	Standard CAR Admin Users	i	📄
<input type="checkbox"/>	Standard CCM Admin Users	i	📄
<input type="checkbox"/>	Standard CCM End Users	i	📄
<input type="checkbox"/>	Standard CCM Gateway Administration	i	📄
<input type="checkbox"/>	Standard CCM Phone Administration	i	📄
<input type="checkbox"/>	Standard CCM Read Only	i	📄
<input type="checkbox"/>	Standard CCM Server Maintenance	i	📄
<input type="checkbox"/>	Standard CCM Server Monitoring	i	📄
<input type="checkbox"/>	Standard CCM Super Users	i	📄
<input type="checkbox"/>	Standard CTI Allow Call Monitoring	i	📄
<input type="checkbox"/>	Standard CTI Allow Call Park Monitoring	i	📄
<input type="checkbox"/>	Standard CTI Allow Call Recording	i	📄
<input type="checkbox"/>	Standard CTI Allow Calling Number Modification	i	📄
<input type="checkbox"/>	Standard CTI Allow Control of All Devices	i	📄
<input type="checkbox"/>	Standard CTI Allow Reception of SRTP Key Material	i	📄
<input type="checkbox"/>	Standard CTI Enabled	i	📄
<input type="checkbox"/>	Standard CTI Secure Connection	i	📄
<input checked="" type="checkbox"/>	Standard EM Authentication Proxy Rights	i	📄
<input type="checkbox"/>	Standard Packet Sniffer Users	i	📄
<input type="checkbox"/>	Standard RealtimeAndTraceCollection	i	📄
<input checked="" type="checkbox"/>	Standard TabSync User	i	📄

Select All Clear All Add Selected Close

223/209

- Step 5** Select Standard EM Authentication Proxy Rights and Standard TabSync User, then click Add Selected. Click Save back on the Application User Configuration.
- Step 6** After configuring the user, you should see the screen in Figure 6-6. Two selections provide Extension Mobility Login rights and AXL API interface from the IMATIS servers.

Figure 6-6 Application User Configuration Complete

Application User Information

User ID* [Edit Credential](#)

Password

Confirm Password

Digest Credentials

Confirm Digest Credentials

Presence Group* ▼

Accept Presence Subscription

Accept Out-of-dialog REFER

Accept Unsolicited Notification

Accept Replaces Header

Device Information

Available Devices [Find more Phones](#)

SEP001AA1928FE9 [Find more Route Points](#)

SEP001AA192971B [Find more Pilot Points](#)

SEP001AA192A13B

SEP001AA192A22B

▼ ▲

Controlled Devices

CAPF Information

Associated CAPF Profiles [View Details](#)

Permissions Information

Groups [View Details](#)

Standard EM Authentication Proxy Rights

[Add to User Group](#)

[Remove from User Group](#)

Roles [View Details](#)

Standard EM Authentication Proxy Rights

[Save](#) [Delete](#) [Copy](#) [Add New](#)

2239300

SNMP Configuration

SNMP configurations must be defined so that the IMATIS server receives periodic updates when changes to phone states or configurations occur for the phones used for the Cisco Imatis Mobile Care service.

- Step 1** In the CUCM Navigation pull down menu, select Cisco Unified Serviceability.
- Step 2** Select SNMP -> V1/V2c -> Community String.
- Step 3** Select the publisher server and choose Find.
- Step 4** Select Add New.
- Step 5** SNMP Community String Configuration.

Figure 6-7 SNMP Community String Configuration

The screenshot displays the 'SNMP Community String Configuration' page in the Cisco Unified Serviceability interface. The page is titled 'SNMP Community String Configuration' and includes a navigation bar with 'Cisco Unified Serviceability' and a 'Go' button. Below the navigation bar, there are tabs for 'Alarm', 'Trace', 'Tools', 'Snmp', and 'Help'. The main content area is divided into several sections:

- Status:** Shows 'Status : Ready'.
- Server:** A dropdown menu is set to 'mc-cm-ca1'.
- Community String Information:** A text field labeled 'Community String' contains the value 'IMATIS'.
- Host IP Addresses Information:** Two radio buttons are present: 'Accept SNMP Packets from any host' (selected) and 'Accept SNMP Packets only from these hosts'. Below the second radio button, there is a 'Host IP Address' input field, an 'Insert' button, a 'Host IP Addresses' list area, and a 'Remove' button.
- Access Privileges:** A dropdown menu labeled 'Access Privileges*' is set to 'ReadWriteNotify'.
- Apply To All Nodes:** A checkbox labeled 'Apply To All Nodes' is checked.

At the bottom of the page, there are 'Save', 'Clear All', and 'Cancel' buttons, and a note: '* - indicates required item.' The page number '222989' is visible in the bottom right corner.

- a. Enter IMATIS for community string and check that the IMATIS server is configured with the same field.
- b. Select Accept SNMP Packets from any host.
- c. Select ReadWriteNotify for access privileges.
- d. Select Apply to All Nodes.
- e. Save this configuration.

Step 6 Select SNMP -> V1/V2c -> Notification Destination.

Step 7 Select the publisher server and choose Find.

Step 8 Select Add New.

Step 9 SNMP Notification Destination Configuration.

Figure 6-8 SNMP Notification Destination Configuration

The screenshot shows the Cisco Unified Serviceability web interface for configuring an SNMP Notification Destination. The page title is "SNMP Notification Destination Configuration". The interface includes a navigation bar with "Alarm", "Trace", "Tools", "Snmp", and "Help" menus. The main content area is divided into several sections:

- Status:** Shows "Status : Ready".
- Server:** A dropdown menu is set to "mc-cm-ca1".
- Host IP Address Information:** Contains two input fields: "Host IP Address" with the value "10.1.1.13" and "Port Number" with the value "162".
- SNMP Version Information:** Contains a radio button selection for "SNMP Version" with "v1" selected.
- Community String Information:** Contains a dropdown menu for "Community String" set to "IMATIS" and a "Create New Community String" button.
- Apply To All Nodes:** A checkbox that is checked.
- Buttons for "Save", "Clear", and "Cancel" are at the bottom.
- A note at the bottom left states: "i* - indicates required item."

- Enter the IMATIS Server IP address under Host IP Address.
- Enter 162 under Port Number.
- Select v1 for SNMP version.
- Select IMATIS for the Community String.
- Select Apply to All Nodes.
- Save this configuration.

Check that the IMATIS server filename IMATIS Ccm Integration Service.exe.config is configured accordingly. In this file the IP addresses, Community String, frequency for traps, and other fields are defined for the SNMP interface. The current recommendation is that SNMP traps are pulled from CUCM every 30 seconds. This is the lowest recommended setting. In addition to the periodic pulling of SNMP traps for the changes that have occurred, also configure the system to perform a full SNMP update once a day during a low traffic volume timeframe. The full update clears any conflicts that may occur between the IMATIS server and CUCM database.

Creating XML Services

XML services running on the Cisco IP phone enable the Cisco Imatis Mobile Care services. These services require an initial system level configuration before any of the users and phones can subscribe to these services. This section covers the initial configuration required on the CUCM system.

**Note**

In all of these examples, the service uses a DNS name for the IMATIS server = IMATIS-server. IMATIS-server resolves to the virtual IP address of the IMATIS server cluster. The primary server of the cluster always serves the request.

IMATIS Login/Logout**Figure 6-9** IMATIS Login/Logout

The screenshot displays the Cisco Unified CM Administration interface for configuring an IP Phone Service. The page title is "IP Phone Services Configuration". The navigation menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The current user is "admin".

The configuration form is divided into three main sections:

- Status:** Shows "Status: Ready".
- Service Information:** Contains fields for "Service Name*" (IMATIS Log In-Out), "ASCII Service Name*" (IMATIS Log In-Out), "Service Description" (IMATIS Login and Logout service), and "Service URL*" (http://imatis-server/ImatisIpWebService/ImatisLogInC).
- Service Parameter Information:** Includes a "Parameters" table with "New", "Edit", and "Delete" buttons.

At the bottom, there are buttons for "Save", "Delete", "Update Subscriptions", and "Add New". A note at the bottom left states: "*- indicates required item."

This service on IMATIS provides the user with single sign-on. Through this login on the IMATIS server, a proxy login to extension mobility is created. More details are provided in the User ID Management section.

Under the Service URL:

<http://imatis-server/ImatisIpWebService/ImatisLogInOut/ImatisLogInOut.asp?device=#DEVICENAME#>

Text Messaging

This service definition enables the text messaging service between users of the system.

Figure 6-10 Text Messaging

The screenshot shows the Cisco Unified CM Administration interface for configuring Text Messaging. The page is titled "IP Phone Services Configuration" and includes a navigation menu at the top with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is divided into three sections:

- Status:** Shows "Status: Ready" with an information icon.
- Service Information:** Contains two rows of configuration fields:

Service Name*	ASCII Service Name*
Text Messages	Text Messages
Service Description	Service URL*
IMATIS Service for Text Messaging	http://imatis-server/ImatisIpWebService/ImatisMeldin
- Service Parameter Information:** Features a large empty text area for parameters and three buttons: "New", "Edit", and "Delete".

At the bottom of the page, there are buttons for "Save", "Delete", "Update Subscriptions", and "Add New". A note at the bottom left states: "i *- indicates required item." The page number "22/29/02" is visible in the bottom right corner.

Under the Service URL: <http://imatis-server/ImatisIpWebService/ImatisMelding/ImatisMelding.asp>

IMATIS Medical Team Assembly

This service definition enables the IMATIS Medical Team Assembly service.

Figure 6-11 IMATIS Medical Team Assembly

The screenshot displays the Cisco Unified CM Administration interface for configuring the IMATIS Medical Team Assembly service. The page includes a navigation menu at the top with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled "IP Phone Services Configuration" and contains several sections:

- Status:** Shows "Status: Ready".
- Service Information:** A table with two columns: "Service Name*" and "ASCII Service Name*". The "Service Name*" field contains "IMATIS Medical Team Assembly" and the "ASCII Service Name*" field contains "IMATIS Medical Team Asembly". Below this, the "Service Description" is "IMATIS Medical Team Assembly" and the "Service URL*" is "http://10.1.1.13/ImatisIpWebService/ImatisTilkalling/I".
- Service Parameter Information:** A section with a "Parameters" list box and buttons for "New", "Edit", and "Delete".

At the bottom of the configuration area, there are buttons for "Save", "Delete", "Update Subscriptions", and "Add New". A note at the bottom left states: "*- indicates required item."

Under the Service URL: <http://imatis-server/ImatisIpWebService/ImatisTilkalling/ImatisTilkalling.asp>

IMATIS Hospital Orderly Request

This service definition enables the IMATIS Hospital Orderly Request service.

Figure 6-12 IMATIS Hospital Orderly Request

The screenshot displays the Cisco Unified CM Administration interface for configuring an IP Phone Service. The page title is "IP Phone Services Configuration". The navigation menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is divided into several sections:

- Status:** Shows "Status: Ready".
- Service Information:** A table with two columns: "Service Name*" and "ASCII Service Name*". The "Service Name*" field contains "IMATIS Hospital Orderly" and the "ASCII Service Name*" field also contains "IMATIS Hospital Orderly". Below this, the "Service Description" is "IMATIS Hospital Orderly" and the "Service URL*" is "http://10.1.1.13/ImatisIpWebService/ImatisPortoer/In".
- Service Parameter Information:** A section with a "Parameters" list box and three buttons: "New", "Edit", and "Delete".

At the bottom of the configuration area, there are buttons for "Save", "Delete", "Update Subscriptions", and "Add New". A note at the bottom left states: "i *- indicates required item."

Under the Service URL: <http://imatis-server/ImatisIpWebService/ImatisPortoer/ImatisPortoer.asp>

IMATIS Main Menu

This definition enables the user to access the IMATIS main menu from the XML Services menu.

Figure 6-13 IMATIS Main Menu

The screenshot displays the Cisco Unified CM Administration interface for configuring the IMATIS Main Menu service. The page title is "IP Phone Services Configuration" and the user is logged in as "admin". The navigation menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area shows the following configuration details:

- Status:** Ready
- Service Information:**
 - Service Name*: IMATIS Main Menu
 - ASCII Service Name*: IMATIS Main Menu
 - Service Description: IMATIS Main Menu
 - Service URL*: <http://imatis-server/ImatisIpWebService/ImatisGetMe>
- Service Parameter Information:**
 - Parameters: (Empty list)
 - Buttons: New, Edit, Delete

At the bottom of the configuration area, there are buttons for Save, Delete, Update Subscriptions, and Add New. A note at the bottom left states: "*- indicates required item."

Under the Service URL: <http://imatis-server/ImatisIpWebService/ImatisGetMessageId.asp>

The other services, IMATIS Mobile Nurse Call and IMATIS Mobile Alerts, do not require an XML Service Menu definition. These services send alerts to users that are assigned in the roles definition in the IMATIS interfaces for User Management and the IMATIS Mobile Nurse Call IMATIS portal. More details on this configuration are provided in [Services Configuration](#).

Creating XML Speed Dial Services

IMATIS enables a Medical Team Assembly service which can be more easily accessed by mapping the request into a speed dial key on the phone to send a URL request. In order to create this mapping to the speed dial key, the service must be defined. The following provides an example of defining a sample service. This service is later mapped to a speed dial button on a Cisco IP phone.

Figure 6-14 IP Phone Services Configuration

The screenshot shows the Cisco Unified CM Administration interface for IP Phone Services Configuration. The page includes a navigation menu, a status section, service information fields, and a service parameter information section.

Status
 Status: Ready

Service Information

Service Name*	ASCII Service Name*
Emerg. Doctor	Emerg. Doctor
Service Description	Service URL*
Speed Dial Service for paging the Emergency Doctor	http://imatis-server/ImatisIpWebService/ImatisTilkalli

Service Parameter Information

Parameters

New Edit Delete

Save Delete Update Subscriptions Add New

*- indicates required item.

Under the Service URL enter:

<http://imatis-server/ImatisIpWebService/ImatisTilkalling/ImatisTilkallingSpeedRollePre.asp?Avd=Emergency%20Dept.&Rolle=Emergency%20Doctor>

The syntax for requesting a “role” is based on

<http://imatis-server/ImatisIpWebService/ImatisTilkalling/ImatisTilkallingSpeedRollePre.asp?Avd=/&Rolle=/>

Where the name for the department as defined in the IMATIS system administration portal is the name for the role. For example: = Emergency%20Dept. and = Emergency%20Doctor.

The syntax for request a “team” is based on

<http://imatis-server/ImatisIpWebService/ImatisTilkalling/ImatisTilkallingSpeedTeamPre.asp?Team=/>

And is equal to the name of the team as defined in the IMATIS system administration portal. For example: the name for the cardiac arrest team is Cardiac%20Arrest%20Team.



Note

%20 is used to represent a space in the filename as defined in the IMATIS system administration portal.

IMATIS Mobile Nurse Call Voice Callback Configuration

For the IMATIS Mobile Nurse Call service, a voice callback to the patient room may be needed. The voice callback may route the call to another IP-based phone. In that case, no extra configuration is required. If the callback is to interface to legacy-wired connections, such as FXS or PRI connections, the CUCM requires an H.323 voice gateway and possibly a H.323 gatekeeper if the dial plans become more complex. The example provided here shows a sample configuration using an ISR with Gatekeeper and Gateway functions combined.

For simplicity, the dial plan shown in this example shows extension 1061 and 1062 as the POTS line extensions for the FXS extensions to integrate with the IMATIS Mobile Nurse Call System. The extension of 105x are extensions on the CUCM Cisco IP phones.

Step 1 Configure the GK function.

```
gatekeeper
zone local mc-gk isemcca.local 10.1.1.22
zone local mc-gk-cm isemcca.local
zone prefix mc-gk-cm 105.
zone prefix mc-gk 106.
gw-type-prefix #1* default-technology
no shutdown
```

Step 2 Configure the POTS lines for the voice gateway.

```
dial-peer voice 101 pots
destination-pattern 1061
port 0/3/0
!
dial-peer voice 102 pots
destination-pattern 1062
port 0/3/1
```

Step 3 Configure the VoIP extension on Communications Manager.

```
dial-peer voice 1050 voip
destination-pattern 105.
session target ras
```



Note There may be a requirement to manipulate digits to interwork with the dial plan structures of the Nurse Call System from BEST or a hospital PBX system. Some systems may require some leading digits used as an access code or for two stage dialing. The integration with the BEST call system required a 9 to be pre-pended to the dialed digits as the access code for calling a nurse call bedside station. If leading digits are required, perform the digit manipulation on the gateway. See this link for digit manipulation on a voice gateway
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_chapter09186a008086f2e2.html#wp1067071

Step 4 Configure the H.323 Gateway to register to the H.323 Gatekeeper.

```
interface FastEthernet0?/0
ip address 10.1.1.22 255.255.255.128
duplex auto
speed auto
h323-gateway voip interface
h323-gateway voip id mc-gk ipaddr 10.1.1.22 1719
h323-gateway voip h323-id mc-voip-gw
```

Step 5 In the CUCM interface, under Device -> Gatekeeper, define the following:

Figure 6-15 Gatekeeper Configuration

The screenshot displays the Cisco Unified CM Administration interface for Gatekeeper Configuration. The page title is "Gatekeeper Configuration" and it includes a "Related Links" section with a "Back To Find/List" button. The interface shows a "Status" section with an information icon and the text "Status: Ready". Below this is the "Gatekeeper Information" section, which contains the following fields and values:

Host Name/IP Address*	10.1.1.22
Description	Mobile Care Gatekeeper
Registration Request Time to Live*	60
Registration Retry Timeout*	300

The "Enable Device" checkbox is checked. At the bottom of the form, there are buttons for "Save", "Delete", "Reset", and "Add New". A note at the bottom left states: "i *- indicates required item."

Step 6 In the CUCM interface, under Device -> Trunk, define the following:

Figure 6-16 Trunk Configuration 1

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

admin | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Trunk Configuration Related Links: Back To Find/List Go

Save Delete Reset Add New

Status
Status: Ready

Device Information

Product:	H.225 Trunk (Gatekeeper Controlled)
Device Protocol:	H.225
Device Name*	mc-cm-voip-gw
Description	
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	OnNet
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
Packet Capture Mode*	None
Packet Capture Duration	0

Media Termination Point Required
 Retry Video Call as Audio
 Wait for Far End H.245 Terminal Capability Set

2220908

Figure 6-17 Trunk Configuration 2

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration GO

admin | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Trunk Configuration Related Links: Back To Find/List GO

Save Delete Reset Add New

Calling Party IE Number Type Unknown* Cisco CallManager ▾
 Called Numbering Plan* Cisco CallManager ▾
 Calling Numbering Plan* Cisco CallManager ▾
 Caller ID DN
 Display IE Delivery
 Redirecting Number IE Delivery - Outbound
 Enable Outbound FastStart
 Codec For Outbound FastStart G711 u-law 64K ▾

Gatekeeper Information

Gatekeeper Name* 10.1.1.22 ▾
 Terminal Type* Gateway ▾
 Technology Prefix #1*
 Zone mc-gk-cm

Save Delete Reset Add New

i *- indicates required item.
i **- Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

Step 7 In the CUCM interface, under Call Routing -> Route/Hunt -> Route Pattern, define the extension range for the FXS ports.

Figure 6-18 Route Pattern Configuration

Route Pattern Configuration

Save Delete Copy Add New

Status
Status: Ready

Pattern Definition

Route Pattern* 106X

Route Partition < None >

Description FXS Analog phones on H.323 GW

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Gateway/Route List* mc-cm-voip-gw (Edit)

Route Option
 Route this pattern
 Block this pattern No Error

Call Classification* OnNet

Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority

Require Forced Authorization Code

Authorization Level* 0

Require Client Matter Code

Step 8 On the gatekeeper, type **show gatekeeper endpoints** to ensure both the gateway and CUCM have registered. Calls route after both devices are registered.



Note

Some legacy voice systems have unique timers for analog interfaces or digital interfaces. Ensure these configurations match the legacy system. See [Chapter 5, “Designing the Cisco Imatis Mobile Care Solution”](#) for specifics on disconnect supervision which may cause fxs lines not to release properly.

XML Services Redundancy on CUCM

The XML services or extension mobility defined for a phone typically is configured with a specific Communications Manager IP address. This presents a single point of failure for the service. As a best practice implement a highly-available XML service by using one of the following three methods:

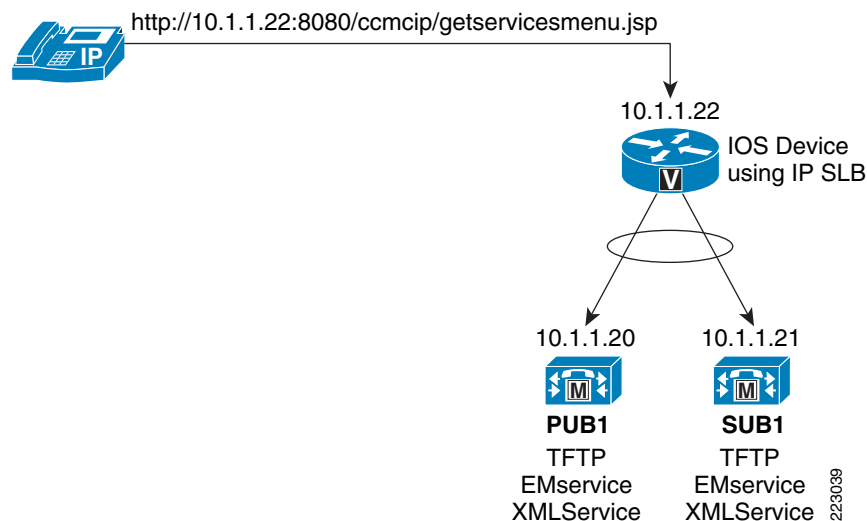
- First method (**recommended**)—Use Server Load Balancing (SLB) on an IOS router. The services button is configured with a virtual IP address or hostname that resolves to that virtual IP address. This virtual IP address is configured on the IOS-based router to perform SLB across a list of configured CM servers. When a particular server fails, a probe defined to detect if the server is alive informs the SLB algorithm to remove that server from the available pool of servers. When the probe

detects that the server is available again, the recovered server is added back to the available pool of servers. Not all platforms support IOS SLB. Before implementing this feature, ensure your platform supports this feature by searching the Cisco feature navigator on CCO.

- Second method (**recommended**)—Use a Content Switch such as CSS 115xx series or ACE module to also perform load balancing.
- Third method—Round Robin DNS is a simple method for redundancy, but this method results in a percentage of failed service request until the failed CUCM server is restored. The failure rate percentage is based on the number of servers that are part of the DNS pool. When the failed server is selected as part of the round robin, the XML request still fails. But when the server that is alive is returned, the service is successful. The usage of round robin DNS is a short term resolution; the first or second method represent long term solutions.

A sample configuration for the first method is described below. Figure 6-19 shows a view of the redundancy configuration.

Figure 6-19 Redundancy Configuration



Step 1 Define a virtual IP address 10.2.2.22. In this example IP address 10.2.2.22 is the virtual IP address for CUCM and IP address 10.2.2.20 and 10.2.2.21 are the physical CUCM server address. 10.2.2.20 and 10.2.2.21 serve the XML services for the IP phones and the IMATIS server. The DNS server should resolve the CUCM address to this virtual IP address when accessing the CUCM server from the Cisco IP phone or from the IMATIS server. This implementation ensures that all queries to CUCM for XML services resolve once the defined probe has detected that a server is unreachable and removes it from the available set of CUCM servers.

Step 2 On the switch before the server farm, implement the following:

```
! probe to check for the availability of the server
ip slb probe MY-PROBE tcp
  address 10.2.2.22
  port 8080

! define a equally balanced access to CUCM servers
ip slb serverfarm MOBILECARE1-0
  nat server
  probe MY-PROBE
!
```

```

real 10.2.2.20
weight 1
inservice
!
real 10.2.2.21
weight 1
inservice
! define the virtual server
ip slb vserver MOBILECARE
virtual 10.2.2.22 tcp 8080
serverfarm MOBILECARE1-0
inservice

```

- Step 3** Under the CUCM interface, the setting under System -> Enterprise Parameters should have the following set with the virtual IP address or DNS name for all the Phone URL Parameters:

Figure 6-20 Enterprise Parameters Configuration

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes "Cisco Unified CM Administration" and "For Cisco Unified Communications Solutions". The user is logged in as "admin". The main menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The "Enterprise Parameters Configuration" page is displayed, showing a list of Phone URL Parameters:

Parameter	Value
URL Authentication	http://10.1.1.22:8080/ccmcip/authenticate.jsp
URL Directories	http://10.1.1.22:8080/ccmcip/xmldirectory.jsp
URL Idle	
URL Idle Time	0
URL Information	http://10.1.1.22:8080/ccmcip/GetTelecasterHelpText.jsp
URL Messages	
IP Phone Proxy Address	
URL Services	http://10.1.1.22:8080/ccmcip/getservicesmenu.jsp

User Management

This section describes the configuration of individual Cisco Imatis Mobile Care users. Use the following checklist to create the individual users.

Summary of key items:

- [IP Phone Configuration](#)
- [Adding Services to the Phone](#)
- [Creating Extension Mobility Users](#)
- [Configuring Speed Dial Button for IMATIS Medical Team Assembly](#)

IP Phone Configuration

The two Cisco IP phones that are tested and supported with Cisco Imatis Mobile Care are the 7921 and 7971G phones. The 7921 is only supported in SCCP mode and the 7971 is supported with SCCP and SIP mode.

To create a phone usable with Cisco Imatis Mobile Care Services:

-
- Step 1** Create a new instance of a 7921 or 7971 phone, under Device -> Phone.
 - Step 2** Define the mandatory and optional settings.
 - Step 3** Under External Data Locations Information -> Idle, enter <http://imatis-server/ImatisIpWebService/ImatisGetMessageid.asp>.
 - Step 4** Under External Data Locations Information -> Idle Timer, enter 4.
 - Step 5** Click the field Enable Extension Mobility.

A sample of what you should enter is shown in [Figure 6-21](#).

Figure 6-21 Sample IP Phone Configuration

The screenshot displays the Cisco Unified CM Administration web interface. At the top, the navigation bar includes 'Cisco Unified CM Administration' and 'Go'. Below this, a menu bar lists various system functions like 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main content area is titled 'Phone Configuration' and includes a 'Related Links' section with a 'Back To Find/List' button. A toolbar at the top of the configuration area contains icons for 'Save', 'Delete', 'Copy', 'Reset', and 'Add New'. The configuration form is divided into two main sections: 'External Data Locations Information (Leave blank to use default)' and 'Extension Information'. The first section contains input fields for 'Information', 'Directory', 'Messages', 'Services', 'Authentication Server', 'Proxy Server', 'Idle' (containing the URL 'http://imatis-server/ImatisIpWebService/ImatisGetMe'), and 'Idle Timer (seconds)' (containing the value '4'). The second section, 'Extension Information', features a checked checkbox for 'Enable Extension Mobility', a dropdown menu for 'Log Out Profile' (set to '-- Use Current Device Settings --'), and two fields for 'Log in Time' and 'Log out Time', both set to '< None >'. A vertical scrollbar is visible on the right side of the form area.

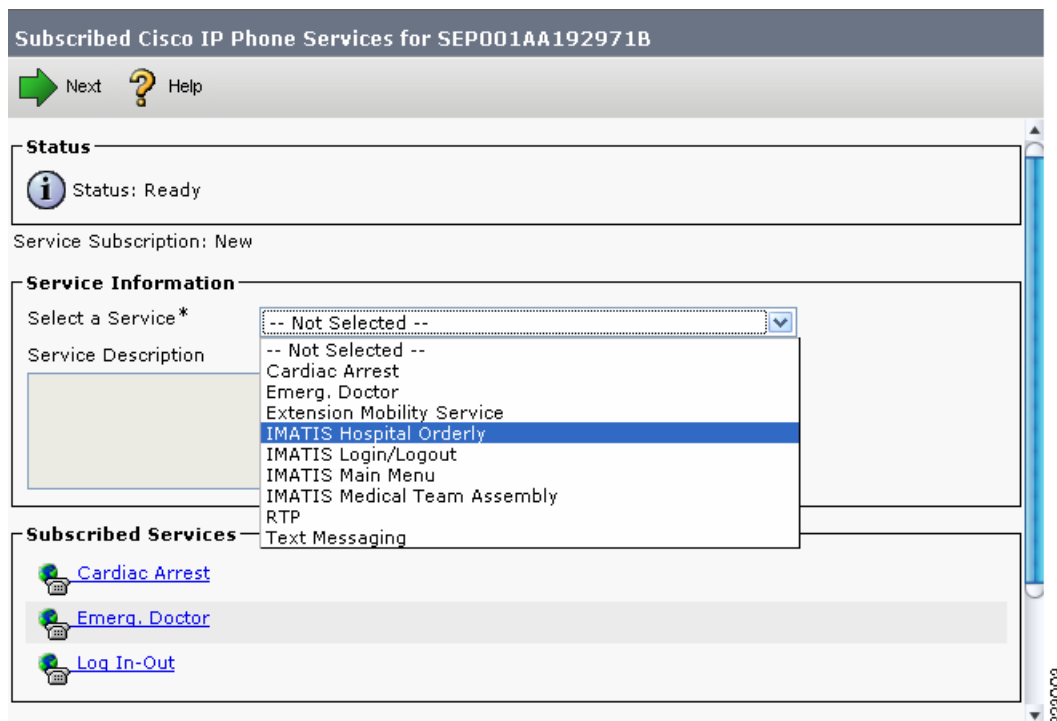
- Step 6** Save the configuration.
 - Step 7** Under User Management -> End User, select the user “cardiac” or the user as defined under the section “Communications Manager User”.
 - Step 8** Select the button Device Association and click Find. Select the Device Name for the phone that has just been defined to add it to the list of devices to which IMATIS may send XML services.
-

Adding Services to the Phone

Now that the phone has been defined, services can be added to the Cisco IP phone. Follow these instructions if extension mobility is not used for the phone. If extension mobility is used, then only IMATIS Login/Logout should be defined on the IP phone. If Extension Mobility is not used, then add all the relevant services including the IMATIS Login/Logout service.

- Step 1** Select under Device -> Phone the device name that requires the services to be added.
- Step 2** On the top right under the pulldown menu called “Related Links”, select “Subscribe/Unsubscribe Services” and click the “Go” button.
- Step 3** Select the service you wish to add and select next.

Figure 6-22 IP Phone Services Information



- Step 4** When the following menu appears, select “Subscribe”. The window updates with the new service shown in the Subscribed Services.

Figure 6-23 Subscribed IP Phone Services

Subscribed Cisco IP Phone Services for SEP001AA192971B

Save Help

Status

Status: Ready

Service Subscription: IMATIS Main Menu

Service Information

Service Name	IMATIS Main Menu
Service Name*	<input type="text" value="IMATIS Main Menu"/>
ASCII Service Name*	<input type="text" value="IMATIS Main Menu"/>

Subscribed Services

- [Cardiac Arrest](#)
- [Emerg. Doctor](#)
- [Log In-Out](#)

Subscribe Back

*- indicates required item.

223004

Repeat this step for all the services you want on the main phone. If Extension Mobility is used, the majority of the services should be reserved for the device profile associated with the EM User.

Creating Extension Mobility Users

The process of creating an extension mobility user is similar to that of creating a phone. You are creating a pointer to a device profile that is then applied to a physical phone after the extension mobility user has logged into a physical phone. To create an extension mobility user:

- Step 1** Under Device -> Device Settings -> Device Profile, add a new device profile.
- Step 2** Enter the mandatory fields, using [Figure 6-24](#) as an example.

Figure 6-24 Device Profile Configuration

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go

admin | About | Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Device Profile Configuration Related Links: Back To Find/List Go

Save Delete Copy Add New

Status
Status: Ready

Association Info
Modify Button Items

1	Line [1] - 1051 (no partition)
2	Line [2] - Add a new DN
3	Add a new SD
4	Add a new SD
5	Add a new SD
6	Add a new SD
----- Unassigned Associated Items -----	
7	Add a new SD
8	Add a new SURL
9	Privacy
10	None

User Device Profile Information

Product Type: Cisco 7921
 Device Protocol: SCCP
 Device Profile Name*: 1051
 Description: Extension Mobility for 7921 - ext 1051
 User Hold MOH Audio Source: < None >
 User Locale: English, United States
 Phone Button Template*: Standard 7921 SCCP
 Softkey Template: Standard User
 Privacy*: Default
 Ignore Presentation Indicators (internal calls only)

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain: < None >
 MLPP Indication*: Default
 MLPP Preemption*: Default

Logged Out (Default) Profile Information

Login User Id: < None >

Save Delete Copy Add New

*- indicates required item.

The Device Profile Name is used in the next step.

- Step 3** Under User Management -> End User, add a new user used for the extension mobility user. Use Figure 6-25 as an example.

Figure 6-25 End User Configuration

The screenshot displays the 'End User Configuration' interface in Cisco Unified CM Administration. The page title is 'Cisco Unified CM Administration For Cisco Unified Communications Solutions'. The navigation menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The current page is 'End User Configuration', with a 'Related Links' section containing 'Back to Find List Users'. The interface is divided into three main sections: 'User Information', 'Device Associations', and 'Extension Mobility'. The 'User Information' section contains fields for User ID*, Password, Confirm Password, PIN, Confirm PIN, Last name*, Middle name, First name, Telephone Number, Mail ID, Manager User ID, Department, User Locale (set to '< None >'), Associated PC, Digest Credentials, and Confirm Digest Credentials. The 'Device Associations' section has a 'Controlled Devices' list and a 'Device Association' button. The 'Extension Mobility' section includes 'Available Profiles' (1052, 1053, 1054, 1061 for 7970 sccp, 1062 for 7970 SCCP), 'Controlled Profiles' (1051), 'Default Profile' (set to '-- Not Selected --'), 'Presence Group*' (set to 'Standard Presence group'), 'SUBSCRIBE Calling Search Space' (set to '< None >'), and a checked checkbox for 'Allow Control of Device from CTI'. A red box highlights the 'User Information' fields and the 'Extension Mobility' section. A summary box on the right states 'User ID = 1051, Password = 1051, PIN = 1051'. The page number '229006' is visible in the bottom right corner.

Step 4 In the fields for User ID, Password, and PIN, it is highly recommended that the same field is entered for ease of use.



Note The extension mobility user is mapped to the IMATIS user described in [Services Configuration](#).

- Step 5** Under Available Profiles, select the device profile name defined in Step 2. Use the down arrow and move that field into the Controlled Profiles.
- Step 6** Select the option Allow Control of Device from CTI.
This user is now available for use within IMATIS for user login.
-

Configuring Speed Dial Button for IMATIS Medical Team Assembly

The service for IMATIS Medical Team Assembly may benefit from having speed dials provisioned on phones. This speed dial allows a function such as IMATIS Medical Team Assembly to summon a nurse or emergency doctor by the press of a speed dial button. To achieve this, the setting should be defined for both the main IP phone and the extension mobility user. To configure speed dial buttons for this service:

-
- Step 1** Define a new template under Device -> Device Settings -> Phone Button Template.
- Step 2** Configure the options using the following as an example for the 7921 phone.

Figure 6-26 Phone Button Template Configuration

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

admin | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Phone Button Template Configuration Related Links:

Status
Status: Ready 223007

Phone Button Template Information
Button Template Name *

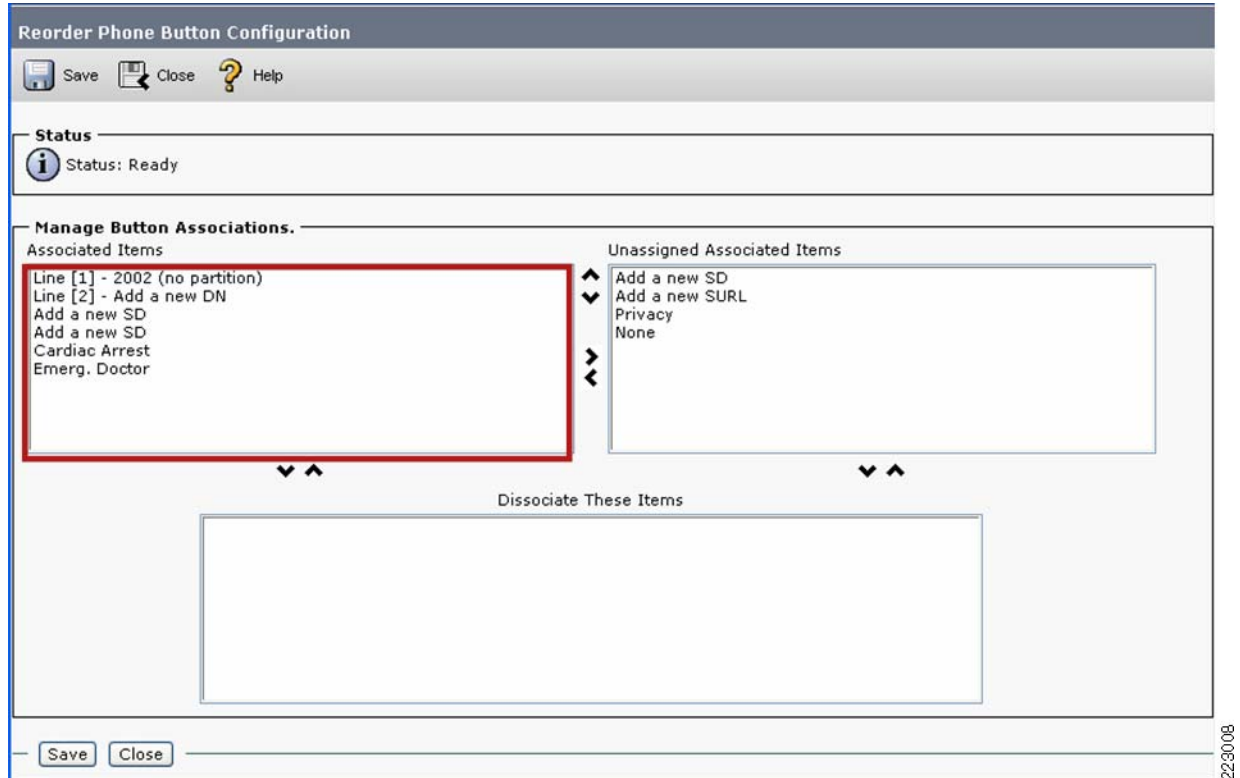
Button Information

Button	Feature	Label
1	Line **	<input type="text" value="Line"/>
2	<input type="text" value="Line"/>	<input type="text" value="Line"/>
3	<input type="text" value="Speed Dial"/>	<input type="text" value="Speed Dial"/>
4	<input type="text" value="Speed Dial"/>	<input type="text" value="Speed Dial"/>
5	<input type="text" value="Service URL"/>	<input type="text" value="Service URL"/>
6	<input type="text" value="Service URL"/>	<input type="text" value="Service URL"/>

i *- indicates required item.

- Step 3** Under the Device -> Phone configuration for a device, subscribe to the XML service that has been defined in [Creating XML Speed Dial Services](#).
- Step 4** Under the Device -> Phone configuration for a device, select the template defined in Step 2 under the option Phone Button Template and save.
- Step 5** Select Modify Button Items and move the speed dial buttons from Unassigned Associated Items to Associated Items. Then move the button into the desired position on the phone.

Figure 6-27 Reorder Phone Button Configuration



- Step 6** (Optional if using extension mobility) Under Device -> Device Setting -> Device Profile, select the device profile and apply the template created in Step 2 to the Phone Button Template option and save.
- Step 7** Select Modify Button Items and move the speed dial buttons from Unassigned Associated Items to Associated Items. Then move the button into the desired position on the phone.



Note On a Cisco IP phone, the Speed Dial URL will be covered by the IMATIS main screen. On a 7971, use the 7914 extension module and define the speed dial keys on the extension module.

Services Configuration

This section describes the configuration required to enable the Cisco Imatis Mobile Care Services. Detailed IMATIS configurations can be obtained through IMATIS. This section covers general areas around IMATIS configurations to enable the IMATIS Mobile Care services with Cisco.

Summary of Cisco Imatis Mobile Care configurations:

- [IMATIS System Configuration](#)
- [IMATIS Worklist and INBOX](#)
- [IMATIS Mobile Nurse Call](#)
- [IMATIS Order Entry Alerts](#)

- [Text Messaging](#)
- [IMATIS Hospital Orderly Request](#)
- [IMATIS Medical Team Assembly](#)
- [IMATIS Mobile Alerts](#)

IMATIS System Configuration

IMATIS recommends that each server be configured with redundancy where each server performs these main functions:

- MT Server 1: IMATIS Server—System and interface server including Web server and system internal interface to catalogue service and Cisco CallManager
- MT Server 2: Microsoft BizTalk Server—Messaging Server with messaging logic
- MT Server 3: Microsoft SQL Server—Database server

For instructions on installing IMATIS, check with Imatis. The IMATIS system utilizes Internet Information Services, ASP.NET, COM+ Access, and DTC Access services from Microsoft Windows Server.

After installing the servers in a redundant fashion, a few steps should be performed.

- AD integration—Create the IMATIS users for the various Cisco Imatis Mobile Care services by integration with active directory. This section does not cover the details of the steps for active directory integration, as those details are provided by Imatis and system integrators identified by Cisco and Imatis. Once this integration is performed, the users are managed through active directory. Inside the IMATIS server for AD users, you see the users as shown in [Figure 6-28](#).

Figure 6-28 IMATIS Users

UPN	First_Name	Given_Name	Title	Department	E-Mail_Address	Internal_Phone_Nu.	Cell_Phone_Numbe	Home_Phone_Num	Pager_Number
User1051	User	1051	<NULL>	<NULL>	<NULL>	1051	<NULL>	<NULL>	<NULL>
user1052	User	1052	<NULL>	<NULL>	<NULL>	1052	<NULL>	<NULL>	<NULL>
user1053	User	1053	<NULL>	<NULL>	<NULL>	1053	<NULL>	<NULL>	<NULL>
user1054	User	1054	<NULL>	<NULL>	<NULL>	1054	<NULL>	<NULL>	<NULL>
User1061	User	1061	<NULL>	<NULL>	<NULL>	1061	<NULL>	<NULL>	<NULL>
user1062	User	1062	<NULL>	<NULL>	<NULL>	1062	<NULL>	<NULL>	<NULL>
user1063	User	1063	<NULL>	<NULL>	<NULL>	1063	<NULL>	<NULL>	<NULL>

Once these users are present in the IMATIS database, these users are ready to utilize Cisco Imatis Mobile Care services.

- IMATIS server configuration with CUCM addresses—There are several integration files that require updates within the IMATIS directory structure to be configured with CUCM addresses. These files require manual updating. A complete set of these integration files are provided by Imatis during the integration.



Note

Any configuration on IMATIS that uses the XML services should be defined with the DNS server name for the CUCM server as defined in [XML Services Redundancy on CUCM](#).

- For other installation and configuration steps, refer to the IMATIS guides. There are additional installation and configuration required for each Cisco Imatis Mobile Care service. Some applications, such as nurse call, have dependencies which use software applications from National Instruments. Other applications, such as IMATIS Medical Team Assembly and IMATIS Hospital Orderly, require software applications from IMATIS to be installed on user PCs. Ensure that these individual services are installed and functioning properly before proceeding.

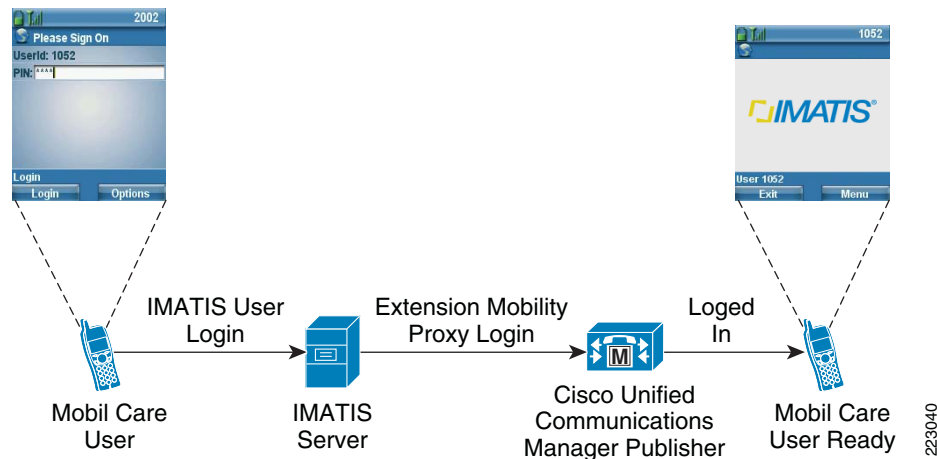
Inside the directory structure of the IMATIS system there are names that are translated as follows:

- pa = nurse call
- tilkalling = team assembly
- oppdrag = orderly
- meldings = messaging
- portoer = porter (summon service)

User ID Management

There are Extension Mobility users created in CUCM that provide the user a specific directory number and there is also an IMATIS user created through the active directory integration. These users should be identical to enable the proxy login from the IMATIS login. [Figure 6-29](#) shows the flow of operations during a user login. With this implementation, the user only needs to log in through the IMATIS login to be automatically logged into to CUCM extension mobility.

Figure 6-29 User ID Management



Note

A best practice is to use the same userID and password in both places.

IMATIS Portal for System Administrator

On the IMATIS server, the system administrator is provided with a portal for administration of several key parameters that are required for each Cisco Imatis Mobile Care service. This application can be found on the IMATIS server through the path `C:\Program Files\CARDIAC\IMATIS\Portal\IMATIS Portal.exe`. Initial configurations for users, floor plans, team groups, and many other areas are configured by the system administrator through this tool.

IMATIS Worklist and INBOX

The services appear on the Cisco IP phones as messages and alerts that are organized into worklist and inbox. A worklist stores messages from IMATIS Mobile Nurse Call, Order Entry Alerts, Mobile Alerts, Hospital Orderly, and Medical Team Alerts. Text messages are stored in the INBOX retrieved by accessing the text messaging service.

Orderly worklists are unique as they serve a different role in a hospital and would not typically receive the other services.

The worklist is also ordered by priority, so Medical Team Assembly is always on top of the list, followed by Urgent nurse call and Normal nurse call. If the messages have the same priority, the messages are ordered by timestamp, with the oldest on top.

The alerts in the worklist are also clearly marked with certain tags to indicate the type of message. A normal nurse call has text such as “Bed 201 07:30” to indicate the location is the bedside or “WC 201 7:30” to indicate the location is the bathroom. An urgent call would be “URGENT 201 07:30”. Messages from Medical Team Assembly also differ regarding the text using, for example, “**Alarm**, 201” or “*Cardiac Arrest*, 201”.

IMATIS Mobile Nurse Call

This section describes several key steps required for integration with nurse call system vendors and a few configuration steps required to set up nurse call alerts to be received by nurses.

IMATIS Mobile Nurse Call Integration

The nurse call system manufactured by Best uses an RS-232 interface to report alerts generated by nurse call stations in a patient room. The RS-232 interface physically connects to an OPC server built by Imatis. Typically the physical location of the nurse call server may not be the same as the OPC server. The recommended implementation is to use RS-232 to IP adapters support the flow of messages from the nurse call system to the IMATIS server via the IP network. For best practices on implementing the RS-232 to IP adapter, refer to [Quality of Service in Chapter 5, “Designing the Cisco Imatis Mobile Care Solution.”](#)

Using an adapter built by Imatis, these alerts are then passed from the OPC server to the IMATIS server via XML. The alert is then routed to the assigned nurse for the room that the alert originated from based on the business rules implemented by IMATIS. The alerts are sent to IMATIS in the form of OPC messages. OPC specifications can be found at

http://www.opcfoundation.org/Default.aspx/01_about/01_whatIs.asp?MID=AboutOPC.

For other nurse call system integrations, contact Imatis for more information.

IMATIS Floor Plan and Bedroom Assignment

The integration with nurse call systems requires a floor plan layout with room assignments for patients. National Instruments is integrated with IMATIS to create the floor plan design for each hospital setting. This design should be performed in conjunction with building facilities. After this layout has been created, a floorplan will be available in the IMATIS portal. To start the IMATIS portal, use the following http query; enter the proper actual address for the IMATIS server:

<http://imatis-server/imatispa>

Click on the Bed Area and select a bed area to view. [Figure 6-30](#) provides a sample floorplan layout for a hospital setting.

Figure 6-30 Sample Floorplan Layout

Signal overview Demo Center, 1.floor, Demo Bed Area 1

Bed Area 1

Bed Area 2

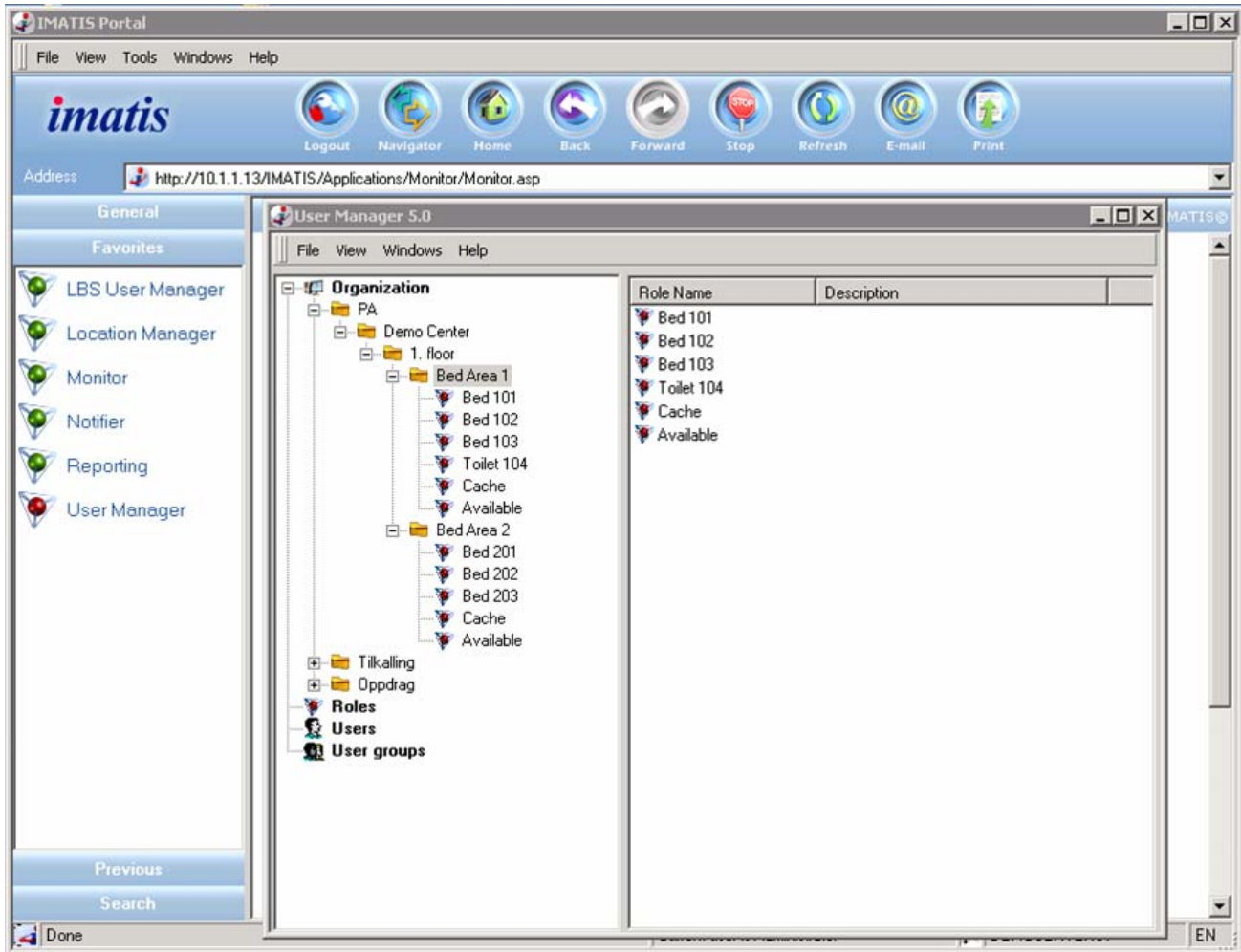
Bed Area 3

Location	Receiver	Message type	Response	Time
BED 101	Disp	Sent		18.04.2006 15:45:28
BED 101	Room 103	Sent		18.04.2006 15:45:28
BED 101	Room 102	Reset		18.04.2006 15:45:25
BED 101	WC 104	Reset		18.04.2006 15:45:25
BED 101	Room 102	Sent		18.04.2006 15:44:46

IMATIS Portal—System Administrator

After the floor plan and room layouts have been assigned, the floors and rooms need to be added. The administrator should select “User Manager”. Under the directory tree of PA, floors and beds per floor can be defined.

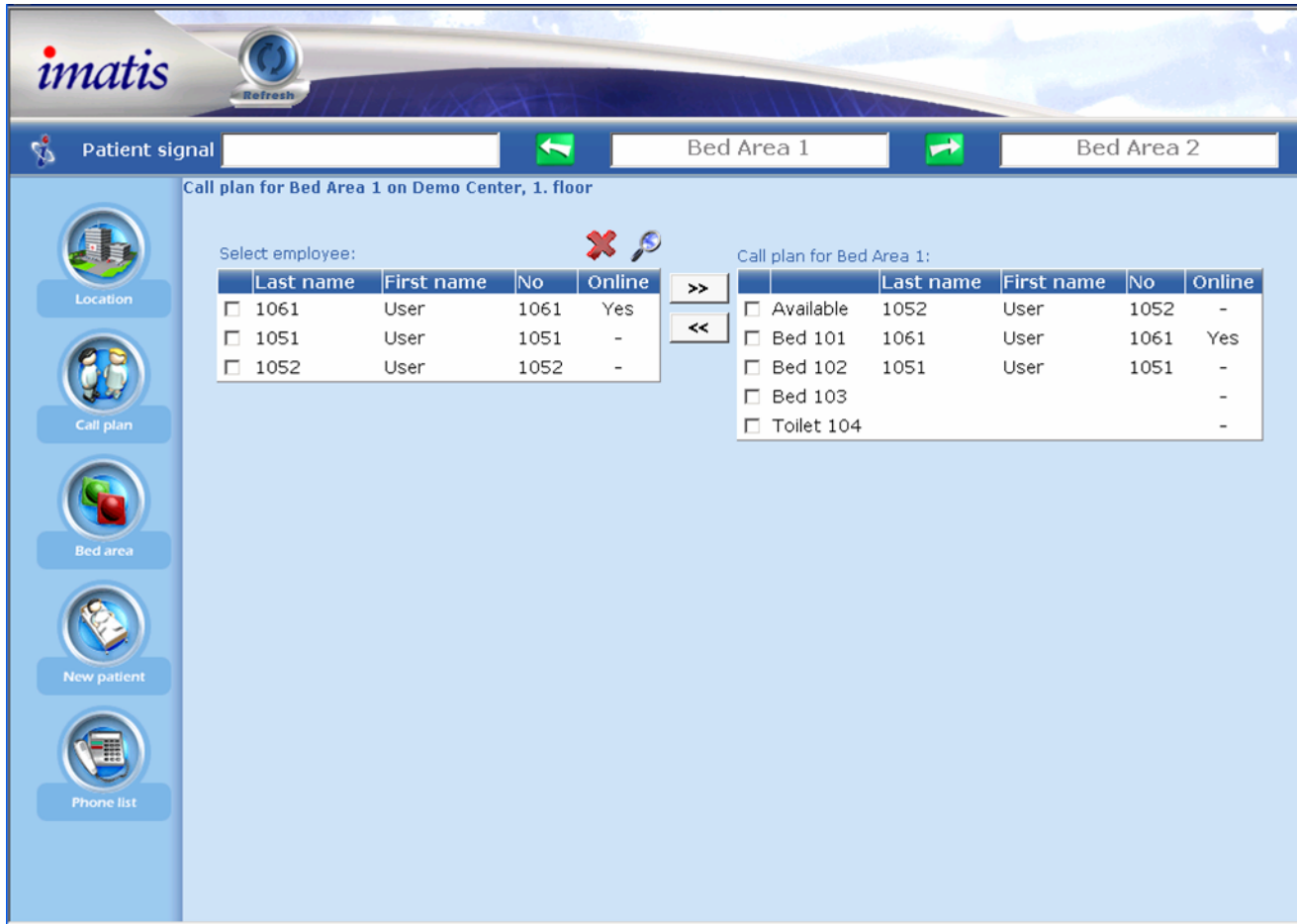
Figure 6-31 Floors and Beds Per Floor



IMATIS Portal for User Assignment—User

Once the users have been added through the active directory integration, the defined users automatically appear within the IMATIS user portal. This portal is the one seen by the users of the system, not the portal used by the system administrator. Figure 6-32 shows the IMATIS portal used to manage the nurse call user assignment to patient rooms.

Figure 6-32 IMATIS Portal for Assignment to Patient Rooms



Click on “Call Plan”. On the left is a list of the employees that can be assigned to the nurse call service. On the right side is a list bedrooms on a particular floor. This floorplan has been created in the previous step. To assign a nurse to a bedroom, click on a user from the list on the left that is shown to be online and click on an area on the right side. Click the set of double arrows pointing to the right and this assignment is created. Once the assignment is created, the location has a user shown after the list, as in example Bed 101 and 102. For areas that are not assigned a nurse, Bed 103 shows an example. Once a patient is assigned to Bed 103, a nurse should be assigned to that location.

Alarm Types

Once the nurses are assigned to the bed locations, the system is ready for use. When an alarm is generated from a patient room via the nurse call bedside stations, the alert is sent to the nurse station as the primary alert system. As a secondary alert, the IMATIS Mobile Nurse Call Server sends the alert to the IMATIS server, which forwards the alert to the Cisco IP phone based on the defined business rules. The following example is a walk through with sample screen shots of a few possible paths through a nurse call workflow.

1. A button press from a nurse call bedside station is sent to a Cisco 7921 phone.

Figure 6-33 Nurse Call Sent to Phone

2. The nurse now has the option to acknowledge the request by selecting OK or dismissing the request if the nurse is busy. If the nurse decides to dismiss the alert, there must be another nurse defined in the escalation rules to accept the request. If there is no other nurse, then the alert returns to the nurse. A reminder alert may also be sent if the nurse does not enter the patient room and press the nurse call button to indicate the alert has been serviced. These reminder alerts are represented by a “(#)” where # represents the number of times the reminder has been sent. This reminder timer is defined on the IMATIS server. The business rules define it as mandatory that after a nurse call alert is sent to the nurses phone, the nurse must press the nurse call button in the patient room to complete the acknowledgment of the alert.
3. Once the alert has been received and the OK button is pressed, the nurse has the option to callback via a voice connection into the room. The voice callback could be to a Cisco IP phone in the patient room or a callback to the bedside terminal via a FXS connection into the room.

Figure 6-34 Option to Callback

4. The location of the alert may also be indicated in the alert. This information must come from the nurse call system, then IMATIS uses these the business rules to send a different type of alert to the phone. [Figure 6-35](#) shows an alert received by the nurse from an alert that came from the restroom area of room 201. This extra information may alert the nurse of the urgency of the alert.

Figure 6-35 Alert Received by Nurse From Restroom Area

- As the nurse receives alerts, the workflow process requires that the nurse enter the patient room and press the bedside terminal to acknowledge the alert. In order for the nurse to clear the alert from their worklist, the nurse must press the nurse call bedside terminal button once again to clear the task from their worklist. This is the only method to clear the alert and signifies the completion of the work related to a nurse call alert. [Figure 6-36](#) shows what is seen by the nurse when there are items on their worklist that have not been fully completed. Once the completion of work occurs, the item is automatically removed from the worklist.

Figure 6-36 Nurse View of Outstanding Worklist Items

- On the IMATIS Portal, the nurse station can see a view of the floor and receive dynamic updates on alerts seen on that floor. [Figure 6-37](#) shows some of the icons that the nurse sees on this portal. In addition, the nurse also sees a historical log of events that have been received for that floor.

Figure 6-37 *Icons on Portal***7. Escalation rules.**

When nurse call alerts go unattended, the business rules in IMATIS force escalations, with escalation rules following the building structure as defined in the IMATIS portal for system administration. Messages that get escalated from a nurse in a particular bed area would escalate to other nurses assigned to that bed area. Once all the nurses in that bed area are exhausted, the next escalation would find other nurses on the same floor. This method of escalation ensures that no nurse call alerts go unattended due to unforeseen circumstances.

8. Urgent alerts.

Urgent alerts may also be generated by the IMATIS Mobile Nurse Call system. A patient would not initiate this urgent request. Instead, this urgent request may be created by the nurse that walks into the patient room. There are several methods that a nurse can use to originate an urgent request:

- Medical Team Alert from a XML Phone service
- Medical Team Alert mapped to a URL speed dial button
- Nurse call button press unique to the nurse user. This operation is dependent on the IMATIS Mobile Nurse Call System and requires the IMATIS Mobile Nurse Call System to send a message over the OPC protocol to the IMATIS OPC Adapter, which would then map to an urgent alert.

When the urgent request is sent, the business rule creates an alert for all nurses attending that bed area. Other users can also be added to this team.

IMATIS Order Entry Alerts

Ancillary System Integration

The integration with ancillary systems for order entry alerts that lab results are available requires HL7 integration. This HL7 adapter is performed through the BizTalk server. The HL7 alert is received from hospital information systems. Based on the business rules applied to the parameters received through the HL7 interface, the message is then sent to the appropriate user. One critical business rule is based on the confidentiality of patient information. If this flag allows patient information to be sent, then the test results and patient name may be passed onto the alert. Otherwise, the alert only indicates that results are ready for review. Another parameter determines if the lab results are urgent or normal priority. There may be other fields that are deemed important as part of the integration that IMATIS may apply to the business rules.

User Assignment

The ordering system for the laboratory request contains an ordering physician's name. The physician's name is a required field to pass across the HL7 interface into IMATIS, along with the laboratory results message. The name is looked up in Active Directory to match a userID that is used as the unique identifier for IMATIS to determine to whom to send the laboratory results message.

Figure 6-38 shows a few samples of normal/urgent alerts and patient/no patient data.

Figure 6-38 Samples of Alerts and Patient Data



Text Messaging

The implementation of text messaging is automatically available once users are defined through the active directory integration. Users are then able to use text messages.

Main Menu Screen and INBOX

Figure 6-39 shows the main menu when entering the text message service. The service is similar to text messaging using SMS on cellular networks. This service is located within the hospital domain and delivered over the Cisco Unified Wireless Network network. An inbox keeps a list of all received messages until they are deleted.

Figure 6-39 Main Text Message Service Menu

Composing a Text Message

To compose a message to a user, there are several options for finding a user.

- Search based on a user name
- Int—When entering a specific extension for the user
- Pager—When sending a message to a pager system
- SMS—When sending a SMS to a cellular system
- Email —To select sending an email to a user

Figure 6-40 Email Options

Once an extension is entered, the user is ready to write the text message.

Figure 6-41 Ready for Text to be Entered



Receiving and Answering a Text Message

Figure 6-42 shows an example of a user receiving a text message. Once this message is read, Figure 6-42 shows a few predefined options for how the text message can be answered. A few predefined messages are created to easily answer the text message or a custom message can be typed. Another option allows a voice call back from the message originator.

Figure 6-42 Example of User Receiving a Text Message and Options for Answering Message

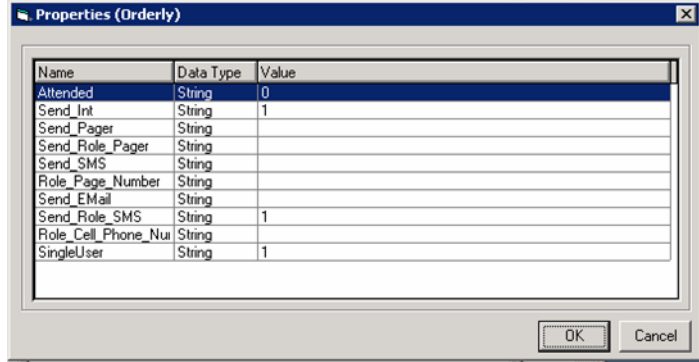


IMATIS Hospital Orderly Request

IMATIS Portal for System Administration

From the IMATIS portal on the IMATIS server used by the system administrator, the orderly groups can be defined. The administrator should select “User Manager”. Under the directory tree of OppDrag, individual orderly teams can be defined. A special note on the role attributes is a field called Attended. When this field is set to “1”, that means the role is 24x7 and can never be unattended. This setting prevents users from un-enrolling before a new user enrolls to take on that shift.

Figure 6-43 IMATIS Portal



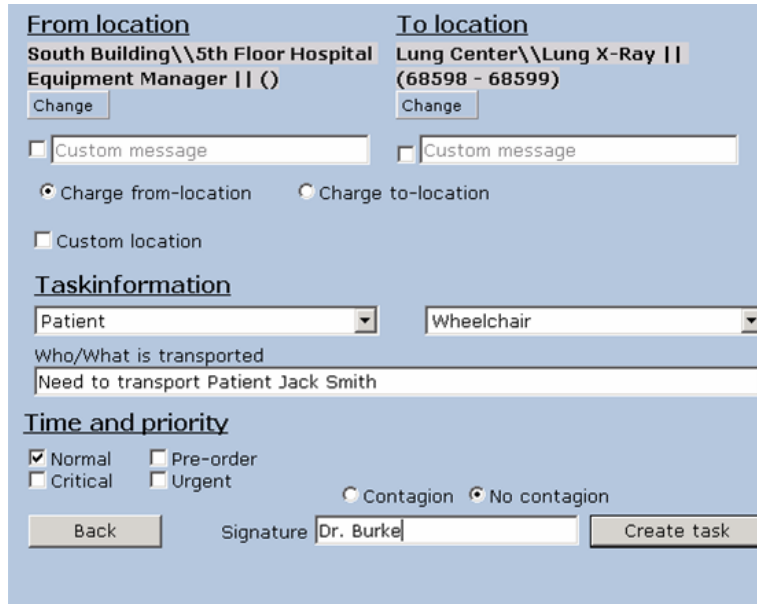
Name	Data Type	Value
Attended	String	0
Send_Int	String	1
Send_Pager	String	
Send_Role_Pager	String	
Send_SMS	String	
Role_Page_Number	String	
Send_Email	String	
Send_Role_SMS	String	1
Role_Cell_Phone_Num	String	
SingleUser	String	1

223023

IMATIS Hospital Orderly Request Interface

The Hospital Orderly Request tool as seen by a hospital staff user is retrieved via the http link <http://imatis-server/ImatisOrderOrderly/AjaxOrderPage.aspx>. This interface provides many options for hospital locations, request types, and the request message. Filling out this form lets hospital staff make a request to an orderly.

Figure 6-44 Hospital Orderly Request Tool



From location
South Building\\5th Floor Hospital Equipment Manager II ()

To location
Lung Center\\Lung X-Ray II (68598 - 68599)

Custom message

Custom message

Charge from-location Charge to-location

Custom location

Task information
Patient Wheelchair

Who/What is transported
Need to transport Patient Jack Smith

Time and priority
 Normal Pre-order
 Critical Urgent
 Contagion No contagion

Signature Dr. Burke

223024

Once the order has been placed, the staff can view the current status of that request. Changes can be made to the request through this same interface. Figure 6-45 shows the order status interface after the order has been placed.

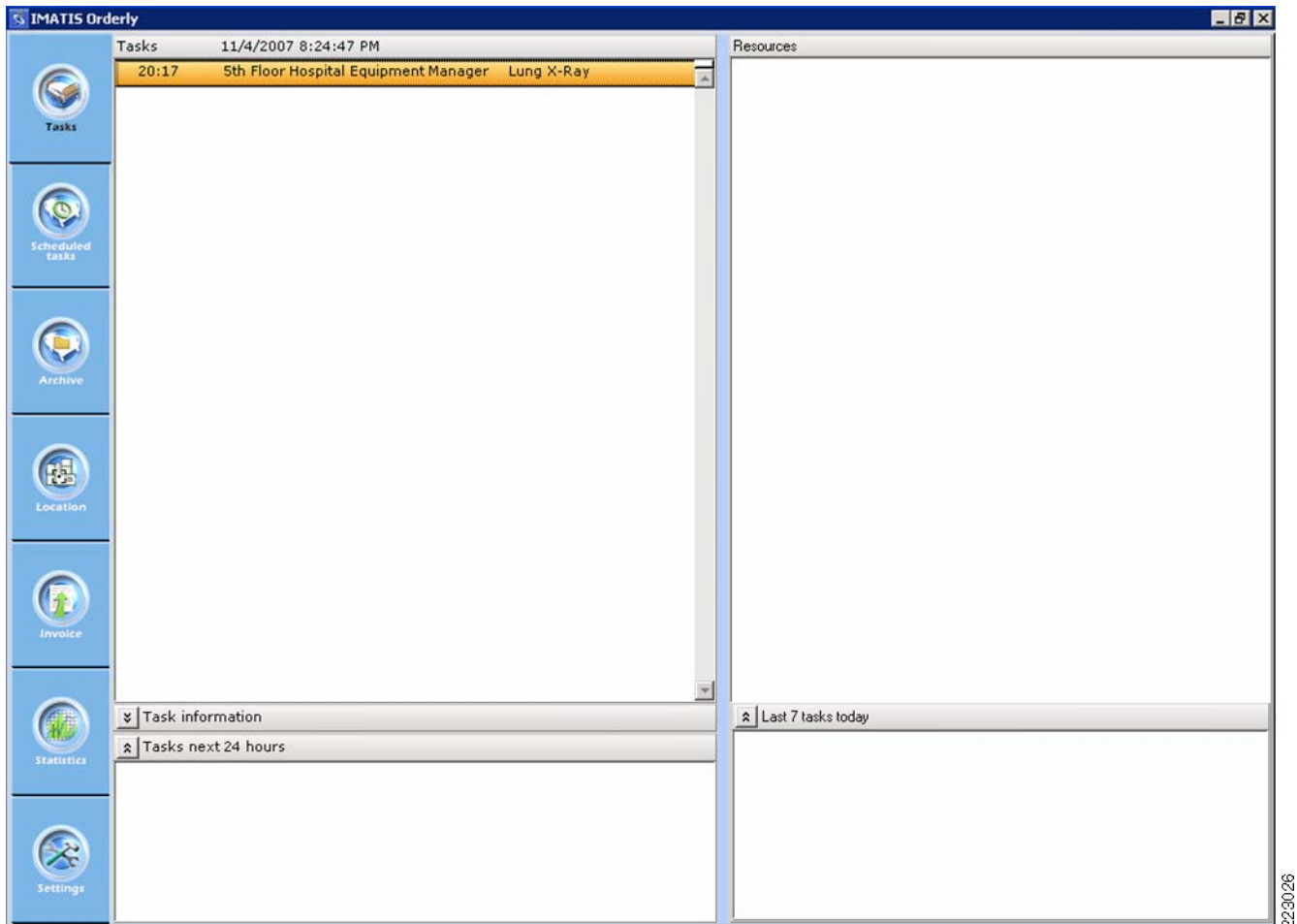
Figure 6-45 Reviewing Requests

This orderly request is they sent to the hospital dispatcher to assign a person to the task.

IMATIS Dispatcher

The dispatcher sees a different interface that allows the dispatcher to see all tasks (incoming, currently unassigned, assigned, and other states) and a list of enrolled orderly staff to which the work can be dispatched. This interface should only be used by the dispatcher. To start this interface, the IMATIS application name is `ImatisTransporter.exe`. Figure 6-46 is a sample of the interface seen by the dispatcher.

Figure 6-46 Sample IMATIS Dispatcher Interface



Hospital Orderly Workflow

The orderly staff users carry a Cisco 7921 IP phone to facilitate their daily workflow as they move about the hospital. Through this interface, the staff can sign in and resign from a role, set the status for their role if they are busy or out to lunch, for example, and also receive requests and notify the dispatcher of their progress in handling the request. [Figure 6-47](#), [Figure 6-48](#), and [Figure 6-49](#) show a few phone interfaces as seen by the staff for invoking these work flow states.

Figure 6-47 Main Menu and Enrolling



Figure 6-48 Setting Orderly State



Figure 6-49 Receiving Orderly Request and Acknowledge

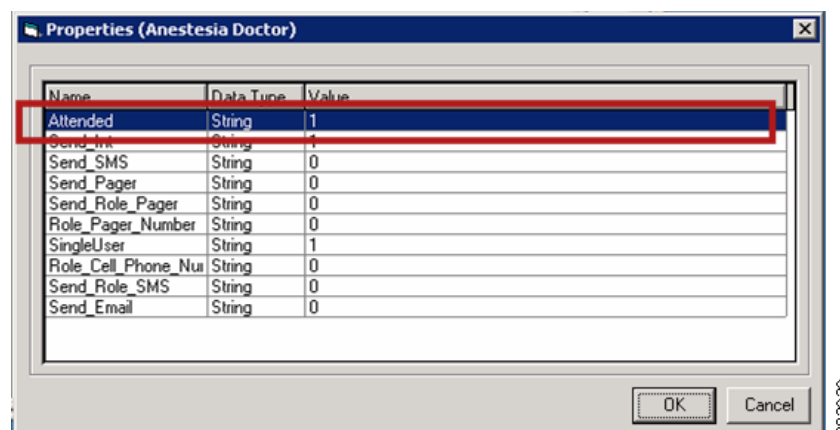


IMATIS Medical Team Assembly

IMATIS Portal for System Administration

From the IMATIS portal on the IMATIS server used by the system administrator, the set of teams can be defined for each hospital setting. The administrator should select “User Manager”. Under the directory tree of Tikalling -> Team, individual teams and roles can be defined. A special note on the role attributes is a field called Attended. When this field is set to “1”, that means the role is 24x7 and can never be unattended. This setting prevents users from un-enrolling before a new user enrolls to take that shift. You can define individual roles, teams, and departments. After these teams and roles are defined, the system can be used to create summons and have users enroll.

Figure 6-50 IMATIS Portal for System Administration



The process for creating the hierarchical structure for these teams is to start with a department. Under the department, there may be various teams that are defined. Then under the teams, define specific roles for these teams. The attributes for these departments, teams, and roles should be defined.

IMATIS Medical Team Assembly Request

After these roles have defined, the system is ready to send summons to users of the system. There are several methods to create a summons:

- IMATIS summons request tool
- XML service from a Cisco IP phone
- URL speed dial defined for a Cisco IP phone

IMATIS Mobile Nurse Call integration for critical summons that has a predefined business rule from IMATIS for that specific alarm generation.

The IMATIS summon tool is shown in [Figure 6-51](#) to illustrate the interface a nurse station might see to request an emergency doctor in room 201. The user may choose to send a summons to a team, an individual role, or a group function. These are specified when the teams and roles are defined by the system administrator. To access this request page, use the following link
<http://imatis-server/imatisamk/resmon.asp>

Figure 6-51 IMATIS Summon Tool

Role:
Emergency Doctor

Who calls internal emergency number

Add location
Free text (max. 12 characters)
HELP! 201 Add

Message
ALARM

Send Close

223031

IMATIS Medical Team Assembly Workflow

As a user initially signs onto their shift, they would also enroll in a particular role. If the user is taking over a 24x7 role shift, a message is sent to the current person in the role.

Figure 6-52 Message to Current Person in Role



Using the phone, a request can also be made to summon a particular role or a team.

Figure 6-53 Message to Summon a Particular Role or Team

When a message is received on the phone, the user can ack the request or call 911 to request help.

Figure 6-54 Options for Responding to Message**Note**

This workflow can be monitored by a hospital staff member or dispatcher. Use the following link to access the Medical Team Assembly call status: <http://imatis-server/imatisamk/callmon.asp>.

IMATIS Mobile Alerts

The integration with fire and building alarm systems for alerts requires integration with the building systems. IMATIS uses ESPA 4.4.4 as one standard for this integration. The ESPA adapter is performed through the BizTalk server. The building alert is received from alarm systems. Based on the business rules applied to the parameters received through the ESPA interface, the message is then sent to the appropriate user. IMATIS uses the parameters received to apply business rules. One business rule may be based on whether the received alert is an emergency or just an equipment malfunction. If the alert is an emergency, the user may be presented with an option for immediately calling emergency 911.

User Assignment

Assignment of these alerts to a user is defined by the roles within the IMATIS system administrator portal. A role that is associated with a technical department or emergency department may be created. Users are assigned to these roles and receive building or fire alarm alerts when sent from the ESPA system.

Figure 6-55 Assignment of Alerts

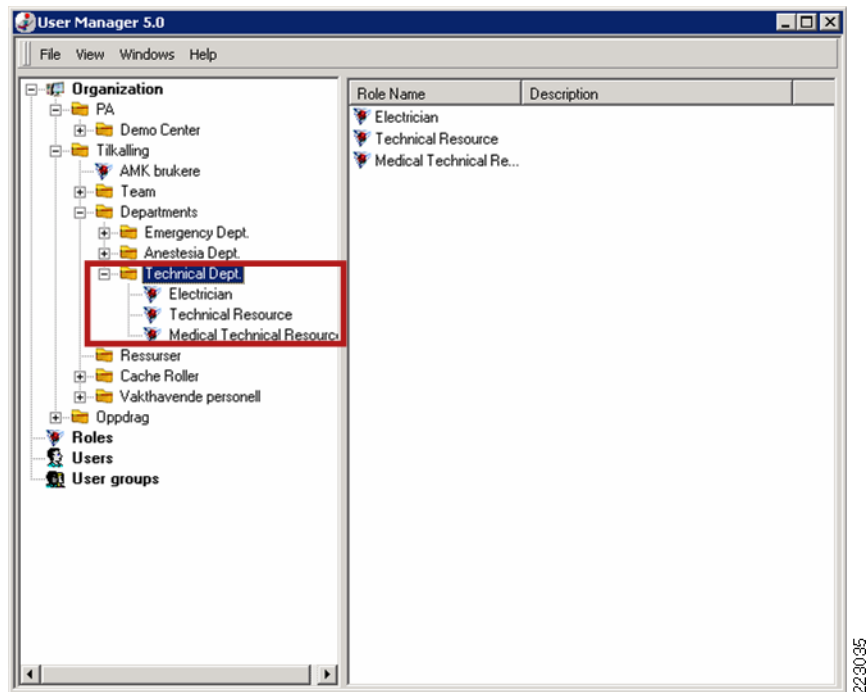


Figure 6-56 shows a sample of three screens with alerts received for fire alarms or building technical problems.

Figure 6-56 Alerts for Fire, Building, and Technical Problems



IMATIS Scalability Considerations

As the deployment of Cisco Imatis Mobile Care services grows and the number of users expands, the scalability of the IMATIS Hospital Communication System is achieved by installing the application over several servers. Using several SQL Servers, the databases and tables can be shared among additional hardware. Microsoft BizTalk is designed to be able to increase performance either by running several servers or by moving components on various servers. The IMATIS servers can run Microsoft Network Load Balancing (NLB) to increase performance or, if necessary, the components can be allocated to different servers.

