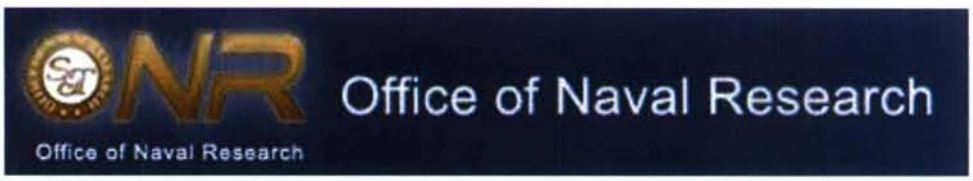
Final Technical Report

Intelligent Advanced Communications IP Telephony Feasibility for the U.S. Navy

ISRN L3COM/HENSCHEL/TR -- 2007/001

Contract Number: N00014-06-C-0062

Prepared For



Submitted by:
Todd D. Binns
Bill Naas

Volume I

Henschel

9 Malcolm Hoyt Drive
Newburyport, MA 01950 U.S.A

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
09-10-2007	Research	Aug 9 2006 – Oct 9 2007

4. TITLE AND SUBTITLE

Intelligent Advanced Communications

Phase 1, Research and Conceptual Design

5a. CONTRACT NUMBER
N00014-06-C-0062

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Binns, Todd D; Principle Investigator

Naas, Bill; Investigator

5d. PROJECT NUMBER
N.A.

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Henschel Inc., L-3 Communications
9 Malcolm Hoyt Drive
Newburyport, MA 01950-4017

8. PERFORMING ORGANIZATION REPORT

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
875 N Randolph St., Suite 1425
Arlington, VA 22203-1995

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research paper is to research technologies and solutions supporting the communications infrastructure necessary to implement an integrated VoIP (IP telephony), Video and Data infrastructure on U.S. Naval vessels.

This report is based on a collection of extensive research topics:

- L3 Henschel internal research
- Commissioned research papers
- Vendor responses to a formal questionnaire
- U.S. Navy vessel specifications
- Government documents focusing on network security and implementation.

Major findings for implementing an integrated VoIP (IP telephony), Video and Data infrastructure on Naval vessels:

- The technology is becoming pervasive within the commercial market sector.
- Implementing an IP solution on U.S. Navy vessels is feasible and achievable.
- Due to the unique requirements of the U.S. Navy, there is a staged implementation planned from feasibility to proof-of-concept (FY08 phase 2), followed by evaluation in a Navy lab and Navy ship (FY09 phase 3).
- Benefits of an integrated VoIP (IP telephony), Video and Data infrastructure are space and weight savings of 50% and cost savings of 25% with additional features and functionality.
- There will continue to be major investments in this infrastructure under an Open Systems Architecture consortium, thus enabling wide availability of COT's products.
- The integration of VoIP (IP telephony), Video and Data will be secure as detailed by Bell Labs and Defense agency publications.

15. SUBJECT TERMS
VoIP, SIP, H.323, US Navy, Vessels, Communications, Network, SVoIP, VoSIP, SVoSIP

16. SECURITY CLASSIFICATION OF: U			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Christopher P. Rigano (CISSP)
a. REPORT	b. ABSTRACT	c. THIS PAGE ii	UU		19b. TELEPHONE NUMBER *(include area code)* 703.696.65942

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Abstract

The purpose of this research paper is to research technologies and solutions supporting the communications infrastructure necessary to implement an integrated VoIP (IP telephony), Video and Data infrastructure on U.S. Naval vessels.

This report is based on a collection of extensive research topics:

- L3 Henschel internal research
- Commissioned research papers
- Vendor responses to a formal questionnaire
- U.S. Navy vessel specifications
- Government documents focusing on network security and implementation.

Major findings for implementing an integrated VoIP (IP telephony), Video and Data infrastructure on Naval vessels:

- The technology is becoming pervasive within the commercial market sector.
- Implementing an IP solution on U.S. Navy vessels is feasible and achievable.
- Due to the unique requirements of the U.S. Navy, there is a staged implementation planned from feasibility to proof-of-concept (FY08 phase 2), followed by evaluation in a Navy lab and Navy ship (FY09 phase 3).
- Benefits of an integrated VoIP (IP telephony), Video and Data infrastructure are space and weight savings of 50% and cost savings of 25% with additional features and functionality.
- There will continue to be major investments in this infrastructure under an Open Systems Architecture consortium, thus enabling wide availability of COT's products.
- The integration of VoIP (IP telephony), Video and Data will be secure as detailed by Bell Labs and Defense agency publications.

This page intentionally left blank.

Table of Contents

List of Figures

This page intentionally left blank.

List of Tables

1 Executive Summary

The objective of this research paper is to research technologies and solutions supporting the communications infrastructure necessary to implement an integrated VoIP (IP telephony), Video and Data infrastructure on U.S. Navy vessels based on a Total System Computing Environment (TSCE). The current TSCE environment has two separate infrastructures, one for telephony and one for data. The recommended integrated VoIP (IP telephony), Video and Data infrastructure will provide one IP based infrastructure for telephony and data.

This report is based on a collection of extensive research topics:

- L3 Henschel internal research
- Commissioned reports
- Vendor responses to a formal questionnaire
- U.S. Navy vessel specifications
- Government documents focusing on network security

The referenced documents and vendor questionnaires are included in the Volume II Appendices A through S.
There are two volumes included in this report. Volume 1 includes a Technical Summary Section followed by a Technical Detail Section on the key technical topics to support a VoIP (IP telephony), Video and Data infrastructure. Also in Volume I is a Phase 2 Recommendations section of the study, which comprises the test bed and proof of concept recommendations.

Volume II incorporates the Technical Appendices that support the technical information and analysis from a number of published industrial and government agency sources, such as:

- Bell Labs
- Defense Information Systems Agency (DISA)
- National Institute of Standards and Technology (NIST)
- National Security Agency (NSA)

These sources address Internet Protocol (IP) Telephony guidance and provide security technical implementation guides.

Volume II incorporates the Vendor Questionnaires (Appendix S) that asks questions about the functionality of the commercial vendor's Commercial-Off-the-Shelf (COTS) products. A matrix is included that summarizes the COTS vendor responses. This report has been structured to provide a readable overview but also to provide technical detail on the relevant topics in support of VoIP (IP telephony), Video and Data infrastructure.

The Internet Protocol Public Branch Exchange (IP PBX) market space has greatly expanded with the predominate deployment of VoIP in the commercial markets, quickly

followed by the expansion into the home market segment. There are multiple analysts' studies that consistently show accelerated growth of the IP PBX's market. An example of this growth is the In-Stat study [1]. Table 1-1 provides a view of this growth. In 2005, the study shows (source In-Stat 9/06) that the total PBX market grew by 23.3 million lines, of which 69.1% were IP lines. By 2010, total new line shipments are projected to reach 38.2 million lines, of which 99% will be IP. This data, a US market analysis, shows that growth is being driven by commercial vendor investments in switching, routing, and Ethernet technology that provides greater call clarity, reduced latency, and reduced deployment costs. Key market drivers for this growth in IP telephony are lower long distance costs, additional features created by the implementation of an IP based infrastructure, and planned integration of multiple mobile devices, wireless IP phones, Personal Digital Assistants (PDA), and other IP based devices. As a result of this market shift (and replacement of the traditional voice segment), the VoIP (IP telephony), Video and Data infrastructure reliability will be at least 99.999%. This translates into less then 5 minutes downtime for an entire year of operational use (a standard requirement for the traditional Time-Division Multiplexing (TDM) legacy phone infrastructure).

Table 1-1. Traditional and IP PBX Line Shipment Forecast

Shipments	2005	2006	2007	2008	2009	2010	CAGR
Traditional	7,426,296	6,509,276	5,489,431	3,959,889	1,959,705	459,286	
% Growth	-42.9%	-12.3%	-15.7%	-27.9%	-50.5%	-76.6%	-42.7%
IP PBX	15,849,062	19,171,997	23,027,883	27,560,710	32,789,222	37,761,165	
% Growth	69.1%	21.0%	20.1%	19.7%	19.0%	15.2%	19.0%
Total PBX	23,275,358	25,681,273	28,517,313	31,520,599	34,748,928	38,220,451	
% Growth	4.0%	10.3%	11.0%	10.5%	10.2%	10.0%	10.4%

Source: In-Stat, 9/06

The implementation of VoIP (IP telephony), Video and Data infrastructure provides clear benefits that will be recognized by the U.S. Navy during the deployment of an integrated VoIP (IP telephony), Video and Data solution on board U.S. Navy vessels. The following outlines some of the key benefits that the U.S. Navy will experience:

- Space and weight savings of the communication center that could approach 50% in cubic feet and an equivalent 50% weight savings when comparing a VoIP (IP telephony), Video and Data infrastructure with a traditional TDM and separate network infrastructure.
- Better system functionality when comparing an equivalently configured VoIP (IP telephony), Video and Data infrastructure to a traditional TDM and separate network infrastructure.
- Cost savings of 25% when comparing an equivalently configured VoIP (IP telephony), Video and Data infrastructure to a traditional TDM and separate network infrastructure. The cost savings are anticipated to get better with time as the commercial world continues to invest, develop and expand the integrated VoIP (IP telephony), Video and Data market.

- Additional features to improved overall communication efficiencies when comparing an equivalently configured VoIP (IP telephony), Video and Data infrastructure to a traditional TDM and separate network infrastructure. These features will continuously increase over time as a result of the extensive investment by the commercial world, and will provide ongoing operational benefits to the U.S. Navy.

Some of these benefits are due to the integration of voice, video and data on the same network instead of multiple separate networks, one for voice and one for data. This makes the end devices (IP based communications terminals, dial phones, and dedicated phones that support voice communications, video on demand, and IP data) extremely powerful to meet a variety of mission critical requirements. Additional functionality that can be added to the end devices include the following:

- Manual selection for viewing through the end devices
- Ability to view video that is stored, live feed, or streaming for training simulation or live damage control monitoring
- Video Conferencing
- Display important vessel information
- Support customize configuration profiles for individual user on the terminals
- Display important weather information
- End devices can be dual homed for more resilience and system availability.

It is important to realize in a VoIP (IP telephony), Video and Data integrated infrastructure that the cost savings achieved by migrating from a TDM solution to a VoIP solution will most likely be offset by adding more and richer features utilized by the end devices. Thus, a cost savings versus feature benefit tradeoff study will likely be required for the final solution to help priorities and control feature expansion.

Additional benefits are expected in the area of reduced manpower hours required to support and maintain the system since both the VoIP, Video, and Data will be implemented on the same infrastructure system (instead of a separate infrastructure for networking and a separate one for the telephony infrastructure). This will require less training for personnel on future deployments and less ongoing maintenance of the system while deployed due to the converged functionality of the IP network. The manpower savings will most likely not be realized until the deployment of this infrastructure has matured and is stable within the U.S. Navy environment. As the IP based system matures over the next several years and as features, functionality, training and operational costs become pervasive, manpower savings should become more quantifiable.

The maturing of the VoIP (IP telephony), Video and Data infrastructure is currently based on an Open System Architecture using the Session Initiated Protocol (SIP). SIP is being utilized by all major vendors to support interoperability, and ease of implementation and scalability. Most of these suppliers, Cisco, Avaya, Nortel, and LGS (Alcatel and Lucent), have a full proprietary solution and, in parallel, an extensive standard SIP based solution. This is not unusual as companies develop a proprietary implementation to insure that customer focused features can be added without being

bound by industry wide standards and then follow-up with an industry open architecture "standard" solution. This is consistent with how Networking infrastructure has been developed and deployed over the past decades. There is no real impact on customer deployment. Customers can have competitive COTS solutions where one vendor may be deployed within a region site or geographical environment with a rich feature set, but still be able to communicate with other vendors through the standard protocols. This scenario will be applicable to the U.S. Navy by using competitive COTS products for the initial ship deployment based on price and features being awarded. For the follow-on procurement, the award may go to another vendor based on price and features. Each ship would have a complete COTS VoIP (IP telephony), Video and Data infrastructure based on competitive bid. However, each ship (independent of vendor) would still be able to communicate with the other due to design adherence to open standards. This is typical of historical technology developments.

During Phase 2 of the program, three different vendor solutions will be fully tested. Along with the testing of multiple SIP implementations, at least one of the vendor's full proprietary solutions will be tested to demonstrate full functionality of a VoIP (IP telephony), Video and Data infrastructure. Also, one of the selected vendors (Sphere) for the Phase 2 Test Bed has implemented an IP PBX using the SIP protocol that has already been certified by the Joint Interoperability Test Command (JITC).

Security is one of the more important parts of a converged network consisting of voice, video and data streams. Aside from the normal security issues revolving around e-mail, network infrastructure and virus scanning, security for the voice must be part of the initial design. There is no benefit for deploying a VoIP system without first ensuring that the data network is secure. Security must be implemented in a layered approach. This means that security must encompass the entire system. Each component must have a focus on security, starting with the End Instrument (IP Phone), by hiding the phone/network parameters. The Call Servers, Media Gateways, Session Border Controllers, Routers, Switches and Firewalls must be locked down and require administrative access (UserId/Password) for management changes. Also, many of the data network precautions, such as virus scan software and patch management systems, need to be in place to keep the soft phones, servers and personal computers up to date. All voice streams and call signaling should be encrypted, ideally end-to-end. Within the technical aspects of this report, extensive support information addressing security for the VoIP (IP telephony), Video and Data infrastructure is included. Also included in the appendices or in the list of references is the following key documents:

- Defense Information System Agency, Network Infrastructure, Security Technical Implementation Guide, V6R4, December 2005 (excellent resource for guidelines when deploying a security policy across the infrastructure).
- National Security Agency, Security Guidance for Deploying IP Telephony Systems, Report 1332-016R-2005, February 2006 has developed additional security configuration guidelines and checklists.
- Defense Information System Agency, Internet Protocol Telephony & Voice Over Internet Protocol, Security Technical Implementation Guide, V2R2, April 2006 (provides specific security guidelines for VoIP installations)

- Defense Information Systems Agency, DOD Telecommunications and Defense Switched Network, Security Technical Implementation Guide, V2R3, April 2006.

During Phase 2 (starting in Oct 2007 and to be completed during government FY2008), L3 Henschel will assemble a test bed at its facility that incorporates multiple vendors solutions based on COTS products for the purpose of evaluating the VoIP (IP telephony), Video and Data infrastructure and its applicability to U.S. Navy shipboard requirements. The test bed will be dynamic in nature, but will be evaluated based on a detailed test plan for the multiple configurations. The test plans may evolve as results of testing and changing requirements are factored back into the project to see how the VoIP (IP telephony), Video and Data infrastructure performs in the test environment. The purpose of the Phase 2 effort is to evaluate the proof of concept and feasibility of implementing VoIP (IP telephony), Video and Data on U.S. Navy vessels. The testing results will support a design that will meet (and exceed) the needs of the U.S. Navy by providing an IP packet network that carries voice, video, and data on the ship. This project will not design end devices for the implementation, but will test COTS products according to U.S. Navy requirements. The goal is to show where enhancements can be found in the new IP packet network infrastructure and to help define and support the future direction of the U.S. Navy with the integration of voice, video and data for vessels. Feasibilities learned about voice, video and data integration, in the areas of IP-PBX, COTS products, encryption methods, and network fault recovery will be presented. Figure 1-1 below shows the test bed design. Specifically, the test bed supports voice, video and data using multiple vendor equipment. During this phase, L3 Henschel will demonstrate operation, function, and findings to the Office of Naval Research.

During the Phase 3 (government FY2009), a representative VoIP (IP telephony), Video and Data infrastructure solution based on the test lab environmental results will be moved into a U.S. Navy Lab, and later moved onto a ship for additional verification for naval vessel suitability. This three phase staged approach (Phase 1 feasibility study (FY07), Phase 2 proof of concept and demonstration to ONR (FY08), and Phase 3 (FY09) verification for implementation) will be used to support the planned deployments during and following Phase 3 of the study. The test bed is described in Section 6 of Volume I of this report. The Configuration will look as shown in Figure 1-1.

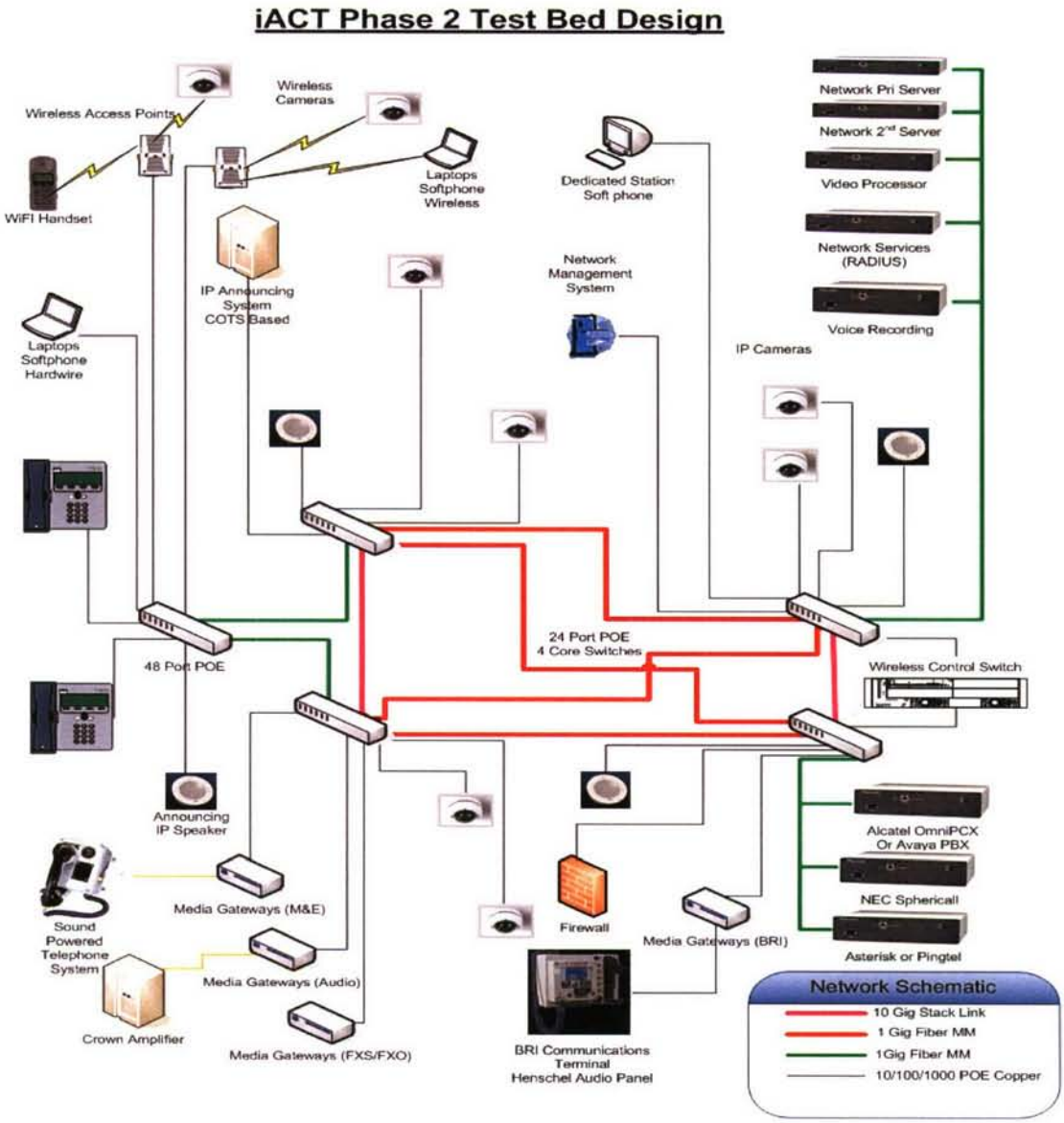


Figure 1-1. iACT Phase 2 Test Bed Design

1.1 Conclusion

The key points of this research paper for implementing VoIP (IP telephony), Video and Data infrastructure on Naval vessels are summarized below:

1) Implementing an integrated VoIP (IP telephony), Video and Data infrastructure is becoming pervasive within the commercial market sector.
2) Implementing an integrated VoIP (IP telephony), Video and Data infrastructure for U.S. Navy vessels is feasible and achievable. Due to the unique requirements of the U.S. Navy, there is a staged implementation planned from feasibility to proof-of-concept, followed by evaluation in a U.S. Navy lab and U.S. Navy ship through FY09.
3) Benefits of an integrated VoIP (IP telephony), Video and Data infrastructure are space, weight and cost savings with additional features and functionality.
4) There is and will continue to be major investments in this infrastructure under an Open Systems Architecture consortium, thus enabling wide availability of COT's products.
5) The integration of VoIP (IP telephony), Video and Data will be secure as detailed by Bell Labs and Defense agency publications.

This page intentionally left blank.

2 Technical Summary

2.1 Current Naval Communications Solution

2.1.1 Introduction

Today's naval voice communications systems provide both internal and external voice communication capabilities for the crew and other personnel onboard a navy vessel. Internally, the voice system provides a means for transmitting information to all areas and spaces onboard the vessel. Externally, the voice system provides interfaces for secure and non-secure off-ship communications.

This section describes a typical voice communications system that would exist onboard a US Navy Ship or Submarine today. It does so by describing the four major components that make up the voice system. These components include the

- Voice Telephone System
- Sound Powered Telephone System
- Wirefree Communications System, and
- Announcing System.

Each of these components provides key capabilities as well as redundant methods for communication at critical command and control positions.

The sections that follow give a general overview of how these components are used onboard a ship or submarine, along with the capabilities each provides. The four system components that make up the voice communications system are then examined in terms of their subcomponents and capabilities.

2.1.2 Voice System Capabilities

The ship's voice communications system provides both internal and external voice communication capabilities. These capabilities are delivered through four major components that make up the voice system. The four components are: the Voice Telephone System, the Sound Powered Telephone System, the Wirefree Communications System, and the Announcing System.

2.1.2.1 Internal Voice Communication Capabilities

The ship's voice communication system is designed to provide primary, auxiliary and supplementary communications capabilities for various control, operating, and service related functions onboard a navy ship. Internal voice communication capabilities include station-to-station calling, intercom calling, conference calling, and the broadcast of alarms and announcements.

The voice communications system provides addressing, and call signaling capabilities for voice circuits across all voice system components. Users on the Voice Telephone System are able to access the Sound Powered Telephone and Wirefree Systems. Similarly, users on the Wirefree System are able to communicate with users on the Voice Telephone System. Both the Voice Telephone and Wirefree Systems also have interfaces to the Announcing System for one-way communications over supported announcing circuits.

In addition to providing one-way communication platform for transmitting information and orders throughout the ship, the Announcing System is also used to broadcast alarm tones and emergency messages alerting the crew to specific conditions or impending dangers.

Critical ship command and control positions are fitted with redundant communications terminals providing primary and auxiliary methods of communication over separate networks. Although this redundancy is normally accomplished with the Voice Telephone System acting as the primary means of communication, and the Sound Powered Telephone System providing an auxiliary or backup system in the event of a power failure, this is not always the case.

Depending upon the location onboard a ship the Sound Powered Telephone System or Wirefree Communications System may act as the primary means for voice communication. Supplementary communications terminals may also exist at many locations. These terminals would serve as an alternate or additional means of communication for various control, operating and service functions.

Other systems that may exist onboard a ship but are not considered part of the ship's voice communications system include the Shipboard Air Traffic Control Communications (SATCC) System, and the Emission Controls (EMCON) System. Interfaces would exist between these systems and the major components of the voice system to provide additional internal communications capabilities.

On large carrier class ships, the Voice Telephone System will interface to the Shipboard Air Traffic Control Communications (SATCC) System to provide supplementary air traffic communications. The Sound Powered Telephone System also has interfaces to the SATCC to provide supplementary communications as defined by the SATCC configuration.

The Wirefree Communications System interfaces to the SATCC or Flight Control Console to transmit and receive Flight Deck communications. Additionally the Wirefree Communications System has interfaces to the Emission Controls (EMCON) System used to disable electromagnetic emissions from the main site equipment and antenna system.

The Announcing System also provides an interface to the SATCC. This interface allows designated SATCC user stations to broadcast announcements to specific announcing circuits onboard the ship.

2.1.2.2 External Voice Communication Capabilities

The ship's voice communication system supports both secure and non-secure off-ship communications. These capabilities are provided through several different interfaces. The use of these interfaces is dependent on whether a ship is in port or underway.

While in port, external communications are handled through pier-side landline connections to the ship's Voice Telephone System. The ship's Wirefree System provides supplementary communications for pier-side operations when in port.

While underway, surface ships will use a ship's Sound Powered Telephone System for external ship-to-ship and bridge-to-bridge communication with other nearby vessels. The Announcing System provides a supplementary means for this type of communication.

The Announcing System is also used to pass orders and information to other ships and tugboats during close-in maneuvering and docking operations. The ship's Wirefree System provides supplementary means of communication for boating operations.

Other systems that exist onboard a ship but are not considered part of the ship's voice communications system include the ship's Radio Communications System (RCS), and Automated Digital Network System (ADNS). These systems have interfaces to the major system components of the voice system and provide additional external communications capabilities.

The Voice Telephone System interfaces with the ship's Radio Communication System (RCS) for external tactical communications. Other external communications are supported from Voice Telephone System to the ADNS while the ship is underway.

2.1.3 Voice Communication System Components

2.1.3.1 Voice Telephone System

The ship's Voice Telephone System consists of one or more interconnected telephone switches, i.e. Private Branch Exchange (PBX) units, along with supported analog and digital voice terminal devices.

The Voice Telephone System is designed to combine the services of a ship's service administration telephones, Sound Powered Telephone System, and Wirefree System into a single voice system that can be connected directly to the Public Switched Telephone Network (PSTN).

2.1.3.2 Telephone Switch

Each Telephone Switch provides control, and switching capabilities for connecting two (2) or more voice terminal devices, and allows direct communication between selected operator positions onboard the ship.

In addition to control and switching capabilities, the telephone switch will normally support many of today's standard commercial telephony features. These features include: auto-answer, distinctive ringing, priority calling, call forwarding, and call transfer.

2.1.3.3 Voice Terminals

Voice terminals include all standard analog and digital telephones, as well as Integrated Communications Terminal (ICT) devices when supported through a separate RCS for tactical communications.

Analog telephones would be standard Tip & Ring, and support Dual Tone Multi-Frequency (DTMF) operations with the telephone switch. Digital telephones would support standard digital protocols such as Integrated Switched Digital Network (ISDN) Basic Rate Interface (BRI). Additionally each of these terminals may could support advanced calling features such as single button activation calling, Push-To-Talk (PTT) signaling, Caller ID, IC calling, and speakerphone operation.

ICT devices, if included would support both interior communications as well as exterior tactical radio communications. Connections from the telephone switch and RCS would be physically segregated up to the ICT device. ICT devices are required to support features including: single button activation calling, non voice-activated PTT signaling, and Caller ID. Each ICT would be associated with a configuration or profile containing single button activation assignments and other unique terminal settings.

Additionally ICT units have two separate headset/handset connectors, one marked user and the second marked supervisor. These connectors provide voice transmission override to the supervisor headset/handset by muting the user microphone when the supervisor PTT is enabled.

2.1.3.4 Multi-Level Precedence and Preemption (MLPP)

The Voice Telephone System will support Multi-Level Precedence and Preemption (MLPP). MLPP is a priority scheme for assigning a precedence level to specific calls such that the Voice Telephone System will handle them in a predefined order and time frame.

In this scheme calls with a higher precedence level will be given control of voice network resources over lower precedence calls. This feature guarantees that network resources will be available to specific persons or end devices. Additionally, MLPP allows for barge-in connections to stations or terminal devices connected in a lower precedence call.

2.1.3.5 Conferencing

The Voice Telephone System provides multi-party (three or more) calling for vital and tactical communications. The system will normally support many of today's standard commercial conferencing features including: pre-set, meet-me and ad hoc conferences.

In addition to these general requirements for conference support, the Voice Telephone System will normally be required to support some upper limit for number of conference attendees, and number of simultaneous active conferences.

2.1.3.6 Intercom (IC) Calling

Some voice terminal devices connected to the Voice Telephone System are required to operate in Intercom (IC) mode. In this mode a voice terminal device would be equipped with a speaker and microphone, and provide single-button activation of intercom functionality.

A terminal device receiving an IC call would also need to be fitted with a speaker and microphone. On receipt of an IC call, that device would be required to auto-answer the call in IC mode.

Although IC calling will normally be supported through the Voice Telephone System directly, some voice communications systems will have a special purpose Intercom System component that must also be integrated into the total voice communications system.

2.1.3.7 Emergency Reporting

The Voice Telephone System provides a means for initial reporting of emergency conditions onboard the ship or submarine. This feature requires that all voice terminals be capable of initiating, through a single programmable button, a non-blocking connection to report the emergency condition. Emergency conditions would include: fire, flood, personal injury, and the like.

Onboard a large surface ship the telephone switch might need to route the emergency call to one of several different emergency stations, while onboard a submarine there may be only one emergency station that all emergency calls are routed to. In other instances the emergency call may get connected to the announcing system allowing the emergency condition to be broadcast over a dedicated emergency announcing circuit.

2.1.3.8 Voice Mail Subsystem

A Voice Mail Subsystem provides voice-messaging capabilities for configured voice terminal devices. This subsystem allows callers to leave a message for the person or station associated with a voice terminal device when calls are not answered.

Typical Voice Mail systems will allow users to record a personal greeting that callers will hear when the user is unable to answer a call. Additionally the system would allow the user to retrieve messages either locally or remotely, and would play back the date and time when the voice message was left.

2.1.3.9 Call Accounting Subsystem

A Call Accounting Subsystem allows for the capture of all call traffic within the Voice Telephone System for configured voice terminal devices. Captured call accounting data is stored electronically for retrieval through pre-configured and user defined call traffic reports.

2.1.3.10 Shore Connections

The Voice Telephone System provides external communication capabilities through landlines when docked in port. These shore connections may be analog or digital.

2.1.3.11 System Administration Terminal

The Voice Telephone System will have a System Administration Terminal for loading, configuring, and backing up telephone switch software and configuration data.

In addition to software configuration, the System Administration Terminal is able to restrict the capabilities of user voice terminals. Restriction capabilities provide a means to limit user-to-user, user-to-interface, interface-to-user, and interface to interface calling capabilities through the entire Voice System.

All administration configuration and restriction changes need to be made without disrupting other system operations and activities.

2.1.4 Sound Powered Telephone System

The ship's Sound Powered Telephone (SPT) System is a failsafe voice communications platform connecting one or more SPT devices over a SPT circuit. This system requires no external power source, but instead relies on the sound pressure of a user's voice to power all connected SPT devices. All users connected on a SPT circuit are able to talk and listen at the same time.

The SPT System is a vital communications system used for communication in damage control central, engineering spaces, weapons control, after steering, radio central, lookout, the combat information center, the steering bridge, and other critical stations onboard the ship. It is used for both routine and emergency communications, and is needed for the ship to function properly and carry out its mission.

2.1.4.1 SPT Circuits

The SPT System consists of three types of SPT circuits: switchboard, switch box, and string. Switchboard circuits are circuits that originate

from a SPT switchboard, switch box circuits originate from a SPT switch box, and string circuits are made up of a series of SPT station jackboxes connected to a common line.

These circuits are divided into three classifications depending upon their usage. These classifications are primary, auxiliary, and supplementary.

Primary circuits provide communication for primary control and operating functions associated with ship control, weapon control, engineering control, and damage control.

Auxiliary circuits provide a backup to certain primary circuits, and offer redundant means of communication should damage occur to the primary circuits. Wiring of auxiliary circuits are kept separate from their corresponding primary circuits.

Finally, supplementary circuits consist of short, direct circuits, normally of the string type. These circuits are normally not manned. Some supplementary services are equipped with a buzzer or horn for calling other stations.

2.1.4.2 SPT Equipment

The SPT equipment includes: headset-chestset terminals, handset terminals, jackboxes, and selector switches.

Headset-chestset terminals have a mouthpiece or transmitter suspended from a yoke that is attached to a metal chest plate. Earphones connected to an adjustable headband function as the receiver. These units are designed for general shipboard use.

Handsets are similar to standard telephone handsets. These devices are designed for general use on a circuit with other handsets and headset-chestsets.

Jackboxes house the connector that a headset-chestset or handset terminal would plug into to access a SPT circuit. Handsets are normally hard-wired to SPT jackboxes while headset-chestsets can be connected and disconnected as needed.

Selector switches are used to communicate over multiple SPT circuits. By turning the rotary dial on a selector switch, a user is able to talk on any one of several different SPT circuits. These units are located throughout a ship at control and operating stations. Most selector switches have a SPT handset hard-wired into the switch.

2.1.5 Wirefree Communications System

The ship's Wirefree Communications System provides both one and two-way wireless (un-tethered) communications to support onboard and off-ship

operations. These operations include: damage control, command and control, engineering, security, ship to boat communications, beach guard, shore patrol, medical, flight operations and propulsion watch standers.

The system is made up of one or more base station units capable of supporting a pre-configured number of radio devices. An administration terminal is used to support each base station, and one or more radio programming workstations allow for configuration of supported radio devices.

2.1.5.1 Wirefree Base Station

The Wirefree Base Station is made up of multiple Radio Frequency (RF) Repeaters to providing the radio circuits, and a wirefree controller to direct, process, and handle connected radio call traffic.

2.1.5.2 Fixed Standard Radios

Fixed Standard Radios are enclosure mounted, and contain an integrated speaker and hand microphone. These radios are powered by the ships Vital 115VAC Distribution System.

2.1.5.3 Fixed Command Radios

Fixed Command Radios are provided with a remote loudspeaker with volume control, a standard U.S. Navy handset, and use a mobile command display appropriate for use in command and control spaces. These radios are powered by the ship's Vital 115VAC Distribution System.

Fixed Command Radios support remote control through a command radio remote. This radio remote has an external connection for a lightweight headset.

2.1.5.4 Portable Radios

Portable Radios are compact, lightweight, and water and impact resistant. These radios are battery powered and require a portable radio charger.

2.1.5.5 Fleet Select Box

A Fleet Select Box (FSB) is a wireless terminal device used on the flight deck of large deck carriers at aviation control stations including: Air Boss, Mini-Boss, Handler, and Carrier Air Group (CAG) Commander.

FSBs have transmit and receive capabilities to all other FSBs, and support a ruthless preemption priority scheme between each other.

The FSB has external connectors to support a standard U.S. Navy amplifier-loudspeaker. Additionally provides two external connectors with volume control for standard U.S. Navy handsets/headsets, and an external connection supporting transmit audio, receive audio, and PTT signaling.

2.1.5.6 Flight Deck Helmet Headset

Flight Deck Helmets are fitted with a monaural headset with left and right earpiece speakers, a microphone, and boom-mounted PTT switch. The helmet headset provides hearing protection to reduce external noise level in the users' ears while providing intelligible receive audio in conditions of extreme ambient noise.

2.1.5.7 Group Hierarchy and Multi-Level Priority Scheme

The system can be configured as hierarchical structure that supports partitioning of wireless users into groups, segregated geographically or organizationally. This hierarchical structure allows lower level groups and users to hear calls and announcements from higher-level groups and users.

The system also supports a multi-level priority scheme for queuing subscribers, talk groups, and subgroups, such that the next available channel available from the wirefree base station will be assigned to the highest priority user.

2.1.5.8 System Administration Terminal

A System Administration Terminal is used to define and maintain base station databases, load and backup system configuration data, and monitor system capacity and traffic loads.

Through the administration terminal, users can add, change and delete individual users and talk groups, and adjust system parameters without disrupting normal operations.

2.1.5.9 Radio Programming Workstation

Radio Programming Workstations are COTS Personal Computer (PC) based systems equipped with the appropriate Operating System (OS) and radio programming software needed to program and configure wireless radios.

The workstation provides storage for all radio configuration parameter files. Additionally the workstation provides a means to backup all radio configuration parameter files onto durable, loadable, removable media.

2.1.6 Announcing System

The ship's Announcing System consists of an Announcing Controller, Announcing Amplifiers and Loudspeaker Strings, and multiple Microphone Control Stations. Some Microphone Control Stations are equipped with Alarm Activation Panels that allow these stations to initiate alarm announcements.

The Announcing System is used for one-way communication of information, alarms and orders to multiple locations onboard a ship or submarine. This system provides an interface to the Ship's Entertainment and Training System for disabling of video and audio signals during alarm and voice announcements.

2.1.6.1 Announcing Controller

The Announcing Controller receives input signals from Microphone Control Stations and Alarm Activation Panels. The controller interprets these input signals and distributes an appropriate one-way alarm or voice announcement to selected announcing circuits.

The Announcing Controller is responsible for proper handling of messages and announcements based on some pre-configured priority scheme. See section 2.1.6.6 below for more information on alarm and announcement priorities.

2.1.6.2 Announcing Amplifiers and Loudspeaker Groups

Alarm and voice announcements are distributed through Announcing Amplifiers to strings of Loudspeakers, arranged in groups, that make up the Multi-Channel (MC) Circuits, i.e. announcing circuits, onboard a ship or submarine.

2.1.6.3 Microphone Control Station

Microphone Control Stations provide the primary interface for voice announcements to selected MC Circuits onboard a ship. When equipped with an Alarm Activation Panel, these units are also used to enable and disable alarm audio signals.

2.1.6.4 Multi-Channel (MC) Circuits

Multi-Channel (MC) Circuits are made up of one or more loudspeaker groups selected simultaneously for the delivery of alarm and voice announcements.

A ship's 1MC Circuit, also known as the General Announcing System, is used for transmitting general information and administrative orders to all spaces onboard a ship. Other MC Circuits found onboard larger surface ships include:

- 2MC – Used to transmit announcements to the Propulsion Plant.
- 3MC – Used to transmit announcements to the Aviator.
- 5MC – Used to transmit announcements to the Flight Deck.
- 6MC – Used for ship-to-ship announcements.

2.1.6.5 Alarms and Visual Alarm Indicator

Alarms are pre-recorded audio tones with defined frequency and cadence used to alert the crew to some emergency condition. Alarm audio signals onboard an aircraft carrier include:

- Collision Alarm
- Chemical Alarm
- General Alarm
- Emergency Alarm (this is a voice announcement override of all other voice announcements)
- Flight Crash Alarm
- Flight Deck Warning

During an alarm announcement, the Announcing Controller may additionally set electrical relays to signal visual alarm indicators in noisy areas of the ship such as machinery spaces where the alarm might not be heard.

2.1.6.6 Alarm and Voice Announcement Priority

A priority scheme exists for the transmission of alarms and voice announcements onboard a ship when multiple announcements are attempted at the same time over a MC Circuit.

This scheme will normally give alarm announcements priority over regular voice announcements. Additionally a priority weight is normally given to all alarms so that the alarm of highest priority will be enabled when multiple alarms are selected simultaneously.

Additional priorities may be given to voice announcements based on Microphone Control Station location. A station in one location onboard ship may have priority over other stations onboard when multiple voice announcements are attempted over the same MC Circuit.

2.1.7 System Fault Monitoring/Reporting

2.1.7.1 Local & Remote Alarms and Visual Indicators

Most of the components that make up the ship's voice communications system provide some method for diagnostic testing as well as health monitoring. Some of the major components are able to initiate alarms and visual indicators to signal technicians in the event of a failure.

The Voice Telephone System has built in diagnostic testing for user, bearer, and line control circuitry and provides mechanisms for both local and remote reporting of alarms that impact switching operations.

The Wireless Communications System includes a monitor and alarm terminal for each base station. This terminal is used to monitor and test radio quality, and verify the integrity of wirefree base station operations. On detection of a failure, this system is able to display error data to the monitor and alarm terminal, and initiate an audible message at selected radios.

2.1.7.2 UPS Backup

Major system components that require power to support operation are equipped with Uninterruptible Power Supplies (UPS). These UPS units have varying time requirements for continuous system operation in the event of a power failure.

Some systems only allow for graceful system shutdown giving enough time for updating and archiving of system data. Other systems require that a UPS provide some pre-defined number of hours of continuous operation on a power failure, and may support alarms and indicators associated with UPS health.

2.1.8 Summary

Naval voice communications systems provide internal and external voice communication capabilities onboard a navy vessel. The ship's voice communication system is designed to provide primary, auxiliary and supplementary communications.

The major components that make up this system and provide its capabilities are the Voice Telephone System, the Sound Powered Telephone System, the Wirefree Communications System, and the Announcing System.

These components support interfaces allowing users on one system to communicate with users on another system. Announcing resources are also shared through these inter-component interfaces. The voice communications system also supports interfaces with other separate communications systems found onboard some ships, and can provide supplementary communications for that system.

Critical ship command and control positions are fitted with redundant communications terminals providing primary and auxiliary methods of communication over separate networks.

The four major components that make up the voice communications system, along with their interfaces were examined. The capabilities and supported functionality provided by these components were discussed along with the end user equipment used to facilitate communications.

2.2 Recommendations and Conceptual Design

2.2.1 Introduction

This report will pull together the different overviews of the technology into a concise recommendation and conceptual design that can be used to move forward on integrated voice, video and data. The following chapters will detail the information that is introduced in this section. Each point in this report relates directly to one or more sections in the body of this report. Even more detail can be found in the appendixes that support the overall recommendations and the conceptual design that is laid out here.

2.2.2 Recommendations

Industry has been moving to Voice over IP (VoIP) for several years. In the beginning the move was slow and has faltered several times with technical issues. The early adaptors have had a rough road that has not had the return that was promised. This has changed over the last couple years. Major Telephony providers have moved into this area, and brought with them the promise of five nines in stability. The adoption of open system protocols has been slow with many of the major vendors using their own proprietary protocol built on top of ITU-T Standard H.323 or Session Initiated Protocol (SIP).

SIP has emerged from the different open system protocols as the default for VoIP. SIP was created by the Internet Engineering Task Force (IETF) in 1999 and then updated in 2002 with Request For Comments (RFC) 3261 [2]. It is still being developed and extended to fulfill the signaling needs of the future. It was designed to be extended in the future and was given the functionality to negotiate the features that the server and client can support. This is the base of the telephony system that we are recommending. Its open system architecture has several different specifications that have been ratified by the IETF and many drafts that are being evaluated. SIP runs on a packet based network the same as an IP network that is currently used for data on board ship.

The network is very important to how SIP will perform. In the past the telephony network was a proprietary network that was developed on a home run design, meaning that each end device would have to travel back to the PBX directly. There was some multiplexing done, but that was very limited. The connection that each end device has to the PBX is not shared with other end devices, so bandwidth is a non-issue. In the TSCE model integrated voice, video and data, can reside on the same network. There are benefits and disadvantages to this new model. Voice video and data are all competing for the resources on the IP network. Over the last several years as the performance of the network has improved the bandwidth has increase. The use of priority on different types of packets allows for the voice and then video to have priority over the data packets. This results in a network that is practical to voice calls. The option to separate the three packets by having them on different wires still can be done, but several of the benefits will not be achieved in that architecture. The network is not the only part that has improved over the last couple years.

The computing power of the PC has come a very long way, compared with what it was only 10 years ago. As the design is looked at this change in performance of the server hardware and the network are key to why this solution can be implemented today, where only a few years ago it was not a viable option. In the current implementation of telephony there is a PBX which is a large cabinet that is located in s node room where all the lines from the individual end devices converge. In the VoIP model it is reduced to several server grade PCs that make up the IP-PBX. Since the system is designed on IP, each end device connects to the network at the location of the end device. It's packets travel through the network to the IP-PBX. The IP-PBX requires a single connection to the IP network that can support the bandwidth; this connection can be done with fiber. Dual network connections can be used for resilience in the event there is a network failure. The IP-PBX server contains several different programs that support the different functions of the old PBX. VoIP is a network-based solution, which also requires the standard services that a data device will require, such as Domain Name Service (DNS), and Dynamic Host Configuration Protocol (DHCP). These services can be dedicated for the VoIP network or be shared with the data network.

Even though the VoIP system can run with a single set of applications, it is almost never installed with out redundancy designed into many of the required functionalities. This would be in the area of the different programs that make up the IP-PBX, as well as multiple connections to the network. In some cases a redundant network, such as the Consolidated Afloat Networks and Enterprise Services (CANES) project, can be used. There are several different ways this is supported, but in all cases it is completely transparent to the end user of the phone. In the implementation care needs to be taken that no device has the Real-Time Transport Protocol (RTP) stream passing through a single device resulting in a single point of failure.

The internal radio is limited in nature compared to what a desk phone can do. The use of wireless telephony will give the mobile user the functionality of the desk phone in a portable package. The wireless access points would be located in each compartment that would require an individual to have contact to the phone system. The different access points are controlled from a redundant controller. The controller manages the individual access points so they appear as a single one to the client that connects to it. The controller also controls power and assists in moving clients from overburdened access points to one that has fewer connections. Because of the ability of the wireless controller, a site survey is not required, reducing the costs and the making the system easier to maintain.

Security is a very large issue. Because of this we found that the DoD has already spent many resources on policies and Security Technical Implementation Guide (STIG)s. These defined why and how security will be implemented. The area that is not discussed is the degradation of performance as the different levels of security are implemented as defined in the STIGs. Even with the guidelines defined there are several areas to look at:

- VLANs will need to be implemented for several different reasons. The first is to secure the different types of IP packets from other types. VLANs will also be used for directing packets through different segments of the network for performance and resilience requirements.

- IP Separation is another method of isolating the IP packets from other types of packets. By having the different end devices in different subnets they will not be able to receive or send data to other devices that are on different subnets.

- Layer 3 Bridging allows switches that support Layer 3 to filter traffic and combine flows where required. This can support both VLANs and IP Separation allowing the switch to combine multiple flows into a single flow and directing the flow to a single port on the switch. For example, several feeds of telephony end devices can be combined into a single feed to be directed to the IP-PBX.

- Layer 2 Protocols are the ones that are defined in the Internet layer of the TCP/IP model. The protocol implemented at this layer is IPSec. It protects the path between two devices; it is also what a virtual private network (VPN) is implemented with. The two devices must support this protocol; there is performance degradation for setup and connection.

- Layer 3 Protocols are the ones that are defined in the Transport layer of the TCP/IP model. These protocols encrypt the packets and send them down a non-encrypted path where the receiving application has to do the de-encryption. As with the Layer 2 Protocols, there is performance degradation.

- The Firewall is a device that is placed between the intranet and the external network. It is configured to only allow defined packets to pass in either direction. A firewall can be combined with a session boarder controller (SBC) so the SBC handles the VoIP packets and the firewall handles the other packets. This must be configured correctly to restrict the traffic and maintain security.

- Update patches are created for several of the components in the network. The operating systems depending on the manufacturer to provide patches on a weekly basis or may only have them monthly. Implementation of a patch on a vessel would require it to be downloaded when in port or to be sent to the vessel through an uplink. However, the size of the patches can be very large in size. The U.S. Navy is already dealing with this on the data network and the process should not need to be changed. In most cases a central management tool is used to force the patches to all computers on the network. The end devices like telephones the patches are less common, but do happen. The method of updating varies by vendor, but most support the use of a file transfer server, such as a TFTP server, that the phone connects to on startup and gathers the patches, as well as their configurations information.

- The current data network should already support an antivirus regimen to protest the current assets that are on the data network. In the case of a vessel, they have limited connection to the outside Internet, so contracting a virus is limited, expect from users of the network itself.

- The administrators of the network need to be at a security level that can handle the highest level of security that the calls will be set at. It is very important that

the administrator understand the network topology so there are no mistakes tying together the wrong networks. This should be reduced by the network management system that will visually show the network and the configuration.

The Network Management System (NMS) will be a tool that the administrator will use to track the network and make configurations. The NMS should be matched to the network switches. It can be purchased from the manufacturer of the switches or there are products from other vendors. If the IP-PBX is purchased from the same vendor as the network switches, then the NMS should be able to manage all of the components of the system. This is a benefit since the administrator only needs to learn a single application that puts the complete network at the administrator's fingertips.

One method of reduction is to use integrated applications. In this case, integrating the telephony device with the console application so the sailor only has to use a single application. It can also be done with foreground and background applications, but this requires switching back and forth between two or more applications. In the development of a real time application, such as a telephone, it needs to always be looking for and processing packets. If it is in the background it may be starved for resources resulting in missed packet issues. This can be worked around in the development and configuration of the operating system, but care needs to be taken during the installation process to iron out any issues between applications. Where possible, the consoles should be integrated with a softphone. This will also have a savings on the cost of the phone hardware compared to the cost of the sound card and handset.

2.2.3 Conceptual Design

The conceptual design is presented in Chapter 3. Figure 2-1and Figure 2-2 show the general configuration of a total ships computing environment (TSCE). Its concentration is on the telephony, but its backbone design will support the other computing environments that need to connect to it. In Appendix C, the topology is taken and analyzed for a larger vessel. In this study it was found that limited bandwidth was being utilized. The use of VLANS was required to make the network resilient and not have a single point of failure.

The design starts with two nodes that contain the main servers and the core network switches connected in a partial or full mesh topology. These can be redundant or Red/Black configuration. These nodes would contain uninterruptible power supplies that would maintain the power when ship's power is lost. Each node would also have other components that are not shown which do not add to the network design but are critical to the survivability of the node. Leaving the individual nodes are edge switches that connect back to two core switches so that one link can be lost without losing the connectivity from the devices to the edge in a Star topology. These edge switches would supply power to the end devices with Power over Ethernet (PoE). This will not power all the end devices, but many of them can be powered by this means. The design relies on wireless network for mobile sailors to connect to other members of the crew through mobile phones. The wireless network will also support data so individuals can use laptops and not have to connect to a hardwire connection.

The next phase is to create the test bed as defined in Chapter 4. This phase will allow the recommendation and the conceptual test bed design be proven and prepared for the sanctioned vessel test lab before being trialed onboard a vessel. This test lab will allow for rapid testing of security, performance, degradation and telephony feature set completeness.

As noted in the Benefits section integrated voice, video and data has major benefits for the U.S. Navy to pursue. Several documents authored by the Chairman of the Joint Chiefs of Staff and Defense Information Systems Agency (DISA) have defined policies and Security Technical Implementation Guides (STIG)s for the implementation of integrated voice, video and data. The benefits and the already defined policies and STIGs make this a very doable and positive forward direction to give the U.S. Navy new features, reduced cost, weight and reduction in cost.

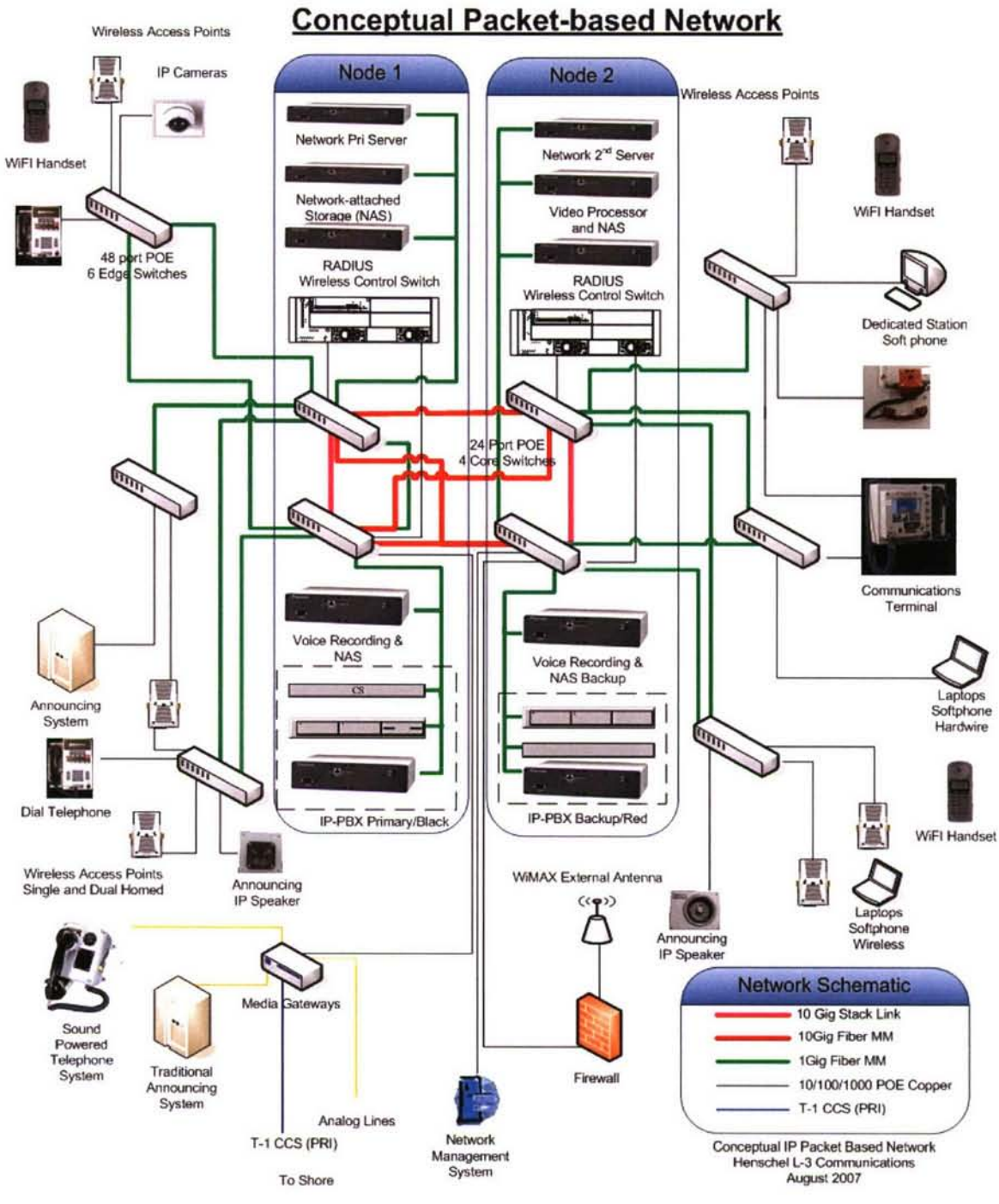


Figure 2-1. Conceptual Packet-Based Network

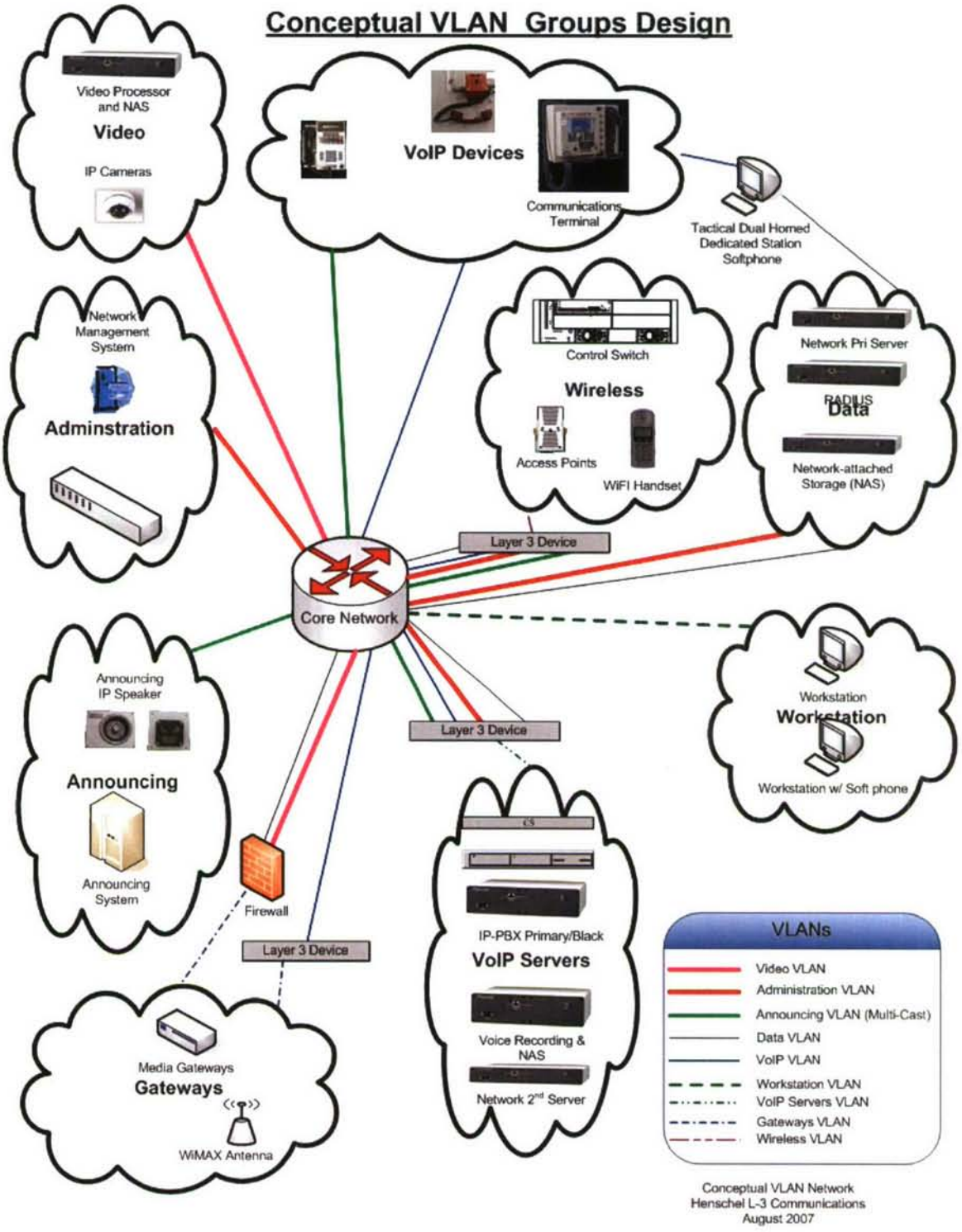


Figure 2-2. Conceptual VLAN Groups Design

This page intentionally left blank.

2.3 *Comparison of the Current Telephony System and VoIP*

2.3.1 Introduction

This report will compare what is presently on board a U.S. Navy vessel, and a new design that would be developed around voice over Internet Protocol (VoIP). This VoIP design would be developed around session initiated protocol (SIP) that is open system architecture. Chapter 4 and 5, will support the methods defined within this report. Both systems are made up of the same main sub systems:

- Voice Telephone System
- Sound Powered Telephone System
- Wirefree Communications System
- Announcing System.
- Total Ships Computing environment (TSCE) (Only VoIP design)

The VoIP design will be integrated to include voice, video, and data on a single IP network. Each subsystem will be discussed individually; and contrasted between the two different technologies. This report will discuss a single design, but for each type of vessel there are differences that will not be covered within. Even with the differences, the main functionalities are covered or can be extrapolated.

2.3.2 Voice System Capabilities

The functional capability of internal and external communications will not change with the introduction of VoIP. The introduction of VoIP will extend the capabilities of the current design.

2.3.2.1 Internal Voice Communication Capabilities

Internal communications will be handled in the same overall method. Both technologies use a PBX to handle the calls. In the Telephone Switch section below the differences between the two PBX technologies is discussed. The current technology uses a home run method of connecting the voice terminal to the PBX. This requires multiple wire runs from the voice terminal to the PBX. The VoIP solution uses the TSCE so the individual voice terminal is connected to the network and the PBX is connected to the network. This results in a reduction in wire, as well as the need for a wire closet to terminate all the wire runs. The wirefree communication system would be included into the VoIP design using wireless network access points and mobile phones. Using this new technology will allow the sailor to have push-to-talk as well as the same features as they would have if he were using a desk phone. The Sound Powered Telephone system would require a media gateway to bridge the two different types of technologies; this is no different than the current design that uses a proprietary card in the PBX. The current Announcing system is designed around amplifiers that are located in racks. The speakers connect to the rack through speaker strings that have multiple speakers that are of the same MC group. In the VoIP design the announcing system would use the TSCE and the speakers would connect through the network; this would reduce the wiring requirements. The amplifiers are built into the individual speakers. The removal of the speaker strings, allow one speaker to

mis-function and not bring down the complete string. Connecting to other onboard communications systems, such as Shipboard Air Traffic Control Communications (SATCC) System or Emission Controls (EMCON) System will be handled by media gateways. As these systems mature, they could be connected on the TSCE by using Layer 3 bridging, since they would reside in different Virtual Local Area Networks (VLAN) on a well-designed network.

2.3.2.2 External Voice Communication Capabilities

In port external communications in the current system has proprietary PBX cards that are wired from the PBX to the exterior of the vessel. In the VoIP solution the use of media gateways are used that convert the IP packets to the type of interface that is required. For the future, the connection to the external communications can be done with IP packets through a firewall or Session Boarder Controller. The Radio Communications System (RCS) and Automated Digital Network System (ADNS) work the same way as the in-port external communications with a proprietary PBX card for the current system. In the VoIP design media gateways would be used to connect to the RCS and ADNS. The media gateways come in different interfaces, some for telephony and others for audio, to mention a couple. This would be the method used to connect to non-IP based technologies to the network.

2.3.3 Voice Communication System Components

2.3.3.1 Voice Telephone System

2.3.3.1.1 Telephone Switch

The current Telephone Switch design is one or more proprietary cabinets that contain processor boards and circuit cards that connects to each individual voice terminal. In the VoIP design it is made up of several server PC that can be as small as 1 or 2 rack units in height and be installed with redundancy. On the current design the loss of a line card affects all voice terminal connected to it. This results in a large savings of space. There is a limited number of media gateways that are also required depending on the number of non-IP based connections. These can be located in the racks with the servers or distributed to reduce the wiring requirements.

2.3.3.1.2 Voice Terminals

The current voice terminal encompasses standard analog and digital phones, as well as an Integrated Communication Terminal (ICT). ICT is designed around multiple BRI connections to the PBX and the RCS. There are also dedicated stations, which are special phones of the above three types that are used through out the vessel. In the VoIP design these main phone groups would be reduce to IP phones and a new version of the ICT. The dedicated stations would all be developed around the IP phone. The technology used for all the IP phones and ICT

would be based on Session Initiated Protocol (SIP), so there would be a reduced number of protocols used on board ship.

2.3.3.1.3 Multi-Level Precedence and Preemption (MLPP)

The current system support MLPP, but on many vessels a more simple "priority" is used instead. In the VoIP design SIP has a couple RCFs that implement MLPP

Request For Comments (RFC) 4412 [3] introduces two new header fields "resource-priority" and "accept-resource-priority" to indicate request for priority treatment during emergencies.

RFC 4411 [4] defines an extension to the REASON header to be included in the BYE requests to allow a User Agent (UA) to know that its session is torn down (preempted) to allow a higher precedence session.

2.3.3.1.4 Conferencing

The current system supports conferencing using the PBX to do the joins between the different legs. For large conferences the PBX vendor may use an external device that does the join between the different legs. The cut off point for how many conferences and the number of individuals in a conference vary by manufacturer. The VoIP design is not very different in nature. SIP can handle conferences natively, but is limited to just a few in the conference. The different vendors implement the conferences in a couple different ways. Most support a small conference of 10 to 25 in their IP-PBX; from there most vendors use a separate device to handle the joins. The connection to this device is IP, where the current solution would have a T1 or other telephony interface that requires proprietary cards in the PBX cabinet.

2.3.3.1.5 Intercom (IC) Calling

The current phone systems support intercom on speakerphones. The VoIP design has some limitation that can be worked around. Currently there is no RFC that deals with intercom calls, but there has been several different drafts, none of which have been ratified. Polycom, Inc. supports it in their speakerphones with an added parameter in the INVITE header of the SIP call. Several IP-PBX manufacturers have supported Polycom's implementation. Sphere Communications division of NEC within its product Sphericall that is Joint Interoperability Test Command (JITC) certified IP-PBX uses Polycom Inc. phones.

2.3.3.1.6 Emergency Reporting

Emergency reporting is more a function of the configuration of the PBX and its voice terminals. As the current system is configured, the VoIP system can also be configured to handle the dedicated numbers, conference calls, and connection to the announcing system. With the VoIP design an auto-attendant can be created that automates several of

these steps, so limited personal intervention would be required. Each vendor of the VoIP systems has different levels of this type of auto-attendant program. There are also other companies like SandCherry Inc. that have platforms that support development of an auto-attendant type application.

2.3.3.1.7 Voice Mail Subsystem

The voice mail system is vendor dependant; the current and the VoIP solution have it. The VoIP offerings provide a unified messaging system that brings together different message media into a single easy to use package. This can be as simple as delivering a voice mail to an email address.

2.3.3.1.8 Call Accounting Subsystem

Call accounting subsystems is a vendor dependant application. All major vendors have offering that basically have the same types of information. The information that is obtained from a VoIP based system varies a little from the current design since the information about the call is different.

2.3.3.1.9 System Administration Terminal

The current design has a terminal either supplied by the manufacturer of the PBX or PC that allows the administrator to connect to the PBX. In the VoIP solution it will depend on which vendor is used. The larger vendors have a complete network management system that manages the IP-PBX as well as infrastructure switches. The dedicated IP-PBX manufacturers have their administration performed from a console or command line. Since the IP-PBX are on PC servers, the administration can be performed from the server or from a remote location either from a web page or from a console application. The method used varies by the required security balanced with the ability to administer the PBX.

2.3.3.2 Sound Powered Telephone System

The sound powered telephony system is not changed by the move to VoIP. The interface to it will change from the proprietary card in the PBX to a media gateway that is purchased for the required interface. The same functionality will be seen with either the current or VoIP design.

2.3.3.3 Wirefree Communications System

The current wirefree communications system is made up of a wireless based station that houses multiple radio frequency repeaters and the wireless controller. There are several different types of radios that are used depending on the type of vessel it is implemented on. Some of the radios are fixed locations that have a ruthless preemptive priority scheme between them.

The wirefree communication system would be included into the VoIP design using wireless network access points and mobile phones. Using this new

technology will allow the sailor to have the same features as they would have if they were using a desk phone. For the locations that are fixed radios in the current design, the solution could be either wireless phones or fixed phones; this design decision will need to be determined on a fixed radio-by-radio basis. Since SIP supports MLPP the preemptive scheme will need to be looked at by vessel type. The mobile phones can support headsets and the push-to-talk feature. The end result is that the VoIP design will bring the two different communication methods together into a single solution that will add more features and functionality to the mobile sailor. There will be no need for a proprietary interface that is used in the current design.

2.3.3.4 Announcing System

The current announcing system has evolved over time and has no commercial counter part. Because of the unique requirements that have evolved, there is no VoIP solution that handles all the required features. The VoIP design uses a software program that handles the priority and grouping of the speakers. This program would require added features to evolve into what the current system has evolved to. The VoIP solution still has several other features that the current system will never have. The speakers are not setup on a single string that becomes the single point of failure. Since the speakers are on the IP network that has redundant paths developed into it, if there is a single failure it should only affect a few speakers. Detailed planning of what speakers are on what switches and weaving them between multiple edge switches will add to the resilience of the solution. The IP speakers are on the network and so are prone to the network delays with the correctly developed network infrastructure as defined in Appendixes A, C, and D; this can be elevated so there is no "out of sync" playback of announcements. The current system can be used in areas that may require its power; the use of a media gateway would be used to connect it to the TSCE. The current announcing system also uses microphone stations on some vessels. This can be done with a standard IP phone that has been repackaged and has defined speed dials for the different MC announcements group and priority.

2.3.4 System Fault Monitoring/Reporting

Fault monitoring and reporting has evolved from the needs of the U.S. Navy on its vessels. The VoIP solution would require the use of several different tactics to monitor the complete system. Because it is based on PC and network infrastructure, the use of a network-monitoring tool maybe the only solution required. As with the current solution the need for un-interruptible power supplies (UPS) will also be required. In the VoIP solution since it relies on the TSCE the network switches will also require UPSs to maintain the infrastructure.

2.3.5 Network Infrastructure

The current design has a separation between telephony and IP-Network. In the VoIP design they are integrated into TSCE. This combining of the two

different networks allows for freedom that can not be accomplished with the networks being separated. A single device can include data, as well as telephony, resulting in reduced terminal that will result in a reduced amount of training. It should also reduce the number of individuals that are required to support the two separate networks when they are integrated into the TSCE.

2.3.6 Summary

The two systems are different because of the technologies used, but the functionality can be achieved with VoIP. With the flexibility of the new technologies, new features can be added that could never have been done with the current technology. VoIP is the direction that the telephony industry is moving and the U.S. Navy needs to start to look at it and evaluate the shortcomings and engineer them out, so a viable solution will be ready when the U.S. Navy decides to make the transition to VoIP.

2.4 Benefits

2.4.1 Introduction

The benefits for the U.S. Navy to go to an integrated VoIP, Video and Data solution on board U.S. Navy vessels can be looked at in several aspects. First being clearly defined benefits that will have direct product cost and operational savings in support of U.S. Navy deployments. Secondly, there are less defined benefits due to the analysis that would be required, but having anticipated additional operational savings and efficiencies that would be realized. Thirdly, in addition to cost and operational efficiencies the integrated solution will offer more product features. These features will continuously increase over time to provide ongoing operational benefits to the U.S. Navy. The reason for this is that the integrated Voice, Data, Video solution is currently being widely deployed by the commercial business environment on a worldwide basis. This solution is being extended to the vast number of home users. The U.S. Navy can easily realize cost savings, operational efficiencies, and additional product features benefiting from the industry investment being made by many companies to support this IP infrastructure expansion.

2.4.2 Cost Savings

L3 Communications Henschel developed a comparison of an integrated VoIP, Video, Data solution based on an IP infrastructure and compared this to a standard Data, Video and Time-Division Multiplexing (TDM) Voice installation based on current shipping legacy technology. This was a complete detailed comparison recently done which was based on a combat ship model implementation. The product cost savings of equipment with the integrated Voice; Video and Data solution represented approximately a 25% product cost savings.

Any actual cost savings is dependant on the actual ship configuration and specific products implemented, but this savings is believed to be very representative of the savings that would be anticipated. It should be noted that the IP technology has been and is projected to be on a better cost saving curve compared with current voice technology, so a 25% product cost savings would be a conservative projection of what the U.S. Navy should expect to see by deploying an integrated VoIP, Video, Data IP solution on combat ships.

2.4.3 Space Savings

As part of the same analysis mentioned in the cost savings paragraph 2.4.2 an integrated IP based VoIP, Video, Data solution compared to a standard data and TDM-based system will take up approximately 50% of space. Refer to configuration comparison and Table 2-2. Conceptual design layouts are provided by Figure 2-3and Figure 2 4.

A typical configuration for equivalent functionality would be 71 cubic feet for an IP VoIP, Video, Data system and 134 cubic feet for a standard data TDM system. The comparison was done for one bay of equipment for a small combat ship. Large vessels will have relatively the same space savings per bay of equipment deployment.

Table 2-1. Summary of IP Implementation Dimensions and Weight

Rack	Width	Depth	Height	Weight
Aft	24	34	76	1032
Forward	24	34	76	985
				2017

71 Cubic Feet
All dimensions are in inches
Weight is in pounds

Table 2-2. Summary of Legacy Implementation Dimensions and Weight

Rack	Width	Depth	Height	Weight
Aft	24	25	76	776
Forward	24	25	76	807
Contingency	24	25	76	767
CIS	24	33.5	65	930
WIFCOM	24	27	69	899
				4179

134 Cubic Feet
All dimensions are in inches
Weight is in pounds

2.4.4 Weight Savings

Based on the space saving the relative weight for the configuration will also be proportionally the same for an approximate 50 % savings when comparing a real model for the IP solution of approximately 2017 lbs and the equivalent weight of the current Data and TDM solution of approximately 4179 lbs. This again is for the same scenario to configure one bay of a combat ship. Both the space and weight analysis were based on actual configuration of a Data and TDM solution and the IP equivalent solution. Additional weight savings is expected from a reduced amount of the associated wiring and depending on the ship configuration a reduced number of racks for the system configuration. The actual weight savings is dependant, of course, on the size of the vessel, but both weight and space would be linear and directly proportional based on the size of the ship.

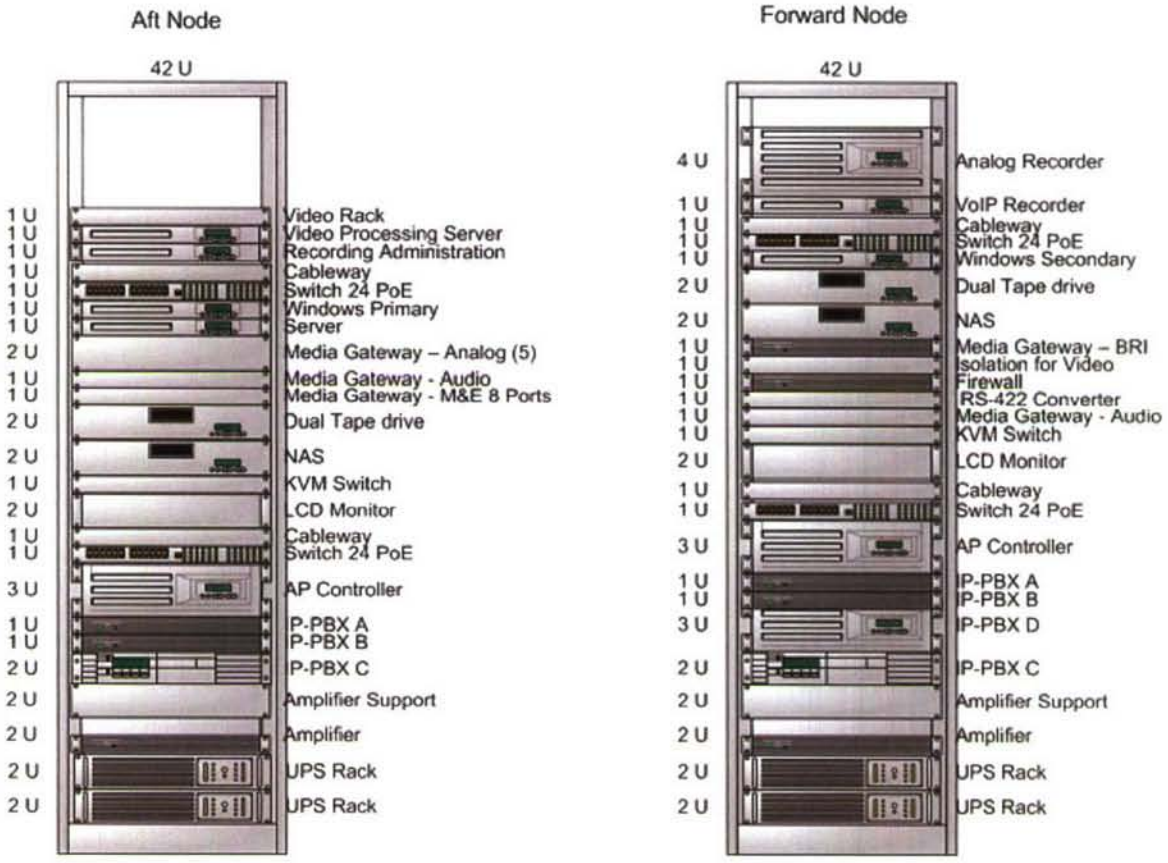


Figure 2-3. Summary of IP Implementation

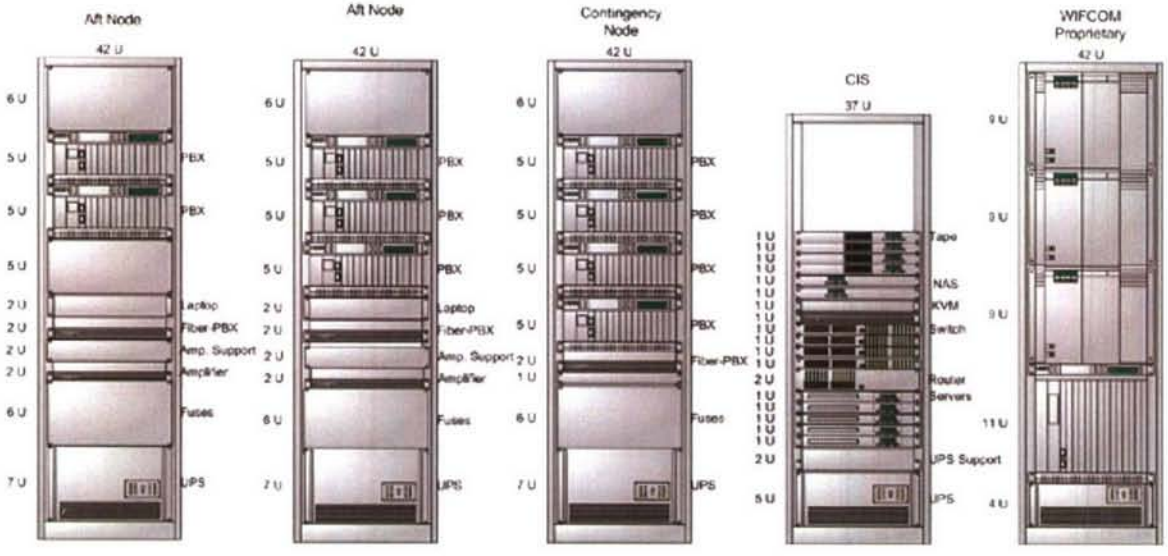


Figure 2 4. Summary of Legacy Implementation

2.4.5 Perceived Additional Benefits

Some of the areas seen having additional benefits would be in the lower manpower operational hours required since both the VoIP, Video; Data solution would be implemented on the same infrastructure system. This would require less training for personnel to support the integrated solution VoIP, Video, Data implementations and also for lower ongoing maintenance of the system while deployed. As part of this paper we did not do a resource study of the operational or of the anticipated maintenance savings. In addition to manpower savings with a VoIP, Video, Data system, there is also expected to be a lower requirement for spares. These operation savings were not studied as part of the technical research program.

2.4.6 Additional Functionality

With an integrated IP system VoIP, Video, Data system there will be additional functionality that is available. Since this technology is becoming widely deployed in the commercial business environment and also in the residential home market, it is anticipated that besides the cost points coming down additional product features will be continuously implemented by many companies. A number of these features are anticipated to be software upgradeable, so that as systems mature they can have the same functionality as newer systems being deployed. Some of the additional features available now or in the short term are as follows:

2.4.6.1 Communications Terminal

Additional add-in programs that can be added to the Communications Terminal on select terminals where the feature would be required are listed below:

- Manuals distribution to terminals
- Ability to view video that is stored or live feed
    - Training videos
    - Damage control live streaming video
- Built in camera
- Display important vessel information
- Support of individual user profiles on the terminals
- Display important weather information
- Display vessel calendar of events
- Voicemail delivered to the station or person at the station
- Portable ICT
    - Wireless for use on specific boats
    - Global Positioning System (GPS) to send back to track the portable unit
    - Battery powered
- Dual homed devices for more resilience

The above list shows the capability of using the Communication Terminal for other functions than just communications. Some of them assist in damage control allowing

individuals to survey a compartment without having to have individual sailors manually go from compartment to compartment or enter a hazardous condition. The ability for the sailor to get access to manuals to allow them to learn material while sitting at a station that needs to be manned, but maybe doesn't have active duties requirements all the time. The ability to allow individuals to gather information about the vessel and/or weather conditions by a press of a button converges many of the different tasks into a single device. All of these features maybe limited to one or a few Communication Terminals or to only particular individuals so they don't have to call or go to another compartment to gather or view the information. These features all need to be evaluated for feasibility for being done on the Communication Terminal, but technically there is no reason these types of features cannot be added to the Communication Terminal. The features can then be restricted by the profile that is enabled, and password protected as required.

2.4.6.2 Voicemail

With the VoIP infrastructure voicemail can be tied to an individual and not to a phone, allowing for greater flexibility for the individual sailor, and commanding officer. This would allow for each to have a mailbox customized for their individual needs. The voicemail systems are more in the realm of a unified messaging system with the different resources combined. The voicemail can be obtained from a web page or sent to the user by email.

2.4.6.3 Announcement Systems

While current IP announcement systems are not fully capable of being implemented an IP solution has inherent benefits in resilience of the IP network. The current system does not rely on a data network; it has its own wiring infrastructure. This makes it isolated from other issues on the network. By using the data network a reduction in wiring should be realized. Resiliency can be achieved by using dual homed devices connected to multiple switches in different segments of the network. Each speaker is connected to a network switch that will supply power over Ethernet (PoE) in most cases. The wiring for the speakers is much lighter. A single wire that has been damaged will not affect a full string of speakers. Also, the use of "cutout and test panels" is removed since a panel to house the speaker strings for testing is not needed. The method of testing will be performed at the network level using a network-monitoring tool. The ability to interconnect different announcement end devices and wireless phones into multiple groups depending on separate configuration profiles is anticipated to reduce some of the speakers that would be required.

2.4.6.4 Wireless

For the Wireless (WiFi) products there are a number of benefits as part of a U.S. Navy deployment.

The commercial success of WiFi and competition (primarily in residential and office environments) has lead to very cost effective equipment. The success has also driven

considerable development efforts to improve the bandwidth and signal quality of WiFi devices. Because WiFi is inexpensive and limited in range, it is common (and feasible) to have many access points to cover small areas (e.g., one access point per room or for every other room). Under good conditions (e.g., a strong signal with few users), VoIP over WiFi operates just like VoIP on a wired network.

Worldwide Interoperability for Microwave Access (WiMAX) provides significant bandwidth and coverage improvements over the other technologies. Because it was designed to support data and voice applications over a broader geographic area (approximately 20 or more miles from the beginning), it is anticipated to be a major cost effective solution in the near term. Major commercial companies from chip vendors, service providers and Fortune 100 companies are making major investments in WiMAX development and deployment. The costs are expected to come down significantly over the next two years. Because of WiMAX being a new technology, not all of its features have been proven in the field but are currently being tested by major service suppliers. The initial WiMAX applications are used primarily for point-to-point connections (similar to what is needed for ship-to-shore) or for a mobile sea operation falling within the area of coverage.

Cellular systems provide near-ubiquitous voice coverage at (or close to) toll quality. Although cellular technologies support data applications, the data rates are lower than the other technologies. The data rates, however, are constantly improving. Unlike the other data networks where voice and data compete for the same resources (e.g., a single channel), cellular systems can reserve channel resources. The limitation is the different frequency spectrums and variety of technologies. The benefit of cellular is maximized in special cases where a lot of access is required in concentrated homeport situations, such as hospital ships in port. The doctors and technical staff can readily access external communications, and simultaneously without interfering with shipboard requirements.

The above is a representative sample of some of the additional benefits that will be achieved with going to an integrated IP based system. The key point is that the commercial market has made and will continue to make major investments in IP infrastructure, especially around the integration of voice, video and data enabling continuous cost improvements and feature enhancements with higher reliable, secure, and robust deployments

2.5 *VoIP Reliability*

2.5.1 Introduction

Reliability is clearly a hot issue. But what kind of reliability does VOIP need to have? There is a key difference between simple reliability and availability. Availability relates to people's expectation of being able to use the service at any time, any day. Users expect a higher level of availability for voice services than for IT. This means no maintenance windows for upgrades, no worm or virus impacts, and no call-attempt blocking during busy hours. And once a call is made, it has to stay up, with no multi-second convergence events, and without any oversubscription/congestion effects.

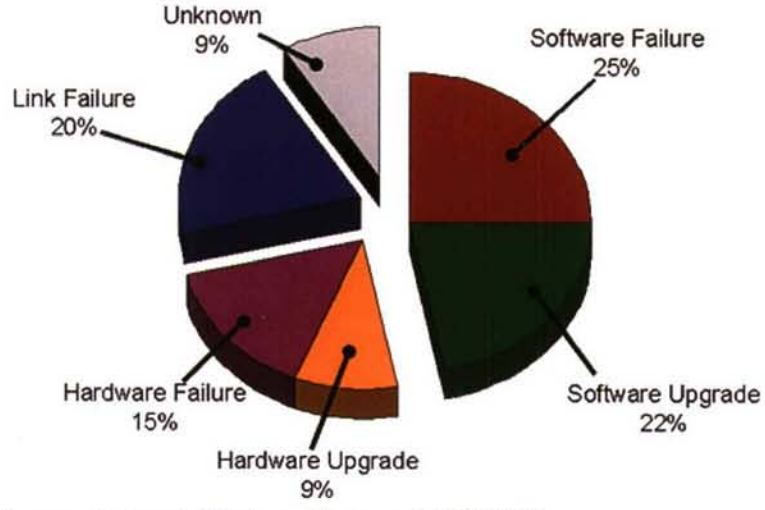
One critical step is to allow the VOIP elements to handle the possibility that the IP network may be trying to reconfigure itself in response to link or node failures, so that any network changes do not effect service. This is an important example of the difference between availability and reliability, because if the network fault is visible to the overlying equipment when the network is recovering, the service will not be available.

This is in stark contrast to legacy IT availability for services such as email or Web browsing. They have always been based on best-effort traffic with congestion/throttling inherent in the protocols, so that if there are more users than the system can handle, they get a reduced subset of the available bandwidth. This just can not happen with VOIP.

This section addresses VoIP reliability issues on a converged network and how these issues are addressed with current technologies and network architectures to achieve a highly reliable solution.

2.5.2 Sources of Failure in IP Networks

In order to adequately discuss how VoIP reliability can be improved, or for that matter, what causes it's reliability to be less the desirable, one must look at the sources of failures with the IP Network. Figure 2-5 [5] shows the types of IP network failures that can disrupt the availability of services on the network.



Source: Network Strategy Partners LLC, 2002

Figure 2-5. Analysis of Types of IP Network Failure

Doing the following will improve the reliability of a VoIP network.

1. Improve hardware and software reliability
2. Decouple the services so that *any failure* does not affect service

Table 2-3 summarizes the improvements.

Table 2-3. Improving VoIP Reliability

Improvement	**Meaning**
Improve hardware and software reliability:	This means hardware redundancy, software/protocol redundancy, link-layer resiliency, and path protection. Vitally, the links between network elements have to be hardened and protected, and this means going a step beyond basic, link-by-link protection and looking at rapid, end-to-end path protection.
Decouple the services so that *any failure* does not affect service:	The softswitches and media gateways have to be able to ignore the fact that the network may be frantically reconfiguring. Any changes that happen to the hardware, software, or protocols must not affect services. VLAN's are applicable here to separate real-time services such as VoIP from data services in order to improve the quality of service for Voice traffic.

2.5.3 Reliability Related Technologies

There is a range of technologies and initiatives now at hand to help reach desired reliability for VoIP. Table 2-4 roughly aligns some of the key technologies for improving reliability with the layers of the OSI protocol stack at which they operate. In terms of protection, some of these mechanisms provide protection for just links and some protect both link and node, and the line is somewhat blurred today. For example, a router can be configured so that, if it fails, a link protection mechanism switches over to a backup router. The following sections describe in more detail the technologies summarized in Table 2-4.

Table 2-4. Key Technologies for Improving Reliability, Roughly Aligned With Layers of OSI Protocol Stack

Location	Technology
Software & Protocol	Virtual Router Redundancy Protocol (VRRP)
Layer 3	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Multi Protocol Label Switching (MPLS) Fast Reroute
Layer 2	Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), Resilient Packet Ring (RPR), Link Aggregation, VLAN
Hardware	Redundant power supplies, fans, fabric, control modules, line modules, etc…

2.5.3.1 Software and Protocol

The IETF's Virtual Router Redundancy Protocol (VRRP) sounds as if it should solve a lot of reliability issues in the upper regions of the OSI stack, but in reality it is much more modest, being basically for host redundancy as a default router. It provides dynamic failover in forwarding responsibility to an elected substitute router should the designated master VRRP router become unavailable. Nevertheless, this is useful for VOIP because a lot of VOIP infrastructure uses gateways, which are actually hosts. VRRP is a fairly slow protection mechanism, at least for the automatic protection failure part, and takes about 3 seconds or more to operate. There is an Internet Draft *draft-ietf-vrrp-ipv6-spec-06.txt* from Hinden that extends VRRP to IPv6. [5]

2.5.3.2 Layer 3

At Layer 3 the key IP/MPLS work is progressing very fast, and a lot has been done on vendor interoperability tests for fast rerouting, including sub-50 ms tests of vendor bypass and detour fast reroute. The key protocol is MPLS Fast Reroute, which aims to provide fast, sub-50 ms link and node protection by using, at least initially, a combination of MPLS traffic-engineering, label-switch paths and established routing protocols such as IS-IS and OSPF. An issue with these routing protocols is that they converge more slowly as the network topology grows, and some vendors are looking at ways to speed up convergence. The current Internet Draft *draft-ietf-mpls-rsvp-lsp-fastreroute-05.txt* by Vasseur and others extends RSVP to establish backup Label-Switch Path (LSP) tunnels for the local repair of LSP tunnels, especially for real-time applications such as VOIP.

The technique is fast because it computes and signals backup LSP tunnels in advance of failure, and redirects traffic as close to the failure point as possible, thus avoiding any path computation or signaling delays, including delays to propagate failure notification between label-switch routers (LSRs).

2.5.3.3 Layer 2

At Layer 2 are various Ethernet technologies, such as Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Link Aggregation, which are all being used for hardware-link and software reliability. Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) are used for enabling loop free topologies with sub-second restoration in case of edge failure.

VLANs are implemented within a network design for load balancing network traffic between the applications and to improve resiliency. VoIP traffic is routed over its own VLAN to keep it away from the data traffic going to and from the servers (which are on there own VLAN). This will improve the quality of the voice communication (reduced voice-jitter) and contributes to a more reliable voice connection.

2.5.3.4 Hardware

At the bottom are basic hardware reliability enhancements such as redundant power supplies and fabric control modules that are now built into a lot of carrier-class MPLS devices. The user devices can also be multi-homed if there is a need for protection from single failures. The topology can be extended to multi-star (e.g., 3-star) with triple homing if there are requirements for protection from double failures, or better load balancing of traffic. In general, this will provide better reliability. However, the trade-off will be in terms of added links, complexity in configuration maintenance, and operations. It needs to be assessed through simulation and testing if this adds to the restoration time for failure recovery.

To address network service availability issues, the distributed-star and mesh topologies are chosen which provides the most connectivity by interconnecting the edge switches through multiple core routers. In this case all the edges are meshed then each edge is only one hop away from each other. This provides better performance, especially for peer-to-peer traffic (like VoIP) and provides alternate paths between source and destination for VoIP traffic in the event of a core router failure.

2.5.4 VoIP Network Infrastructure

In order to provide the reliability/availability required of VoIP applications, the infrastructure must be redundant, robust and quickly adaptable to changes. The solution that best meets the criteria is depicted in Figure 2-6. This infrastructure is flexible and can be enhanced (dual-homing, triple-homing, etc…) to improve reliability even further. As with any Network design, Network analysis needs to be done with automated test programs to create and validate the design and make adjustments, if necessary, to achieve the level of reliability required.

The edge switches are connected to core switches in a meshed topology in a way that the number of hops between edge networks is optimized. The core switch connection is by way of two 1 Gigabit multimode fibers, which provide a high-speed, redundant link to the network backbone (and thus the servers). The core switches are interconnected in a mesh configuration to provide load balancing for increased performance and also to increase the resiliency of the network in the event that one of the core switches fail. The connection between core switches is 10 Gigabit multimode fibers, which provide ample bandwidth for even the most demanding of applications (i.e. VoIP and Video).

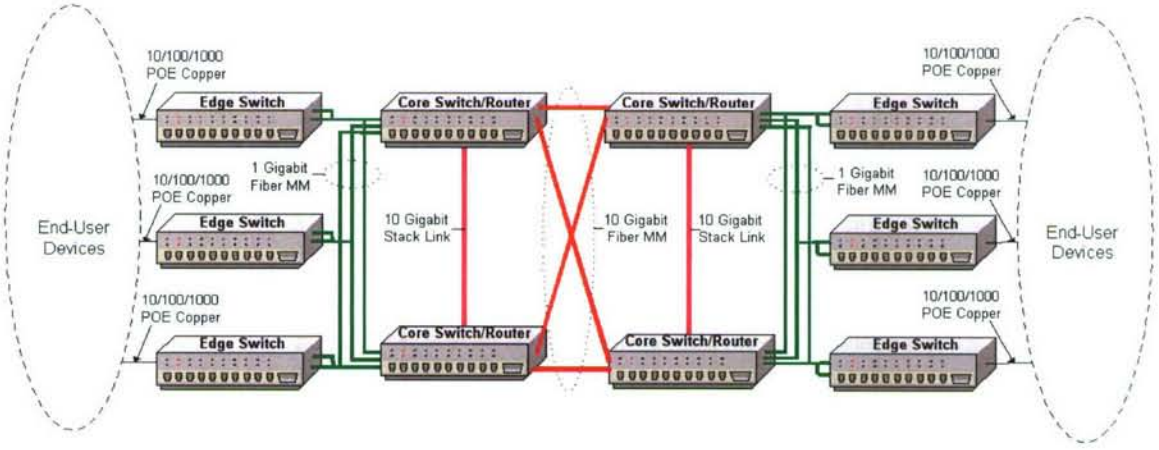


Figure 2-6. Network Diagram

VLANs are implemented within the network design for load balancing network traffic between the applications. VoIP traffic is routed over its own VLAN to keep it away from the data traffic going to and from the servers (which are on there own VLAN). This will improve the quality of the voice communication (reduced voice-jitter). Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) are used for enabling loop free topologies with sub-second restoration in case of edge failure. Additional VLANs may be implemented on an as-needed basis.

2.5.5 Conclusion

Network reliability must be built into the network design at all levels of the infrastructure. The hardware (switches, routers, gateways, etc…) should be highly reliable and robust. Hardware should also possess redundancy (power supply, fans, etc…) to eliminate single points of failure. The network topology (distributed-star and mesh) will provide a network architecture that is self-healing in the event of a network component failure.

Fail over strategies are desirable for cases when network devices malfunction or links are broken. An important strategy is to deploy redundant links between network devices and/or to deploy redundant equipment. IP networks use routing protocols to exchange routing information. As part of their operation, routing protocols monitor the status of interconnecting links. Routing protocols typically detect and reroute packets around a failure if an alternate path exists. Depending on the interconnecting media used for these links, the time taken to detect and recalculate an alternate path can vary.

Having media gateways and media gateway controllers that can actively detect the status of their next-hop address (default gateway) as part of their failover mechanism decreases the likelihood of a large service disruption. Another possible option is that the media gateway and media gateway controller could be directly connected to the router. In this case, the possibility of a link failure (depending on the nature of the failure) could be immediately detected and the network devices would take appropriate action. Still another option for reducing long-term failure could be to employ a redundancy mechanism such as the Virtual Router Redundancy Protocol (VRRP).

On top of a robust hardware platform is layered the software and protocols such as VRRP, STP, and RSTP necessary to respond to changing network conditions whereby automatically selecting an alternate path without any perceivable interruption of service. Through the application of VLANs within the network design one can load balance the network traffic between the applications and also improve resiliency.

The standard practice for a data network relies on redundancy of equipment and connections between the hardware with very high levels of reliability and availability. Just adding equipment and network connections between switches and routers will not always result in a faster recovery time and more stability solution. Network analysis needs to be done with automated test programs like OPNet's SPGuru® to create and validate the design before it is purchased and installed.

2.6 *VoIP Alternate Network Topologies*

2.6.1 Introduction

Advances in computer network technologies and industry trends are transforming how the Navy should best deploy their information systems. In the past, use of separate networks for different functions was acceptable and sometimes advantageous for security. Today, the Navy can derive cost benefits by adding Voice over IP (VoIP) capabilities to existing communication networks. The cost savings materialize by reusing the core network infrastructure for different network functions. The telephony and data networks are examples of networks that have been disparate in the past. The use of VoIP allows convergence of voice and data networks. The maturity of today's cryptographic systems allows classified data to be encrypted and transmitted over unsecured networks.

IP telephony (IPT) systems are replacing legacy PBX systems in both government and enterprises due to expectations of cost and feature advantages. It is important that taking advantage of these benefits does not put sensitive information and mission continuity at risk. It is also imperative that U.S. Navy carefully considers the security implications of deploying IP telephony systems. While IP telephony systems can be secured, doing so requires careful evaluation, detailed planning, measured deployment, continuous testing, and vigilant maintenance. [6]

2.6.2 Background

IP telephony systems are considered to be any primary voice communication system, which uses an IP network as the underlying transport for signaling and media. An IP telephony system that is replacing an existing legacy PBX system would fall into this category. The primary goal of this architecture is to supply highly reliable, available, and secure unclassified voice services. IP telephony also creates an opportunity to use applications that were not possible or convenient with legacy systems. While this architecture does make provisions for using these applications, such use is a secondary goal. [6]

The tremendous growth of the IP-based technologies for data applications over the last decade has resulted in a cost effective system for moving data between remote hosts. Due to the value of the transmitted data, customers have invested many billions of dollars into this infrastructure. The growing investments in IP technologies and the sluggish growth of traditional telephony systems have progressed to the point where it is less expensive to run telephony services over an IP infrastructure than to use traditional TDM-based systems. Furthermore, integration with IP enables new services, such as click-to-dial (where a user can "dial" another party from a web page link) or unified communications (which can combine voice mail, e-mail, instant messaging, etc.).

VoIP provides telephony services over an IP network such as the Internet. VoIP base services utilize the existing data network instead of relying on traditional TDM-based telephony technologies such as T1, Primary Rate Interface (PRI), Common Associated Signaling (CAS) or System Signaling #7 (SS7). The topology of VoIP networks can be very different from TDM systems because IP links are independent of the physical location of the servers, whereas TDM systems usually have a dedicated physical link between each adjacent pair of servers.

2.6.3 Why Migrate to VoIP?

The first reason would be that all major common carriers and telecommunications switch vendors plan to migrate to VoIP. As they migrate, their support to circuit switches will diminish. Secondly, the same component concepts that make up the TDM Defense Switched Network (DSN)/ Public Switched Telephone Network (PSTN) are also found in VoIP environments. The last reason is the cost savings derived by not having separate networks and separate sets of network equipment.

Regardless of the vendor solution or architecture selected, certain VoIP components exist for normal operation. These four major components are:

- The IP network
- Call processor/controllers
- Media/signaling gateways
- Subscriber terminals (End Instruments EI's)

2.6.4 Security

IP telephony security should be tailored to the specific threat environment. Doing this successfully requires developing a security policy which specifies the importance of the information to be protected and defines what security mechanisms are needed to adequately protect that information. Securing IP telephony also requires developing a deployment plan, which does not leave the IP telephony system vulnerable before it is completely deployed. [6]

A defense-in-depth approach is required to protect the many components of IP telephony systems. Defenses should be deployed in the network, at the network perimeter, within the IP telephony applications, and in all IP telephony end points. Network security mechanisms limit attacker access to crucial IP telephony services, prevent impersonation of network hosts by insiders, make eavesdropping on calls more difficult, and help ensure availability of service. Perimeter security controls keep unauthorized users from accessing the internal network and ensure both Public Switched Telephone Network (PSTN) and voice over IP (VoIP) connections to the outside do not compromise the network. Authentication and encryption in the application-layer prevent eavesdropping and impersonation of IP telephony end points. Finally, security hardening of end points and servers reduces vulnerabilities and limits extraneous functionality. [6]

2.6.4.1 VoIP Component Architecture

VoIP architecture consists of Telephony Servers, Data Service Servers, End-Instruments (IP Phones, Soft Phones, etc.) and network switching equipment. Each class of equipment provides unique services to the end user. The following Figure 2-7 depicts a typical non-converged (IP Calls only) VoIP architecture. This example does not include redundancy and assumes a single level of security.

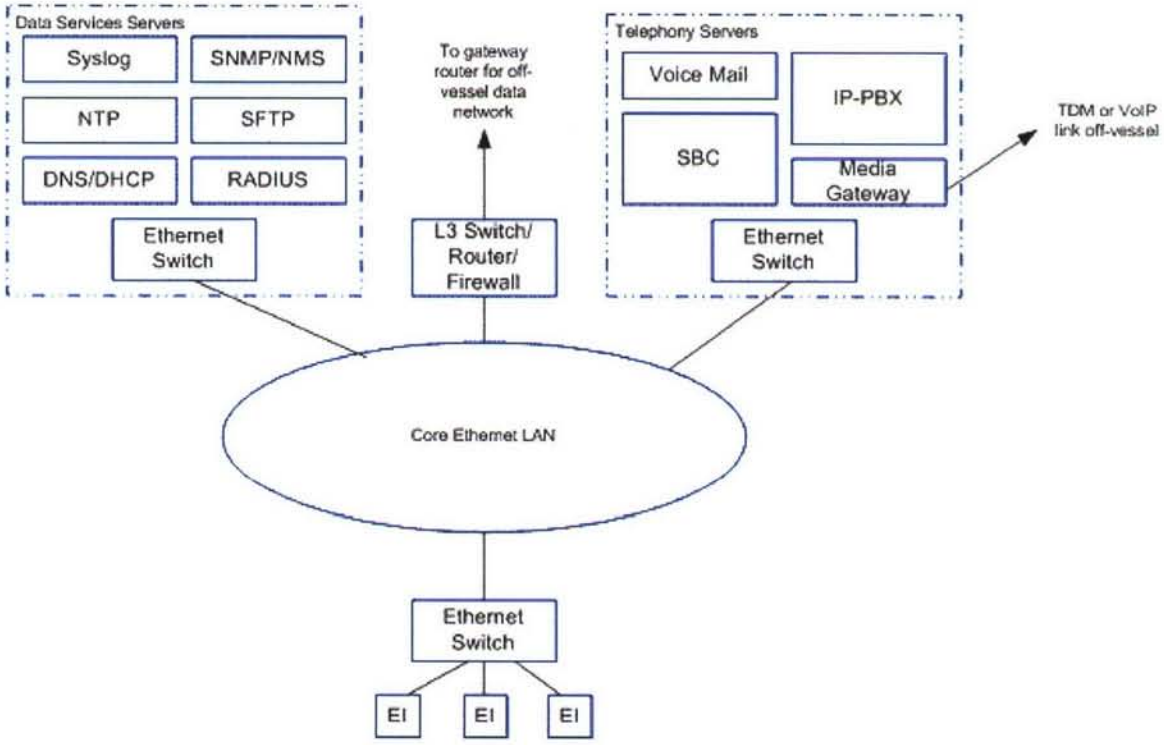


Figure 2-7. VoIP Architecture (Non-Converged)

The telephony servers are a collection of servers providing the telephony application. Although the servers are generally distinct devices, it is possible for a single device to integrate multiple services (e.g., an IP-PBX could include an integrated voice mail service). The IP-PBX provides services similar to what one would expect from a traditional PBX. Its primary functions include registering endpoints, processing call control messages (e.g., call forwarding, call transfer, do-not-disturb, supervised transfer, hotline routing), and billing (e.g., generating Call Detail Records (CDR). Operations, Administration, Maintenance, and Provisioning (OAM&P) functions of the IP-PBX typically use a northbound interface (i.e., one that is separate from the network interface to the production network). This architecture assumes that all administrative IP-PBX functions are performed from a direct physical connection to the IP-PBX. Conversely an administrative VLAN can be designed into the network to perform out-of-band administrative functions. Four VoIP network convergence options are considered. The options range from completely separate VoIP networks per security level to a single converged network that supports multiple security level VoIP calls and data.

2.6.5 Network Option 1

In Network Option 1 secured and non-secured communications are handled on separate networks and separate end devices.

Network Option 1 uses separate networks for unclassified VoIP, classified VoIP, and network data. This scenario reflects the present mode of operation, but uses VoIP networks instead of traditional TDM networks.

Figure 2-8 shows a diagram of Network Option 1. The blue (unclassified) and red (classified) networks are identical. The "Data Services" box contains the various servers that the VoIP servers and EIs depend upon. The VoIP servers are shown individually within the dashed line. The black lines connect devices to the vessel-wide LAN.

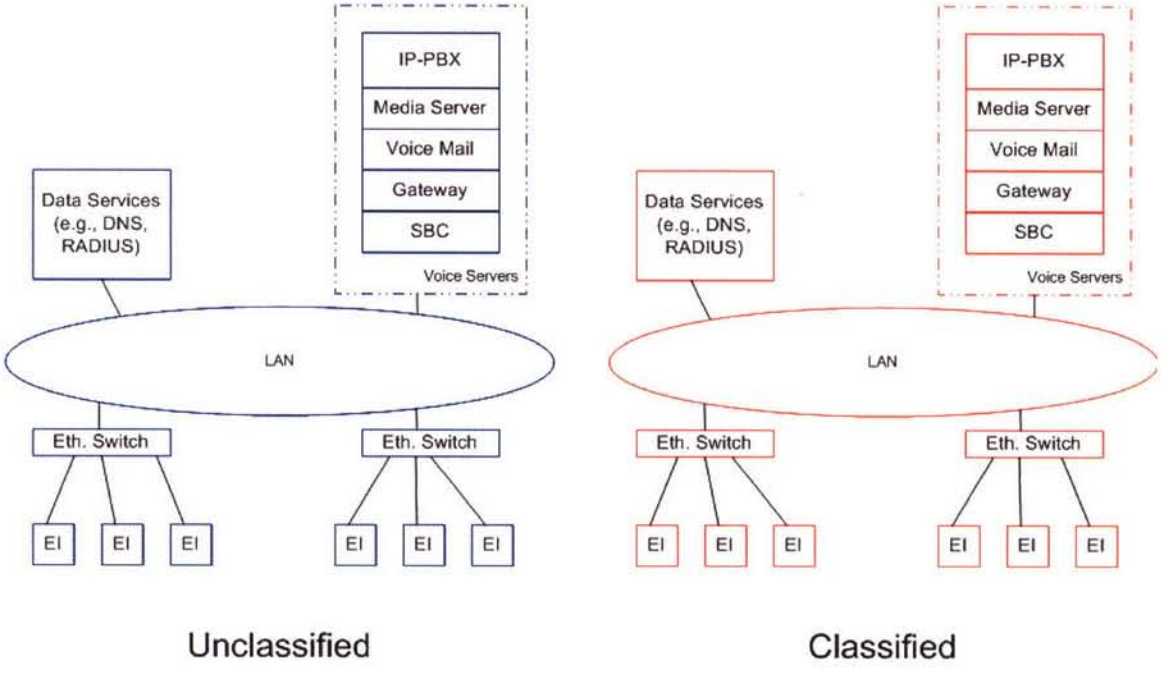


Figure 2-8. IP Network Option 1 Separate Networks

This scenario is the most expensive because each security level needs its own equipment. IP Network Option 1 is very secure because the infrastructure for the classified voice network is secured and it is physically separate from that of the unclassified network voice and data networks. Denial of Service attacks is still a lingering issue with any VoIP network. VoIP security must be implemented at multiple levels to ensure maximum network uptime.

2.6.6 Network Option 2

In Network Option 2 secured and non-secured communications are handled on separate networks, but are connected at the end devices.

This scenario is similar to Network Option 1, except at the End Instruments (EIs). Secure EIs connect to both the classified and unclassified networks. This enables a single secure EI device to make calls to classified and unclassified EIs. A Secured Terminal Equipment (STE) provides similar functionality in today's TDM network. The scenario uses separate PBXs for classified and for unclassified communications. All provisioning of the EI would be done at the highest security level it supports. For example, the EI's boot server would be on the classified network rather than the unclassified network. The EI would need to pass the standard IT accreditation process to mitigate basic threats that might lead to data leaking from one network to another. Figure 2-9 depicts the classified EI's connected to both classified and unclassified switches.

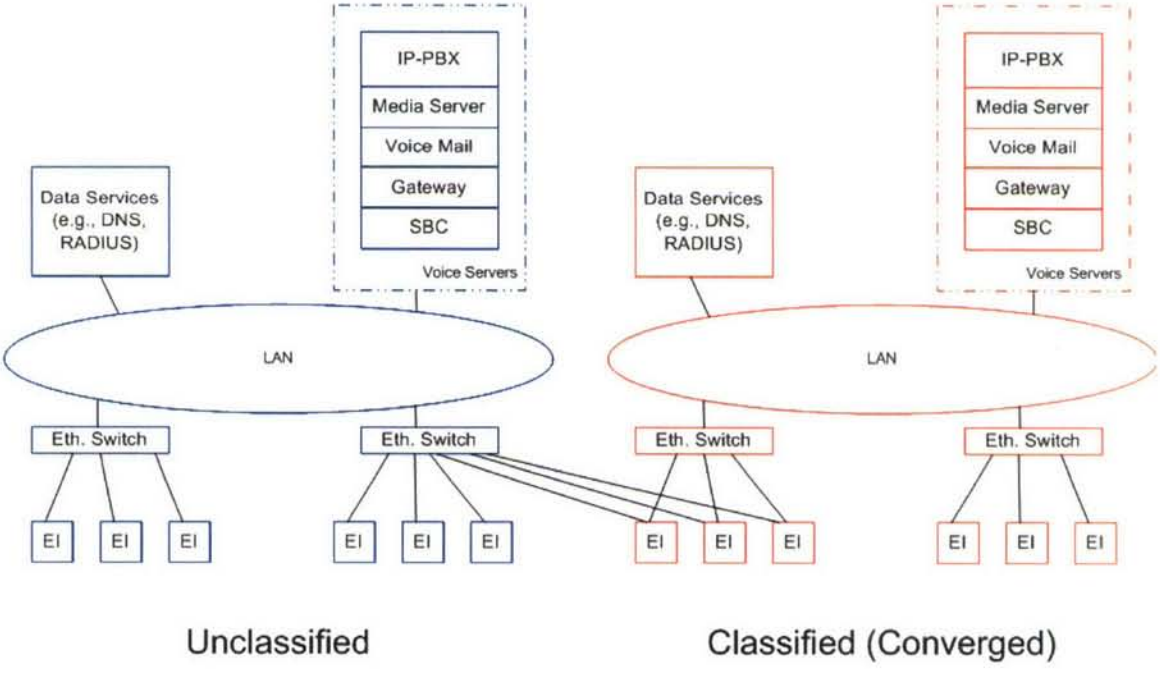


Figure 2-9. IP Network Option 2 - Converged End Instruments (EIs)

This option provides some cost savings over Network Option 1 because EIs (including expensive video terminals) are reused and provides a small improvement in usability because a user who needs to make both classified and unclassified calls can do so from a single EI. Unlike in Network Option 1, there is a concern about potential information exchange between the classified and unclassified networks because the EI spans both. Security architectures are necessary to address this concern, as is an accreditation process to ensure that the EIs have adequate safeguards to handle the convergence. A well-defined security plan must be applied to this approach to limit potential security breaches or denial of service attacks.

2.6.7 Network Option 3

In Network Option 3 all voice communications are on the same VoIP network (Classified and Unclassified) but normal network data is on a separate network.

Network Option 3 converges the network infrastructure of the VoIP network such that the classified and unclassified VoIP traffic use the same set of switches and routers. Network Option 2 demonstrates that secure EIs are capable of operating at multiple security levels. In Network Option 3, Separate PBXs handle classified and unclassified communications.

Figure 4 shows Network Option 3, which has a single (unclassified) vessel-wide LAN connecting the switches and server blocks. Each security level uses a different VLAN (not shown in the diagram). Figure 2-10 shows two connections from each converged EI: one connected to a classified switch port and one connected to an unclassified switch port. Alternatively, the EI could be configured to set the VLAN tag for the appropriate VLAN, instead of configuring the switch port. Use of separate physical connections is consistent with a migration path that reuses the converged EI from Network Option 2.

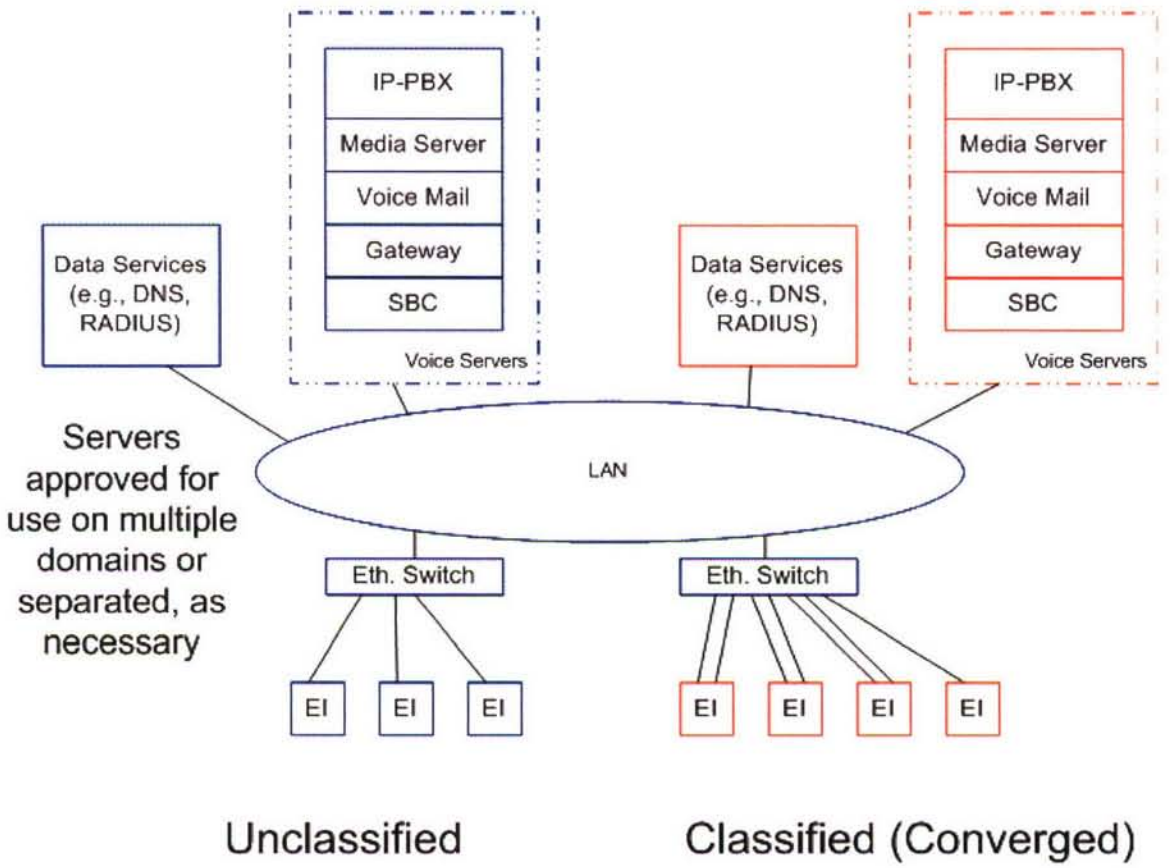


Figure 2-10. IP Network Option 3 - Converged Voice Networks

Note that the converged EIs could be configured with a single link to the Ethernet switch instead of being dual-homed. In that case, the EIs would be responsible for applying the

VLAN tag on every packet. The reason for showing dual-homed EIs is to suggest a migration path from Network Option 2, where each EI had dual-homed interfaces connected to separate switches.

This scenario provides considerable cost savings by requiring only a single network infrastructure for VoIP instead of the two networks needed in the previous network options. This option raises questions about the security level at which the converged LAN is managed. It is unlikely that the access switches and all links in the LAN can meet the physical requirements necessary to operate at the secret or top-secret level. In particular, physical constraints on the vessel may make it prohibitively expensive to physically secure the network links in switch closets. We assume that the LAN will operate as an unclassified network with non-cleared administrators. Operations such as granting VLAN membership connecting classified networks and configuring parameters for switch-port authentication would be done at the unclassified level. With the network infrastructure operating at the unclassified level, the VoIP service must rely on the built in security architecture. The security architecture must implement security at the switch port level as well as implementing secure voice VLAN tags for each secure EI to connect to. The EI must also adopt security measures to conceal network configuration data as well as locking any unused data ports. Additionally, the switch must adhere to a strict Port Authentication policy that only allows specifically configured EI's to gain access. At each level security must be addressed. Lastly, the voice data itself should be encrypted to ensure that classified voice traffic is not compromised.

2.6.8 Network Option 4

In Network Option 4 all voice and data communications exist on the same backbone network. Classified and Unclassified voice traffic coexists with data on the same core network infrastructure.

This Option depicts dual-homed EIs (see Figure 2-11). It is also possible to have a single-homed EI that applies its own VLAN tag. We assume that the data network uses a system of VPN gateways (e.g., High Assurance Internet Protocol Encryptor (HAIPE)) to interconnect sets of classified edge subnets and simple VLANS to segregate the unclassified data traffic. Given that the networks contain legacy applications that cannot provide their own security, this may be the only reasonable option to connect such systems.

One approach to securing the VoIP network would be to reuse the same technologies used in the data network to secure arbitrary applications. In essence, that approach would treat the entire VoIP network as a single "data" application.

Instead, assume that the VoIP network is secured independently from the data network and that the VoIP network uses the same architecture options as in the other three options.

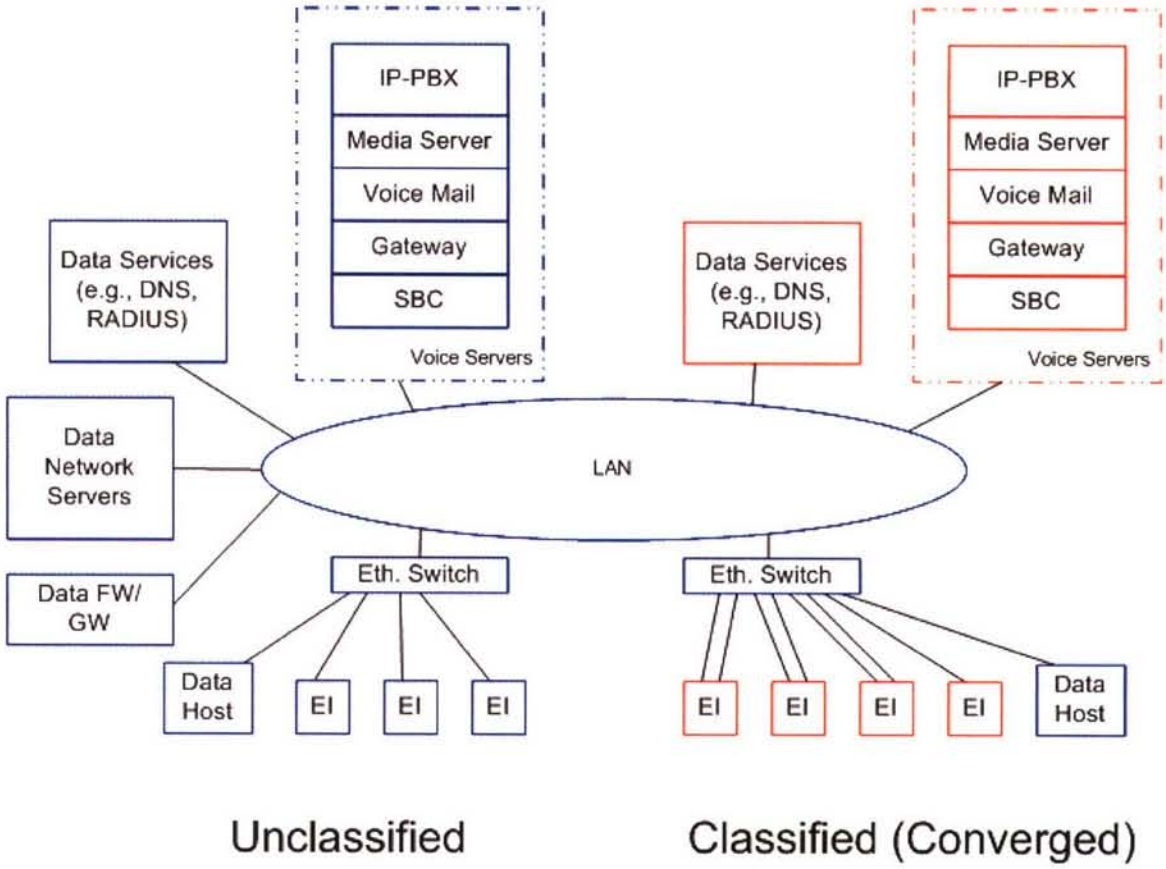


Figure 2-11. Network Option 4 Full Voice and Data Convergence

This option represents further cost savings over the previous options because the VoIP and data networks share a single network infrastructure. Further savings are possible by reusing network services, such as NTP and RADIUS, between the data and VoIP networks. The convergence may also facilitate new functionality, such as multimedia collaboration.

As stated in Option 3, the VoIP service must rely on the built in security architecture. The security architecture must implement security at the network switch; the individual switch ports as well as implementing secure voice VLAN tags for each secure EI to connect to. The EI must also adopt security measures to conceal network configuration data as well as locking any unused data ports. Additionally, the switch must adhere to a strict Port Authentication policy that only allows specifically configured EI's to gain access. At each level security must be addressed. Lastly, the voice data itself should be encrypted to ensure that classified voice traffic is not compromised.

Grouping voice and data elements together in a converged backbone is a challenging task when it comes to security. NSA's Systems and Network Attack Center has provides a recommended IP Telephony (IPT) network architecture. Figure 2-12 depicts this architecture. [6]

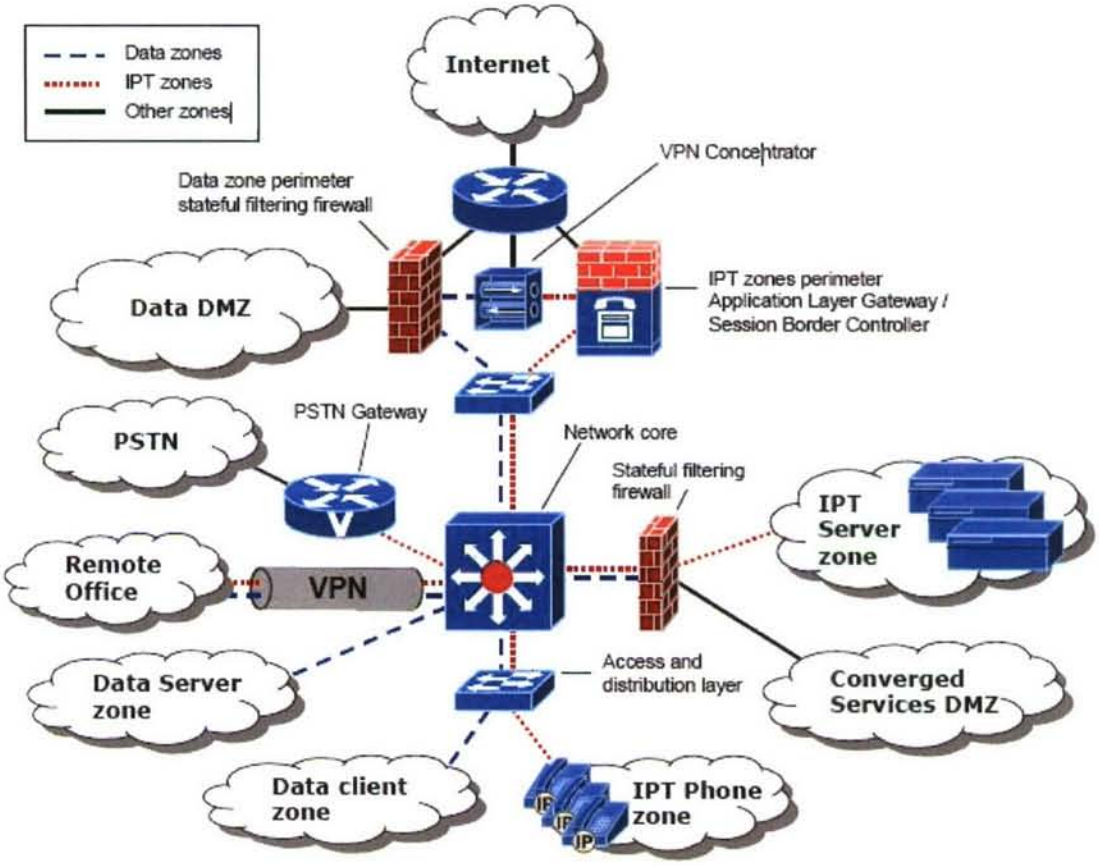


Figure 2-12. NSA Recommended IP Telephony Architecture

NSA recommends that the network be divided into multiple security zones. A security zone contains a common set of devices that need similar protections. It controls access to these devices from the rest of the network by allowing only authorized hosts and protocols access to the security zone. More in-depth information about designing a secure VoIP network can be found in reference [6].

2.6.9 Conclusion

This discussion presents four different implementations for handling classified and unclassified VoIP voice traffic. Each network option addresses choices for handling classified calls however each option is still exposed to some security risk. Security with respect to classified and unclassified can be somewhat mitigated with encryption. However, denial of service, IP snooping and theft of service all present problems with the disruption of voice communications. It does not matter if the call is classified or unclassified when the network is bogged down by one of the aforementioned threats. Regardless which network option is chosen, a well-designed security plan must be established and implemented to both the data and voice networks as a whole.

References [7] and [8] provide excellent Security Technical Implementation Guides {STIGs) created for the Department of Defense (DOD) by Defense Information Systems Agency (DISA). References [6] and [5] provide the recommended IP Telephony Architecture and Security Guidance for Deploying IP Telephony systems from the National Security Agency. The combination of the four mentioned references provides excellent guidelines for designing and deploying a secure converged network.

2.7 *Network Summary*

2.7.1 Topologies

This section summarizes the following network topologies and discusses their suitability to support multiple services (VoIP, video, and data) over an IP network.

- Bus
- Ring
- Tree
- Star/Distributed Star
- Mesh/Partial Mesh

The key metrics used in our analysis are resiliency of application flows to failures, voice jitter and video end-to-end delay. The bus, ring, and tree topologies were reviewed, but due to limitations of these designs, as summarized in the following paragraphs, they were not considered to be suitable solutions and therefore no further analysis was performed on them.

2.7.1.1 Bus

The bus topology is contention-constrained because of multiple applications and different user communities competing for time on a single transmission medium. It is also not well suited for reasons of scalability.

2.7.1.2 Ring

In ring topology each device has exactly two neighbors and messages travel in one direction until it reaches the intended destination. The ring topology suits well in areas of directional communication among devices, which is not the case here. It is also not well suited for reasons of scalability and performance.

2.7.1.3 Tree

The tree topology was considered as a possible candidate as it supports the client-server and computing-cluster types of application flow models and because it suits applications that require communication and interaction with multiple servers attached to different edge hubs. However, the tree topology is primarily architected for reasons of geographic conformity with user communities as in cable networks. If some of the nodes in the tree's trunk require higher levels of interconnection due to traffic flow requirements, the tree essentially becomes a partial mesh topology.

2.7.1.4 Star

The basic single-star topology features a hub and spoke architecture and is suitable for client-server applications and traffic flows. Depending on performance and reliability requirements, multiple hubs and multi-homing of the edges to the hubs can result in a highly robust and well performing network. The disadvantage of star topologies is that when the hub fails all devices attached to the hub are affected. The distributed star topology with hub backups solves that issue to a large extent.

2.7.1.5 Mesh

Mesh networks provide the most connectivity by interconnecting the nodes directly. If all the edges are meshed then each edge is only one hop away from each other. This provides better performance, especially for peer-to-peer traffic (like VoIP), since traffic between edge switches does not have to pass through the core routers. The trade-offs will be in terms of added links and the complexity in configuration when adding nodes. In most network designs, depending on the performance requirements (e.g., maximum number of hops, latency, jitter, network reliability) instead of a full mesh a partial mesh suffices.

2.7.2 Conclusion

In conclusion, both the distributed-star and the mesh/partial mesh topologies are suitable to support the assumed traffic load from the given applications. In both topologies, deploying VLANs load balances the traffic, and greatly reduces the effect of failures on application flows. This load balancing also reduces in half the traffic on the links to the video server. Thus, VLANs are very beneficial to the survivability and utilization of the network.

In the meshed topology a separate VLAN for VoIP will balance traffic by keeping VoIP traffic away from the traffic flowing to the servers. In the 2-star network, a separate VoIP VLAN would be of little benefit, since all traffic must flow through the core routers. Hence, the mesh topology is better for distributing and balancing traffic, especially if there is peer-to-peer traffic in the network, like VoIP.

2.8 *Infrastructure Summary*

2.8.1 Overview

The proposed network infrastructure consists of end devices that are star-connected (dual-star) to edge switches and the edge switches are connected in a mesh configuration. The degree of meshing is based on the traffic flow and performance requirements. Two of the edge switches are switch/routers that are dual-homed to central servers. This design is well suited to support peer-to-peer applications like VoIP. This connection pattern is chosen so that every edge switch is no more than two hops from every other edge switch. The interface among the edge switches and core switch/routers is Gigabit Ethernet.

Both the dual-star and the mesh/partial mesh topologies can support the assumed traffic load from the given applications (VoIP, Video, and Data). In both cases, additionally, resiliency techniques such as implementing Virtual Router Redundancy Protocol (VRRP) should be utilized for the routers.

2.8.2 Network Switch Requirements

2.8.2.1 Common Requirements

- Supports IPv6
- Configurable via a local console and also through a Web interface.
- Supports 10/100/1000BaseT Ethernet
- Implements Auto sensing 10/100/1000BASE-T ports
- Implements CoS with IP precedence
- Supports 802.1q (VLAN Tagging)
- Performs layer 2 and layer 3 switching

2.8.2.2 Edge Switches and Switches/Routers

In addition to the common switch requirements described in section 2.8.2.1, the following requirements are also required for the edge switches.

- Implements the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP)
- Supports 10/100/1000BaseX Ethernet (Fiber)
- Supports Power-over-Ethernet (PoE)
- Supports routing protocols VRRP, RIP, and OSPF
- Supports multicast routing protocols (IGMP and DVMRP)

2.8.2.3 Core Switch

No additional requirements beyond those stated in section 2.8.2.1.

2.8.2.4 Supporting Switches

No additional requirements beyond those stated in section 2.8.2.1.

2.8.3 Network Switch Management

Managing the configuration of network switches can be a daunting task on medium to large scale networks. A means of centrallized management is a neccessity.

Listed below are management features typically found in a managed switch:

- Turning on and off some particular port range
- Setting link speed and duplex mode
- Setting port priority
- Filtering MAC addresses - and other types of "port security" features which prevent MAC flooding
- Use of Spanning Tree Protocol (STP)
- SNMP monitoring of device and link health
- Port mirroring (also named: Port monitoring, spanning port, Switched Port Analyzer (SPAN) port, Roving Analysis Port, link mode port)
- Link aggregation (also called: bonding/trunking)
- Setting and managing VLAN configurations.
- 802.1X Network access control

The switch should also provide a serial console to allow the administrator to configure the switch in the event that the switch is not reachable remotely. Management through a command-line interface via telnet and ssh, as well as management via SNMP should also be supported. More recent devices also provide a web interface. Limited functions, such as a complete reset by pushing buttons on the switch are usually also provided.

2.8.4 VLANs

VLANs are used to load balance traffic and improve application performance. This is accomplished by keeping VoIP traffic away from the traffic flowing to the servers. The choices for VLAN design are port-based, MAC-based, or protocol-based. A port-based design is typically used since MAC-based and protocol-based VLANs are difficult to administer because of the necessity to install MAC address tables, or protocol policies on each switch.

VLANs are very useful and needed in order to optimize load balancing across the critical node(s) so that a failure at the critical node does not disrupt all or most of the traffic.

2.8.5 Protocols

This section summarizes the Layer 2 and Layer 3 network protocols used on an IP based network. This section does not include the security protocols, such as IPSec or Layer 4 through 7 protocols (with the exception of SNMP).

2.8.5.1 Routing Protocols

2.8.5.1.1 VRRP

The Virtual Router Redundancy Protocol (VRRP) is used to add additional resiliency to increase the availability of the routers servicing hosts on the same subnet. This increased reliability is achieved by advertising a "virtual router" (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router.

2.8.5.1.2 RIP

The Routing Information Protocol (RIP) is used by routers to dynamically adapt to changes of network connections by communicating information about which networks each router can reach and how far away those networks are.

2.8.5.1.3 OSPF

The Open Shortest Path First (OSPF) protocol is a hierarchical interior gateway protocol (IGP) for routing IP packets. OSPF uses path cost as its basic routing metric. In practice, it is determined by the speed (bandwidth) of the interface addressing the given route, although that tends to need network-specific scaling factors.

2.8.5.2 Spanning Tree Protocols

2.8.5.2.1 STP

The Spanning Tree Protocol (STP), creates a spanning tree within a mesh network of connected Layer-2 switches, and disables the links which are not part of that tree, leaving a single active path between any two network nodes. The purpose of this is create a loop-free infrustructure within the mehed network.

2.8.5.2.2 RSTP

This protocol provides for faster spanning tree convergence after a topology change.

2.8.5.2.3 MSTP & PVST

A VLAN design requires replacing the single spanning tree (running RSTP) with multiple spanning trees (running MSTP or per-VLAN Spanning Tree (PVST)) in order to improve the performance and resiliency of the network and applications. These protocols are used for enabling loop free topologies with sub-second restoration in case of edge switch failure, switchover, or the addition of switches.

2.8.5.3 Network Management Protocols

2.8.5.3.1 SNMP

Simple Network Management Protocol (SNMP) is used as the transport protocol for network management. Network management consists of network management stations communicating with network elements such as hosts, routers, servers, or printers. The agent is the software on the network element (host, router, printer) that runs the network management software. The agent stores information in a management information base (MIB). Management software polls the various network devices and gets the information stored in the MIB.

2.8.5.4 Network Supporting Protocols

2.8.5.4.1 ARP

The Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address when only its IP address is known.

2.8.5.4.2 ICMP

The Internet Control Message Protoc (ICMP) is one of the core protocols of the Internet protocol suite. It is mainly used by networked computers operating systems to send error messages indicating, for instance, that a requested service is not available or that a host or router could not be reached.

2.8.6 Multicast

To support functionality required by, for example, an announcing system, IP Multicasting is needed to handle the many-to-many communications over an IP infrastructure. It scales to a larger receiver population by not requiring prior knowledge of who or how many receivers there are. Multicast utilizes network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. The nodes in the network take care of replicating the packet to reach multiple receivers only where necessary.

2.8.7 VPN

A virtual private network (VPN) is a communications network tunneled through another network, and dedicated for a specific network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

2.8.8 Network Management

Network management refers to the maintenance and administration of large-scale computer networks and telecommunications networks at the top level. Network management is the execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network, including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, bandwidth management, and and accounting management.

Data for network management is collected through several mechanisms, including agents installed on the infrastructure, synthetic monitoring that simulates transactions, logs of activity, sniffers and real user monitoring.

At minimum, the network management software should have the following features:

- Performance Monitor - Monitors and alerts on availability, bandwidth utilization, CPU load, memory and disk space utilization.
- Device Monitor - Monitors the availability of devices and provides alerts the moment a router, circuit or server becomes unavailable.
- Network Discovery - Performs a detailed discovery on one device or scans a range of subnets.
- Real-time Interface Monitor - Displays statistics from routers and switches such as packet loss count, response times, and total packet counts processed.
- Port Scanner - Allows testing for open TCP ports across IP Address and port ranges or selection of specific machines and ports.
- Network Mapping – Automatically maps the network and provides a graphical view of the network infrastructure (devices and connections) to reduce the burden of network troubleshooting.

2.9 *VoIP Review*

2.9.1 Overview

The Internet landscape of today borrows immensely from the researches funded by the Advanced Research Project Agency (ARPA), later renamed as Defense Advanced Research Projects Agency (DARPA). That was the beginning with the objective of allowing communications among geographically distributed computers. One of the results was the Network Voice Protocol (NVP) that enabled transporting "real-time full-duplex digital voice over packet switched computer networks" [1] as in the Advanced Research Projects Agency Network (ARPANET), the precursor of today's Internet. NVP was first implemented in December 1973 and was used to send speech between ARPANET sites. [10]

VoIP entrepreneurs noted the business potential of sending voice data packets over the Internet rather than communicating through standard telephone service to avoid long distance charges. Vocaltec introduced its Internet phone software in 1995. This software used the H.323 protocol and ran in personal computers (PCs) with sound cards, microphones, and speakers. Both the caller and the called PC needed to have a computer equipped with the same software and the same kind of soundcard with the latest drivers installed. By 1998, PC to phone service was in place and phone-to-phone service soon followed with a computer establishing the connection. VoIP traffic grew to approximately 1% of all voice traffic in the United States by 1998. by 2000, VoIP traffic accounted for more than 3% of all voice traffic. Once hardware started becoming more affordable, larger companies were able to implement VoIP on their internal IP networks, and long distance providers even began routing some of the calls on their networks over the Internet.

Since 2000, VoIP usage has expanded dramatically. The standards bodies and research consortia, such as the Internet Engineering task Force (IETF), International Telecommunications Union (ITU), and CableLabs, worked on defining standards and interoperable VoIP solutions. Over the years, many different technical standards for VoIP packet transfer and switching has been created such as, H.323, Simple Gateway Control Protocol (SGCP), IP Device Control (IPDC), Media Gateway Control Protocol (MGCP), Megaco/H.248, Data Over Cable Service Interface Specification (DOCSIS), and SIP [2], just to name a few of the major ones. At present it seems that the vendors are converging towards accepting SIP as the premier next generation VoIP protocol for its simplicity and adaptability. However that comes with the price that by now there are quite a few SIP extensions and SIP is notorious for having several ways to implement any given service. In just a few short years, VoIP has gone from being a fringe R&D topic to a viable alternative to standard telephone service.

Given the worldwide move towards IP technology, the rapid acceptance of VoIP, and the pace of development of multiple applications that are quickly being integrated over IP, it is recommended without any reservation that a multi-theater and multi-location enterprise like the US Navy should place emphasis on introducing multi-services networks over IP, assess its benefits as well as limitations, and expand the services as the tests prove to be

satisfactory. Below is a small time line to show how fast VoIP has moved from a laboratory experiment to a viable telephony service.

Timeline: [10 (unless otherwise noted)]
1973 – NVP
1995 – Vocaltec - First Internet phone
1996 – H323 is approved [11]
1996 – SIP is designed designed by Henning Schulzrinne (Columbia University) and Mark Handley (UCL) [12]
1996 – Internet phones catch the attention of US telecommunication companies who ask the US Congress to ban the technology, Telecommunications act of 1996 the beginning of convergence.[13]
1998 – 1% of all voice traffic
1999 – SIP RFC 2543 ratified [14]
2000 – 3% of all voice traffic
2002 – SIP RFC 3261 is ratified [2]
2005 – 16 million users and 5 billion dollar revenue
2009 – est. 55 million users and 17 billion dollar revenue

At present, two major application layer protocol suites dominate multi-service communications over IP. These are: SIP and H.323. They offer very different approaches to application signaling and services. H.323 started earlier in the mid 90's but SIP is rapidly becoming the application protocol of choice, specifically for VoIP, for its scalability and adaptability. However, along with the ease comes the issue of uniformity in implementation. SIP is notorious for having several ways of implementing any given service. Mostly for this reason, many manufacturers support SIP natively with a restricted set of features and also use it purely as a signaling protocol over which their proprietary protocols are run. Alcatel-Lucent for example, supports both SIP and H.323. H.323 is used as a transport for its proprietary protocol "Universal Alcatel (UA)". SIP is supported natively with a set of basic telephony features and also as a signaling protocol in combination with Hyper-Text Transfer Protocol (HTTP) and Voice eXtensible Markup Language (VxML) with softphones. As SIP's capability in supporting a larger set of telephony features natively is enhanced with extensions through the efforts and support of the Internet Engineering Task Force (IETF) and other Internet communities, the features will be incorporated with native SIP.

H.323 is based heavily on the ITU multimedia protocols that preceded it, including H.320 for Integrated Services Digital Network (ISDN), H.321 for Broadband Integrated Services Digital Network (BISDN), and H.324 for General Switched Telephone Network (GSTN) terminals. The encoding mechanisms, protocol fields, and basic operation are somewhat simplified versions of the Q.931 ISDN signaling protocol.

The Session Initiation Protocol (SIP) [10], developed in the Multiparty Multimedia Session Control (MMUSIC) working group of the IETF, takes a different approach to Internet telephony signaling by reusing many of the header fields, encoding rules, error codes, and authentication mechanisms of HTTP.

SIP is becoming the protocol of choice for the application layer for its extensibility, scalability, and adaptability. And, for the same reasons, different SIP extensions indicate different ways of implementing any given service, which is extremely vexing in the user and the vendor community. Relevant SIP protocol suites with extensions should be tested at Department of Defense (DoD) test laboratories and the Defense community should be a major driver for pushing a common, interoperable set of SIP features.

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants without dependency on the type of session that is being established. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP itself does not participate in the sessions themselves but merely enables and controls them. There are several other protocols that have been developed to do the actual work of carrying the session data.

As it stands today, not many extensions have been standardized. Several proposals have been introduced that would provide additional functionality for telephony applications but as of yet they have not been ratified. Because only a few extensions have been ratified, SIP on its own can only perform a few basic functions as it relates to telephony. It is for this reason that vendors have had to develop their solutions to this problem while they wait for the protocol to mature. However, this does not prevent the use of SIP today.

SIP is a request-response protocol that closely resembles two other Internet protocols, HTTP and SMTP (the protocols used for the world wide web and email); consequently, SIP sits comfortably alongside Internet applications. Using SIP, telephony becomes another web application and integrates easily into other Internet services. SIP is a simple toolkit that service providers can use to build converged voice and multimedia services. It is crucial to understand that other protocols must be used alongside SIP in order to provide complete telephony services.

2.9.2 Components in a SIP Environment

In the simplest SIP environment, the only two required components in SIP transaction are a User Agent Client and a User Agent Server. To achieve a complete communications system there are several other dedicated server applications. These server applications may be individual applications on individual computers, or be integrated into a few applications housed on a limited number of computers. The number of applications and computers is dependent on the vendor, size of the implementation and requirement for redundancy in the final solution. Here is a list of the more popular server applications, some of them are defined in the specifications, where others are implemented to serve a set need, which is not defined directly in the different specifications.

2.9.2.1 User Agent Client (UAC)

The UAC is the caller, typically a hard or soft phone.
"A User Agent Client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a User Agent Server for the processing of that transaction." [2]

2.9.2.2 User Agent Server (UAS)

The UAS is the callee, which could be another phone or server.
"The user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a User Agent Client for the processing of that transaction." [2]

2.9.2.3 Back-to-Back User Agent (B2BUA)

"A Back-to-Back User Agent (B2BUA) is a logical entity that receives a request and processes it as a User Agent Server (UAS). In order to determine how the request should be answered, it acts as a User Agent Client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior." [2]

2.9.2.4 Location Server

From RFC 3261, "A location service is used by a SIP redirect or proxy server to obtain information about a callee's possible location(s). It contains a list of bindings of address-of-record keys to zero or more contact addresses. The bindings can be created and removed in many ways; this specification defines a REGISTER method that updates the bindings." [2]
In simple terms, this is a lookup service allowing one to resolve an identity to an (optimized) list of URLs for the contact.

2.9.2.5 Outbound Proxy

"A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a UA is manually configured with an outbound proxy, or can learn about one through auto-configuration protocols." [2]
An outbound proxy is typically used when one wishes all the outgoing calls to go through a proxy, typically because external rules need to be applied to the outbound call. This would be common in the case where you were using a media gateway to convert from SIP to PSTN.

2.9.2.6 Media Gateway (MG)

"A Media Gateway acts as a translation unit between disparate telecommunications networks such as PSTN; Next Generation Networks; 2G, 2.5G and 3G radio access networks or PBX. Media Gateways enable multimedia communications across Next Generation Networks over multiple transport protocols such as ATM and IP.
Because the MG connects different types of networks, one of its main functions is to convert between the different transmission and coding techniques. Media streaming functions such as echo cancellation, DTMF, and tone sender are also located in the MG." [2]

2.9.2.7 Presence Server

A presence server allows users to update their presence information that is then shared with others on the network. This presence information can allow others to see your availability, and contact you appropriately. SIP Instant Messaging (IM) Presence is an extension that provides Instant Messaging functionality alongside availability information.

2.9.2.8 Proxy Server

"An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it" [2]

2.9.2.9 Redirect Server

"A redirect server is a User Agent Server that generates 3xx responses to requests it receives, directing the client to contact an alternate set of URIs." [2]
It accepts SIP requests, maps the address into new addresses which are then returned to the client and provides information on callers' redirect and proxy servers.

2.9.2.10 Registration Server

From RFC 3261, "A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles." [2]

In simple terms, clients register with the registration server when they come online, giving it information about their identity, how to reach them, and who they will allow to communicate with them. This info is then stored in the same database that the Location Server uses for client lookups.

2.9.2.11 Session Border Controller (SBC)

"A Session Border Controller is a device used in some VoIP networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down calls." [2]

A session border controller is normally used at the border of a companies network along with a firewall to enforce company security and network policies. A Session Border Controller can act as either a Back-to-Back User Agent or a proxy, both restricting and changing the contents of the SIP packets. Some more interesting uses of SBCs include the ability to record calls leaving an organization and allowing transcoding due to incompatible codecs.

2.9.2.12 Simple Traversal of UDP Through NATs Server

A Simple Traversal of UDP Through NATs (STUN) server is used typically by a UAC to determine it's public IP address and help identify the type of firewall Network Address Translators (NAT) in place. This information is used to help setup UDP communications for a call behind a NAT'd endpoint.

2.9.3 SIP Limitations

SIP was designed to solve a small but important set of issues and to allow interoperability with a broad spectrum of existing and future IP telephony protocols. To this end SIP provides four basic functions:

1. User Location: mapping a user's name to their current network address (similar to DNS)
2. Feature Negotiation: Allows User Agents (UA) to negotiate a common set of features
3. Call participant management: adding, dropping, or transferring participants
4. Modifying session features while a call is in progress.

Any other functions must be performed by other protocols.

Its simplicity means that SIP is not a Session Description Protocol (e.g., SDP) nor is it able to perform Conference Control functions. It is also not a Resource Reservation Protocol (e.g., RSVP) and it has nothing to do with guaranteeing quality of service (QoS) (e.g., 802.1p, Type of Service (TOS)). SIP can work within a framework with other protocols to insure these roles are played out - but SIP does not perform these functions itself. SIP is regularly deployed alongside SOAP, HTTP, XML, VXML, WSDL, UDDI, SDP, RTP and a variety of other protocols.

Because of the simple nature of SIP many of the functions under study are not achievable with native SIP alone. Standard methods for deploying these features have not yet been ratified due to the myriad of different potential methods to deploy any given feature. Vendors have independently chosen varying methods to solve these issues, which, in turn create a non-interoperable or proprietary situation. Due to this current situation where vendors have not reached agreement and the lack of standards it will be many years before multi-vendor solutions with "plug-and-play" advanced features are available to the

marketplace. This leads to an environment today where COTS SIP products cannot be guaranteed to interoperate or even have similar feature sets.

2.9.4 Current Supported features

Table 2-5 is an abbreviated list of features that are supported by Sphere's Sphericall IP PBX in release 5.[1] JITC-certified Sphericall IP PBX delivers assured connectivity via MLPP for special C2 (command and control) users including strategic leadership and those who manage strategic assets. The list is very extensive, compared to the few items that were determined to need to be implemented in above and supported in the SIP Feasibility section and appendix F.

Table 2-5. Features Supported Sphericall IP PBX Release 5

General Telephony Services
Call Announce
Call Transfer
Call Coverage: Multi-Level, Follow Me, Conditional
Call forward
Call Hold
Call Waiting
Music-On-Hold
On-Hold Reminder
Dial-Out Authorization Codes
Direct Inward Dial
Direct Outward Dial
Inbound Routing Schedules (Automatic)
Message Waiting Indicators
Multi-Party Conferencing
Park Zones
Pickup Groups
Class Of Service Profiles
Permission Lists: Allow / Disallow Specific Numbers
Trunk Hunt Groups: Directional
User Access Authorization Codes
Automatic Route Selection (ARS)
Call Recording (Optional)
Call Admission Control
Multi-Level Precedence and Preemption for Emergency / Critical Communications
Call Accounting
Call Detail Reporting
Data Export: Originator ID, Receiver ID, Intended Receiver ID, Time, Duration, Outcome, Reason
Key Industry Standards Support
SIP - RFC 2543 / 3261
MGCP - RFC 2705 / 3149
SIPConnect for SIP Trunking
SIMPLE (Windows Messenger)
TAPI 3.0
DirectX 8.0
SMDI
TCP / IP / UDP
DHCP
FTP / TFTP
SNTP
RTP / RTCP
SOAP

[1] http://www.spherecom.com/product_docs/Sphericall_Data_Sheet_53106.pdf

XML
Advanced Communications Features
Call Recording (Optional)
Multi-Level Precedence and Preemption for Emergency / Critical Communications
Softphone for Mobile and Remote Users
User Presence Status Monitoring
Standard Telephony Features*
Caller ID Display
Call Transfer (Attended or Unattended)
Mute
Hold
Park / Unpark
Do Not Disturb
Transfer to Voice Mail
Redial
Incoming Call Indication with Caller ID
Message Waiting Indication
Missed Call Indication with Caller ID
Multi-Party Audio Conferencing
* Phone/device dependent.

A key group of features were chosen to be reviewed in detail as how they would be implemented in SIP and if the protocol supported the feature directly. The features chosen were ones that were determined as important to an installation on a U.S. Navy vessel. There were other features which were not evaluated because they were known to be implemented or not required.

2.9.5 Selected SIP Features

A group of features that are not documented were chosen for a more detailed review. These features were felt that they would be required in different U.S. Navy internal communications systems. Each feature is listed independently and described, and then a section that explains the changes that may be required in SIP to implemented. Companies, such as Sphere and Pingtel, under the umbrella of the SIP specifications and drafts, have implemented many of these features.

2.9.5.1 Conference Call

A conference call is the creation of a group of end devices coupled together so all participants can hold a conversation. It requires action of the end user to pick up their end device or call into a conference number.

SIP was defined to allow for the establishment, maintenance, and termination of calls between one or more users. However, despite its origins as a large-scale multiparty conferencing protocol, SIP is used today primarily for point-to-point calls. This configuration is the focus of the SIP specification and most of its extensions. As a result, there is a lot of confusion about how SIP supports multi-party conferencing.

There are a number of conferencing models supported by native SIP. These models range from Three-Party Calling with end system mixing to large multicast conferences, to dial-in or dial-out conferences servers, to ad-hoc centralized conferences, to conferences using centralized signaling and distributed media. Most conference calls involving more than a dozen or so participants have the need for more advanced features such as the ability of the moderator to mute all phones, set the length of time for the conference call, record and display the participants of the conference call, etc. However, there is no ratified standard for any of these models as of yet. A draft exists by Rosenberg, titled *draft-rosenberg-sip-conferencing-models-00* [15] that describes all of these models in detail. There are products available that work with different vendors solutions. All the vendors confirmed they had a method to support it.

Changes Needed to SIP Protocol
No changes or modifications of SIP are required to implement this feature, however, a User Agent Server (UAS) or mixer is required.

2.9.5.2 Intercom

This feature involves the creation of a group of end devices coupled together so all participants can hold a conversation. It doesn't require the end user to pick up their end device or hang it up. The end device goes off-hook automatically and then returns to on-hook after the intercom is completed.

The Session Initiation Protocol does not currently provide a mechanism to force the UA (User Agent) to go *off-hook*. A UA could be configured to *auto-answer* incoming calls. It is possible, and some manufacturers have implemented this method, to add a field to the standard INVITE header that would cause the receiving UA to go off-hook automatically with or without mute. In essence, the called device must understand this field or flag and it must be programmed to act on it. A number of manufacturers have successfully implemented this feature. One of the end devices that support it is Polycom; they use a parameter in the INVITE SIP header to signal the phone. This method can be used but must be implemented in the IP-PBX as well as the end device. To use the phone for announcing, the Pager Server must also support the method. There is an Internet draft called "draft-ietf-sip-answermode-00" but it expired in June of 2006 with no action taken. The creation of a group of end devices so all participants can hold a conversation is in essence a form of Conference Call.

Changes Needed to SIP Protocol
Methods to extend SIP have been implemented by some manufacturers but an Internet draft must be proposed, discussed and ratified in order to provide this function in a standard manner and guarantee availability in any given SIP device.

2.9.5.3 Group Page

The creation of a group of end devices coupled together so a one-way announcement can be done. The end device goes off-hook automatically and then returns to on-hook after the announcement is completed.

This feature has similar issues to the Intercom feature described above in that it involves calling a group of users simultaneously. Like the Intercom feature above, it would also be an invite-based conference call. The basic difference between these features is that the Intercom feature calls for a two-way conversation and Group Page calls for a one-way conversation but the mechanics are identical. The native SIP vendors that didn't support it indicated that it could be added to their product line. This can also be done by the Announcing system, or a conjunction between the two systems.

Changes Needed to SIP Protocol
An auto-mute function must be added to SIP.

2.9.5.4 Priority Calls

The ability for an individual to break into a call that is in progress by use of a feature code and supervisor login.
SIP, as a signaling protocol, does not have the ability to break into ongoing calls. The support for Multi-Level Precedence and Preemption (MLPP), can be used instead, see below.

Changes Needed to SIP Protocol
Extensions to SIP would need to be drafted and ratified in order to provide this function. The SIP protocol would need to have the ability to signal the UA and have the UA duplicate the incoming and outgoing voice streams to add the new UA into a new conference call.

2.9.5.5 NCS Voice Precedence System

Known as Multi-Level Precedence and Preemption gives individuals the ability to override a call that is in progress between two or more parties. This feature is presently not being used onboard US Navy vessels. Instead, Priority Calling is being used. Priority Calling differs from MLPP in that it is a method of inserting a third-party into an ongoing call without notification to the original parties. An operator or similar person traditionally used it to check the status of the line. MLPP on the other hand, is a priority-based call override system. This system may affect all SIP elements in a network. It is identical to a basic call with the addition of the *Resource-Priority* field in the INVITE message. Not all vendors have implemented this feature but it has been implemented by Sphere for their JITC certification.

Changes Needed to SIP Protocol
No changes needed to SIP. At a minimum, support of RFC 4412 [3] is required by the UA's. Preferably, all SIP elements should support this RFC.

2.9.5.6 Call Park

The ability to park a call onto a virtual extension and then have a third-party or the same individual, retrieve the call. To the caller, the call appears to be on hold and is presented with "music on hold", dependant on the implementation.

This feature, like many others, can be implemented with SIP in several ways. It is defined in RFC 4240 [16] and in the *draft-procter-sipping-call-park-extension-00* draft document [17]. Several different methods are also described in books and SIP-related sites on the Internet. It has been implemented by both of the native SIP vendors.

Changes Needed to SIP Protocol
No changes required for this method. The only requirement is a "Park Server". Other methods may require modifications and/or additional servers.

2.9.5.7 Directed Call Pick-up

This feature provides the ability to pick-up a call that is ringing on another end device. Call Pickup is described in the IETF draft called *draft-worley-sipping-pickup-02*. This document states:
"There are several different schemes for implementing call pickup. The basic method is the one specified in the Sylantro "SIP-B" specification, which despite its proprietary air, uses standard SIP features in an end-point call control (EPCC) style. All other methods are variations on the same theme, usually by using an agent process (in a proxy or communications server) to provide a feature that the user agents are lacking.
Like call transfer, effecting call pickup requires some support from the caller's end. These caller-end features will, therefore, soon come to be considered necessary for any "quality" SIP implementation." It has been implemented by both of the native SIP vendors.

Changes Needed to SIP Protocol
No changes to the protocol itself are required. Some of the more complex implementations, in particular those requiring proxies and servers, will require software additions. It would be beneficial to have a RFC so a single method is used across multiple vendors' in their implementations

2.9.5.8 Group Call Pick-up

The SIP flows for this function are identical to the flows required for Directed Call-Pickup (above). The exception being that the called extension is a conference URI. In other words, the group of end-devices must be in a conference. You may then poll the conference URI to obtain the ringing party's URI. It has been implemented by both of the native SIP vendors.

Changes Needed to SIP Protocol
No changes to the protocol itself are required. Some of the more complex implementations, in particular those requiring proxies and servers, will require software additions.

2.9.5.9 Recording of Calls

This feature would provide the ability to record calls from a set of pre-defined end devices as soon as they are off hook. This would be used for all calls that the bridge handles.

There are a number of ways in which this feature might be implemented. The community has discussed this subject extensively since the year 2000. Several ideas have been bandied about but no drafts or standards have come of it. The potential implementations would all require the creation of a Conference Call and the automatic addition (or INVITE) of a *recorder*. The *recorder* would simply act as a standard UA and store the mixed streams it receives. Another method that some companies use a promiscuous mode to look at the SIP traffic on the network and record calls per a pre-defined filter that captures the packets for a particular call. This method has no requirements of the SIP protocol; other then its headers must conform to the RFC 3261 specification. [2] The securing of the control signal and the bearer streams complicates this. The recording device must be able to decrypt the stream or it must be decrypted by a Session Board Controller.

Changes Needed to SIP Protocol

No changes to SIP need be implemented. However, a standard should be proposed and ratified that defines the methodology for achieving this functionality. Until a standard is available there is no guarantee any two vendors will implement this feature in the same way.

2.9.6 Selected SIP Features Summary

After extensive research, the salient point to be made is simple: all of the above features have been or could be implemented with SIP with approximately 90% of the above features implemented to the SIP standard or to draft versions of the standard. For any given feature there are a number of ways to achieve it and this is typical for new protocol implementations as they mature. This, coupled with SIP's simplicity, we believe, the reason for the current state of any confusion with regards to SIP standardization. Several of the features such as Intercom have been implemented with Polycom phones; this method is well documented and can be added into the end devices that would be used. Group Paging also requires the auto-answer like the Intercom. The use of the Announcing system can also be used instead of group paging on the phone system.

Priority Calls can be achieved with the use of MLPP. None of them seem to be a show stopper, and in the future these will have a ratified RFC that will have support from multiple vendors. In addition, we can envision that eventually the SIP protocol standard will be completed in such a manner as to provide standard methods of implementation for these and other telephony features as the market matures, which is being lead by the readily available cost effective products being deployed in the business and home environments.

2.10 Announcing System

2.10.1 Introduction

The announcing system is an important sub-system of the internal communications system on U.S. Navy vessels. It is used for day-to-day announcements as well as during emergences on the vessel. The present design is based an amplifiers that power strings of loudspeakers. Depending on the vessel; there is a vast array of specifications. The derived baseline is a subset of the different specification from the different vessels that were reviewed. The announcements are done through the phone system or dedicated microphone stations. An alternative design would be to transfer the audio through the IP packet network. There are pros and cons with this alternative that will be discussed in this section.

2.10.2 Present System

The current implementations vary from vessel type to type. This description of a "standard" system is from the derived baseline section. Refer to Figure 2-13. The dedicated cabinet houses the different components of the system except for the speakers and microphone stations. The input to the cabinet comes from three main sources. The first is the alarm initiate system that allows an individual to initiate an alarm from different locations around the vessel. The second is from the phone system through a telephony interface to the announcing system. The third system is an independent microphone station that allows the user to select the speaker string for the announcement to go over. The announcement comes into the cabinet from anyone of the sources and is routed through a relay based, processor controlled, circuit. This circuit determines the speaker string that the announcement will go out to. It also determines if a pre-recorded file needs to be played or if the audio is coming from the person making the announcement. The audio is then forwarded through the amplifier and then out to the speaker string. This is a simplified review of a complicated system that will set the framework for the following sections.

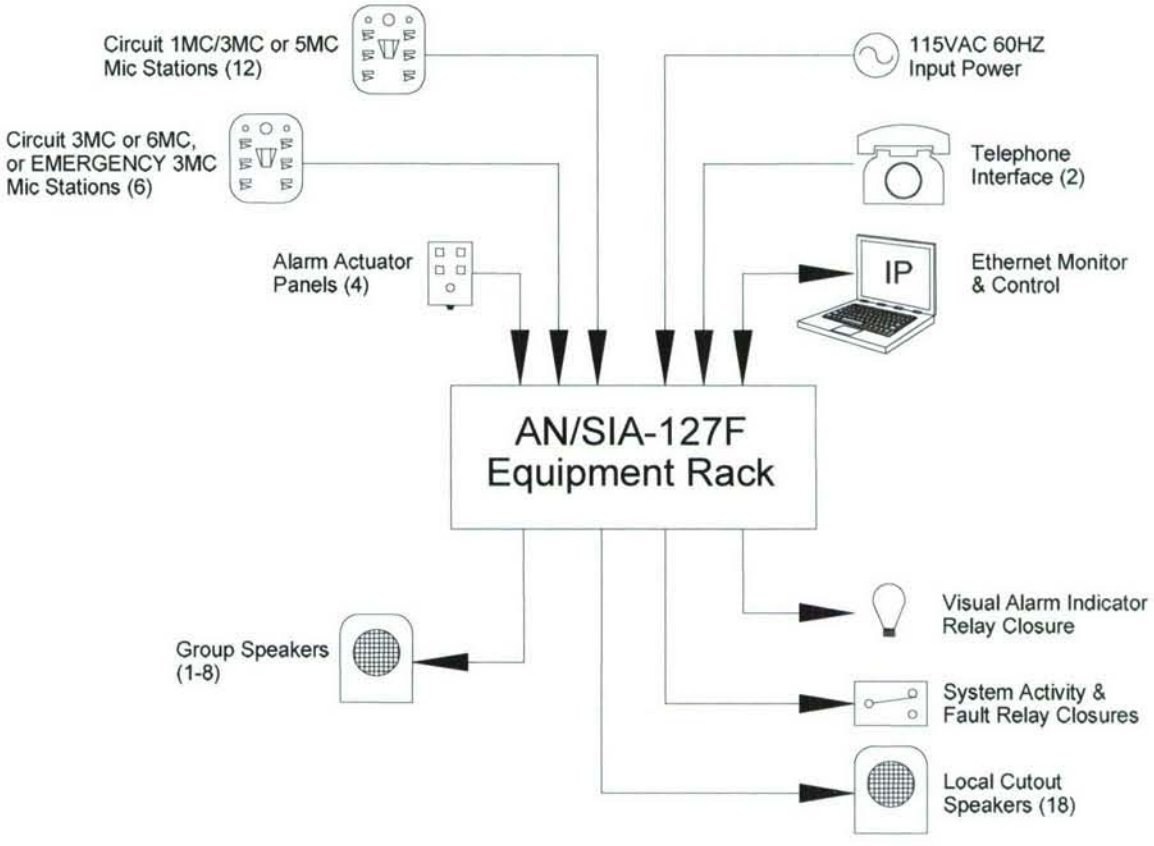


Figure 2-13. Present Announcing System Diagram, Typical

2.10.3 IP Packet System

In an IP packet based system the speakers are located on the IP network and the audio is carried in packets to the speakers that contain the amplifier. In the COTS world many of the parts have been defined and are commercially available from multiple vendors. Figure 2-14 [18] is a typical diagram that shows the connections for a commercial implementation.

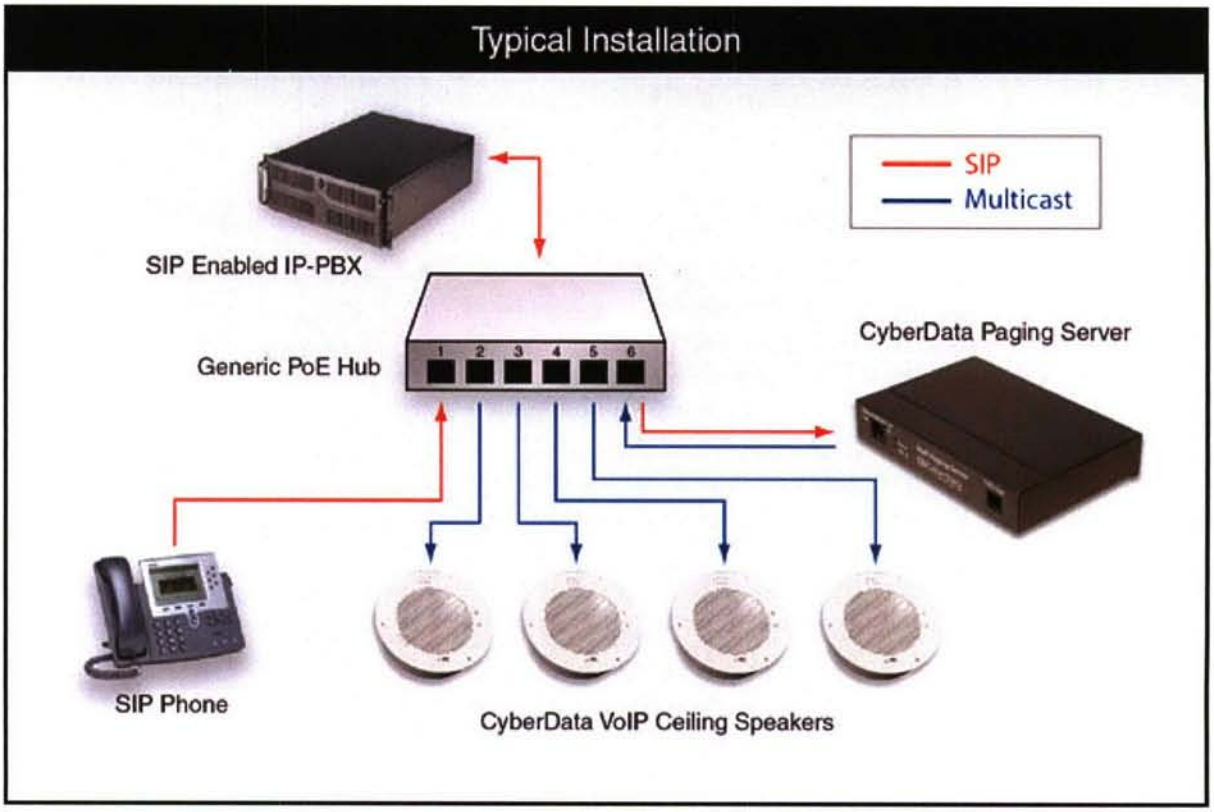


Figure 2-14. IP Packet Based System, Typical

This particular design uses multicast between the pager server and the speakers to create the groups and pass the audio to the individual speakers within the multicast group. The initiating of the announcement is done through a SIP device using the IP-PBX server. The speakers, depending on the output size, can be either PoE or powered through external connection to ship power.

2.10.4 Short Falls of COTS

Moving the present announcing system to a packet-based system appears at first glance to be a very easy task. As shown in Figure 2-14, the individual parts are available for a system used for a commercial implementation. A look into the current COTS products and a comparison of them to the derived baseline shows that there are several short falls. In the design the initiated announcement is from a phone. The U.S. Navy requirements call for two other methods that do not fall into this present schematic cleanly. The microphone stations have several features that can not be implemented from a standard IP phone. The pager servers from the different companies vary in functionality, but they all fall short of the requirements represented in the derived baseline. The commercial products have a priority-based system that will allow the highest priority announcement to supersede a lower priority one. The ability to play pre-recorded files is not natively defined in their products. This could be achieved through several methods that will need to be evaluated. The use of the IP-PBX's may contain, store and forward messages that could be conferenced into the announcement, but this is still an issue since some alarms should continue until the alarm completes, even though the initiator has hung-up. The

other is a prerecorded player that is used in the current system. This would need to be evaluated if the output format can be integrated into the packet-based network. The commercial system does not have provisions for actuating a strobe to indicate the presence of the announcement. The current system will increase volume of a speaker string to maintain a set volume over the ambient noise level.

2.10.5 Design Concepts New IP System

Conceptually, the design for the announcing system is multi-facetted. The system would break down to three major parts: page server, speakers, and microphone stations. Each section is independent, but needs to communicate with each other through one or more protocols. We will deal with each one separately and then at the end interconnect them and discuss the complete system.

2.10.5.1 Page Server

The page server can be located in a small appliance or a PC based system and co-exists with other applications in the internal communication system. The design for the priority is a great start, but the rules for dealing with the different MC zones is more complicated than the simple priority implementation can achieve. The commercial design is a single layer of priorities, where the specification requires multiple level of priority depending on the different MC and the source of the announcement. The new design will need to make programming the different priority levels and groups of the MC easy, maybe with the use of a graphical interface that will be more object orientated than a spreadsheet type of interface. The page server will need to communicate with the other devices in the system through another protocol, such as SOAP, to transfer the information, such as zones, output levels, and alarm type. The server also needs to be natively redundant. The current design relies on DNS or a cluster, but the new design should be closer coupled so the configuration and what announcement is presently in process are distributed between the different redundant servers. This is important to be able to maintain the announcement functionality during emergency scenarios.

2.10.5.2 Speaker

The speaker needs to become smarter and be able to handle functions that were dedicated to the announcing server rack. In addition to the physical speaker there is a circuit card that converts the multicast or SIP information into audio that is then sent to the speaker. The circuit itself requires a limited amount of power. The first feature is to be able to maintain an offset to the ambient noise level. This could be implemented onto the SIP controlling circuit as an optional card. The requirement for the light could be handled with a single addition of a relay that is actuated when the announcement is underway. This could be done as an optional card or just added to the card; the contacts are exposed through a plug on the speaker's housing. Depending on the power requirement the speaker can be operated from PoE on speakers that require less then 15 watts total. A power output over the 15 watts will require external power supplied from the ship to power the amplifier circuit. The speakers can be designed with dual-homed network cards to allow the speaker to connect to two different switches adding resilience to the design.

2.10.5.3 Microphone Station

The microphone station is really a specialized device; nothing in the COTS world comes close to this unit. Over and above the ability to allow the user to create the audio, it has other control features that do not lend themselves to a typical SIP phone. The three main requirements are: display microphone signal level, allow selection of a speaker group and display active speaker groups. The first requirement is contained in the microphone station and is just giving the amount of signal power of the individual voice. This is only a design feature that will not affect the information that is transferred back to the page server. The second feature is selection of the speaker group that the announcement will be placed over. This can be done in multiple ways. The first is to use how the COTS systems work that defines each group as an extension or a group number that is dialed after an extension that gets them into the page server. Other methods would be to use a different protocol, such as SOAP, to transfer the speaker group to the pager server in a separate packet from the audio that is in a RTP packet. This would require a specialized page server, but would then allow more customization of the paging groups that are actuated at a single time. The last major feature in this area is the ability for the user to see what speaker groups are currently being used. This will allow the user to determine if they want to try to supersede the current announcement. The microphone station and the speaker group it is initiating define the priority of the announcement. This functionality can be controlled through another protocol again like SOAP that is running alongside the SIP that is carrying the audio. More evaluation needs be done to determine if SIP should even be used or if the use of SOAP and RTP should be used directly and not incur the overhead and limitation that SIP could cause. Even this approach could be done in an open system design so it is not proprietary in nature.

2.10.6 Summary

Because the commercial requirements are small compared to the U.S. Navy's requirements, this system will not be able to be accomplished in a COTS solution unless the requirements are changed to conform to a COTS solution. Parts can be used from commercial sources. The major components will need to be created from open system designs but be created to fulfill the U.S. Navy's requirements.

Another area to look at is the resilience of the IP network. The current system does not rely on a data network; it has its own wiring infrastructure. This makes it isolated from other issues on the network. By using the data network a reduction in wiring should be realized. Resiliency can be achieved by using dual homed devices to multiple switches in different segments of the network. Each speaker is connected to a network switch that will supply PoE in most cases. The wiring for the speakers is much lighter and a single wire that is damaged will not affect a full string of speakers. Also the use of "cutout and test panels" is removed since you do not need a panel to house the speaker strings for testing. The method of testing will be done at the network level using a network-monitoring tool. This tool could be COTS supplied or a customized tool for just the announcing system. This is one of the areas that the VoIP solution from COTS will not address the needs of the U.S. Navy.

2.11 Mobile Communications

2.11.1 Introduction

An investigation was performed into the use of Commercial off the Shelf (COTS) wireless technologies for mobile communications in a naval environment. The wireless technologies investigated include Wireless Fidelity (WiFi/802.11), Worldwide Interoperability for Microwave Access (WiMAX/802.16), and Cellular.

2.11.2 Issues and Impairments

Mobile communications onboard a naval ship are affected by the same impairments seen in traditional environments (e.g., commercial office space, urban areas). In some cases these impairments can be even more pronounced onboard a navy ship. Impairments due to multipath interference, user mobility, signal attenuation, competing wireless devices, and various EMI sources all exist onboard a ship.

Beyond these impairments, other issues that should be considered include: operating spectrum, support for voice and data, security, interference, jamming, Quality of Service (QoS), cost, and availability of COTS equipment.

2.11.3 Environmental Issues

A shipboard environment poses several challenges for wireless communications. The ship's metal infrastructure interacts with wireless signals. Additionally, the ship's metal walls reflect wireless signals and may contribute to the effects of multipath interference. Other subsystems onboard ship may contribute to background Radio Frequency (RF) emissions that may interfere with the wireless signals.

The characteristics of the wireless environment aboard a ship can change based on location and usage. Certain impairments that may not be an issue in one location may cause significant problems in another location. A solution that may be appropriate for one area of the ship may not be appropriate or even work in another area.

Larger interior rooms such as the hanger of an aircraft carrier would see problems associated with echoes and long delays, while smaller interior rooms might need to deal with issues associated with signal attenuation. Areas outside the ship, which tend to be relatively good environments for wireless communication, may need to deal with interference from other communication devices or radar systems.

The actual performance for wireless technologies within the ship can be assessed best with a site survey, where accurate measurements of wireless equipment can be made at sample locations.

2.11.4 Wireless Principles & Techniques

Useful wireless systems need to support multiple users. Several different multiplexing techniques have been developed to support multiple users in wireless environments. Some techniques are better than others for guarding against certain impairments seen in wireless communication.

Various modulation techniques have also been developed for mapping data bits to digital signals. These techniques may include Forward Error Correction (FEC) codes that allow the receiver to recreate the original transmitted data even when bit errors exist. There is generally a tradeoff between the data overhead and a modulation techniques ability to tolerate bit errors. Some data systems use per-frame error detection codes (e.g., Cyclic Redundancy Check (CRC)) to detect (but not correct) errors. High data-rate protocols tend to rely on the correcting ability of FEC codes.

Channel equalization signal processing techniques may also be used to guard against multipath impairments. An efficient equalizer can actually enhance the received signal by combining each received reflection.

2.11.5 Conclusions

Between WiFi, WiMAX, and cellular technologies, there is no clear winner. One can choose a technology for the interior of the ship (and on deck) independent of the choice for ship-to-ship/ship-to-shore communication because they are independent networks connected to the wired backbone network.

2.11.5.1 WiFi

WiFi is most likely the best choice for mobile communications inside the ship, primarily because it is a proven technology and very cost effective. In large open interior rooms however (e.g., an airplane hanger on a carrier), WiFi might not operate. Voice quality over WiFi (e.g., VoIP over WiFi) has provided particular low quality in the past. Newer systems may provide better service due to better bandwidth and coverage.

Problems associated with attenuation and the limited range of WiFi signals can easily be corrected through the use of many access points. State of the art access points for $100 to $200 are readily available, and network interface cards range from $20 to $100. Connecting to the wired network is easy because WiFi access points use standard Ethernet interfaces.

2.11.5.2 WiMAX

WiMAX appears to be the best choice for ship-to-ship and ship-to-shore communication because of its high data rate and range. Because it was designed to support data and voice applications, it has provided QoS capabilities from its inception. WiMAX also supports protocols that are resistant to most of the impairments found in RF-challenged environments.

WiMAX attempts to position itself between WiFi and cellular in terms of cost. WiMAX devices are starting to appear on the market. WiMAX infrastructure (e.g., base stations) and PC cards appeared on the market within the last year. Today, full-featured WiMAX routers for high-speed point-to-point links cost upwards of $10,000. Smaller routers for indoor use start at a few hundred dollars each.

One potential area of concern with WiMAX is spectrum availability. Independent decisions to allocate bands for specific applications and resistance to change historically allocated bands, has resulted in fragmented spectrums that differ between countries, despite economic advantages to having global interoperable standards. A naval system needs to be aware of potential issues in (or near) foreign ports.

2.11.5.3 Cellular

Cellular technologies could also be used for ship-to-ship and ship-to-shore communication. Although cellular technologies support data applications, the data rates are lower than the other technologies. The data rates, however, are constantly improving. The next generation is expected to provide broadband data rates to mobile users.

Cellular systems can be very expensive (in the hundreds of thousands of dollars). Smaller systems, such as base-station routers, provide a subset of the features commercial providers require and range in price from a few hundred to a few thousand dollars each.

Spectrum license issues may restrict usage for ship-to-shore applications. In general, voice bands are fairly well standardized because of the industry's push for mobile sets that can operate globally. It is not clear that data services will be able to share the same level of commonality.

2.12 Communication Terminal

2.12.1 Introduction

The internal communication terminal (ICT) is found where communications are critical to the operation of the vessel. It is considered a tactical device that must be easy to use, and have a very high reliability level. These units are produced by a very limited number of manufacturers of which three of them are L-3 Communications divisions.
This section will combine many of the other sections that deal with individual components of the ICT as well as sections that contain information that can be applied to the terminal. It is not installed on all vessels, but many vessel and submarines in the past have had them installed in the tactical locations.

2.12.2 Uses

ICT are installed in several different locations on the vessels. In each location the screens can be different to customize it for the needs of the sailors that man that location. It is used on the bridge that has special needs for night modes that may not used in other compartments that are not exposed to the nighttime light requirements. The unit is also used on the bridge of the submarine as a portable unit that has to be able to withstand the external environment including direct sun light. The ICT that are used by the sailor on watch has the same requirements as the above ones. The internal components of the ICTs are the same between the different models; only the external casing varies depending on the use. The units also come in two different sizes for use on different vessels and locations. The difference is the screen size and some of the soft controls are moved to external knobs to make the configuration easier on the end user.

2.12.3 GUI

The GUI is very different than what would be found on many devices that would be in the same category as the ICT. The personal digital assistant (PDA) has a very sleek user interface, but there are some simple differences between these two devices that need to be kept in mind when the GUI is discussed. The first one that really defines the rest of them is that the sailor must be able to operate the ICT with fire protective gloves on. The ability to get feed back from touch is all but impossible through these gloves. The ability to select a small menu and then navigate down to the selection and then down another menu is impossible with these gloves on. So the principle, user interface control for the ICT is the button. The size of the button must be large, because the end of the gloved finger is large. One way to keep from having multiple buttons hit at a single time is to have only the center of the button active for selection and then have the rest of the graphical button as a border around the active center. The next requirement is for the ease of use that also translates into limited levels of abstraction. In a PDA it may take four clicks or more with the stylus to get to dial a number and then the number must be entered. Since the main purpose of the ICT is dialing numbers and those numbers are predefined for the location, the use of speed dials are used from the initial screen. The

first two screens are speed dials that are the most commonly used for that location. The display could have two sections, the permanent and the variable. The permanent stays the same so the user does not have to think about where set buttons are; the variable section changes depending on what is selected in the permanent section. With this separation of the screen the end user can quickly navigate the screen and reduce the number of button presses to one or two for all the normal operations. For more detailed description of the GUI requirements and methods to implement them see the GUI section.

2.12.4 Hardware

The present ICT are all form-fit-function to what is presently on the vessels. Currently there are two sizes, but the internal components of many of the ICT are the same for each vendor and only the case and the screen is different. The input device varies from different manufacturers. The two most common input devices is the touch screen that appears in the derived baseline, as well as buttons that have LCD displays on each individual switch. Both methods fulfill the same needs with differing degrees of flexibility. The touch screen allows for the button pattern to be changed as required to reduce clutter. The internal circuitry boards that are used in the individual vendor ICT is unknown, since they are proprietary to the individual companies. Research was done to see what options are available for this type of unit designed around a VoIP communication infrastructure from COTS products. In the embedded section there are three COTS types of devices reviewed. They are Stand-Alone, Integrated Circuit (IC) and custom VoIP devices. The first category had nothing that could be modified to support this product. The other two categories contained viable candidates that should be looked at for a new VoIP-based ICT. The IC, also referred to as "phone on a chip", lets the developer design a supporting circuit as well as the firmware for the IC to accomplish the required task for the ICT. This approach has its benefits and disadvantages for both the vendor and the U.S. Navy. On the end of the vendor it is more costly of a development cycle and changes after production are usually expensive. The benefits are that the package size and functionality can be tailored for the requirements of the product. The U.S. Navy needs to make sure they have all the requirements defined before the vendor development progresses because changes are usually costly and may not be possible without scrapping production units. The benefits are that for shock and vibration the design can include them from the conception. Because nothing is added extra to the design the power requirements can usually be reduced on this type of design. The custom devices range in types from dedicated computing systems, such as the R.L.C Enterprise offering, to PC/104 package units that are computer boards in a universally supported form facture. The benefits are that the cost of development is reduced since the individual components and circuits are already designed and individual components are assembled to create the final product. The final product was not designed for shock and vibration, as well as extra circuits are many times included since you have to use what is already designed. In many cases you cannot get exactly what you want but something that is close may fulfill the requirement. The other approach is to mix the two methods and create custom boards in the same form factor that the IC required for the application, but use other production cards for functions that are available and meet the requirements. The hardware and design used is controlled by many different factors. A complete understanding of the requirements and how it will integrate with the other devices in the

network will be critical to the correct choice. The software SIP stack in either of these methods is flexible and should be able to be changed as required as SIP matures. See the different sections on SIP and Open Source for more information on the options for the SIP stack design.

2.12.5 Derived Specification

The derived baseline is a starting point for the requirements of the ICT. It was reduced from hundreds of requirements that came from many different vessel specifications and covers several different generations. For the purpose of this report and the follow on project it gives a basis to evaluate what can be done with COTS products and what is not possible. In some cases, such as the telephony connections, it will not be followed since the method of signaling is changing from TDM to VoIP. The derived baseline does not show any of the next generation features that can be added to the system. These were learned from meetings with U.S. Navy personnel, as well as conversations with manufactures and other organizations. The next section will cover some of the new features that can be added with the change to an IP-based communication system that is PC-based and converged with the data network.

2.12.6 Future Features

In the light of the discussion of the PDA above, that device brings to light many features that could be beneficial to the ICT. The concept of add-in programs for set tasks that an individual user may need. Even though the base operation of the ICT needs to be streamlined for tactical use, there are other times that the unit can be used to distribute information that would usually not be available through the ICT. Some concepts that were found were:

- Manuals distribution
- Ability to view video that is stored or live feed
    - Training videos
    - Damage control live streaming video
- Built in camera
- Display important vessel information
- Display important weather information
- Display vessel calendar of events
- Voicemail delivered to the station or person at the station
- Portable ICT
    - Wireless for use on support boats
    - GPS to send back to track the portable unit
    - Battery powered

The list shows the interest of using the ICT for other things than just communications. Some of them assist in damage control allowing individuals to survey compartments without having to have individual sailors manually go from compartment to compartment or enter a hazardous area. Some of them enable the sailor to get access to manuals allowing them to learn material while sitting at a station that needs to be manned. The

ability to allow individuals to gather information about the vessel and/or weather conditions by the press of a button converges many of the different tasks into a single device. All of these features maybe limited to a few ICTs or to only particular individuals so they do not have to call or go to another compartment to gather or view the information. These features all need to be evaluated for feasibility for being done on the ICT, but technically there is no reason these types of features cannot be added to the ICT and restricted by the profile that is enabled.

2.12.7 Security

Security is addressed in several different sections. When we talk about security for the ICT we have a few different areas that need to be addressed. The major one is the handling of red and black communications. This one alone covers several different areas that need to be evaluated. The communications stream needs to be separated and never allowed to cross between them. This can be done with separate networks or with converged networks with different security methods that are in use today in other industries. This is covered in the Appendix I. The display must inform the end user if the call is encrypted or non-encrypted; this is discuss in detail in the GUI section 5.22 of this report. The profiles need to be protected so individuals cannot assume the identity of another individual allowing them access to areas of the configuration, add-on applications and secured calls. The method of doing this has not been heavily researched for this report. There are many different methods that are in use in the corporate world and military that could be modified for this use. Things that would need to be evaluated is the ease and freedom that needs to be maintained for the sailor, in their day-to-day work. The use of an identification card that must be inserted into the unit each time they sit down, with a matching password would result in extended times to getting the ICT operational. Another issue that needs to be decided is if there are two operators how is the login process to be handled or does the lowest level profile take precedence. If the method means the individual has to log in each time he sits down with a large complicated password with fire safety gloves on, there is a problem with the security method. A solution is the base profile that comes up when the ICT is started has no login required, but has a limited functionality that is defined by the location of the ICT. If the user needs more functionality then they need to log into the ICT to get their own profile. Profiles are reviewed in greater detail in the GUI section.

2.12.8 Summary

The ICT is not a product that will be found in COTS. It is very specialized for the application that the U.S. Navy uses it for. From the research there is no reason that the functionality can't be maintained with the change to VoIP. With the change to being an IP based device many new features can be visited to make the ICT a more rounded product. There will be challenges to making it work with SIP and new extensions will need to be written for SIP. See the section on SIP for more details on the changes and how it can be accomplished.

2.13 End Devices

2.13.1 Introduction

There are multiple End Devices used to meet the communications requirements of a naval vessel including standard devices in various configurations and form factors and specialized end devices customized to meet specific requirements. These include Intelligent Communication Terminals (ICT), Dial Telephones, Dedicated Stations, and Speakers or similar devices under different names depending on the specific vessel. These individual devices are all specialized for the U.S. Navy's requirements; in progressing through the following section the amount of customization decreases. This section will introduce the different devices and explain some methods that can be used to adapt it to a VoIP environment.

2.13.2 Integrated Communication Terminal

The Integrated Communications Terminal (ICT) is a device that is not available from any non-military commercial supplier. It is very specialized to the requirements for the U.S. Navy and the individual vessels on which it is installed. There are a few manufacturers for the U.S. Navy of this device; L-3 Communications has three divisions that manufacture them, one of them being Henschel. Even though the form and fit are the same, the design and technologies used are very different. ICT connect to the switch through a multiple basic rate interface (BRI) or a proprietary interface depending on the PBX that is installed on the vessel. The ICTs also come in a few different configurations for the vessel on which they are used, but the underlying components are the same. The derived baseline defines the different requirements for the ICT. The section on graphic user interface (GUI) also discusses the general GUI for this device, but focuses on the requirements for an efficient user interface.

The areas that need to change are the ones that relate to the connection to the PBX and how it will provide isolation and security between the red and black communications. The ICT connects to multiple devices. This could be multiple PBXs or to the external radio transmitter. Connections to the announcing system will be handled through the PBX, and would not be directly connected to the ICT. The security section discusses the methods of securing the IP network. In this section, several options are given, ranging from segmentation of the networks to converged networks with different methods of securing the data on the converged network. The security and the degree of convergence will set the requirements for the handling of the communications between the ICT and the PBXs and/or radio transmitter.

Independent of the level of converged network that is used, the method of connection will be the same. The use of SIP as the telephony protocol has several benefits but also falls short in a few areas, however the other VoIP protocols also fall short in the same areas as well as others. See the section on SIP for more details on VoIP protocols. The use of a commercially available SIP stack has a few drawbacks. The SIP stacks that have been reviewed do not support multiple active calls. In the business environment, a single line is active and the rest of the lines are placed on hold. There are a couple different areas that this affects. The first is that the stacks do not allow multiple hooks into the media-

device (sound board). This problem may be corrected by re-writing the stack to allow multiple calls to be active and to allow each individual call to have its own hook into the media-device. The media-device also needs to have multiple channels to support the multiple call feeds. The embedded device section discusses this in more detail, and gives a number of products that could be used to fulfill the requirements. There is also information that needs to be displayed that is not required in the commercial environment. The SIP specifications support Caller ID (RFC 2543bis) but the encrypted and un-encrypted information coming from the radio connections also need to be supported.. This can be included into the SIP header, but currently there is no specification or draft that deals with this type of information. The SIP specification also does not support the auto-answer feature. There is a draft (draft-ietf-sip-answermode-04)) which will expire December 14, 2007 that offers a solution for this feature that is required for the Intercom Call requirements. Push-to-talk (PTT) is another place that needs to have more review. RFC 4354 "A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service" is the specification that defines PTT; it addresses the cellular phone market place requirements. The Open Mobile Alliance (OMA) (http://www.openmobilealliance.org) is currently specifying the Push-to-talk over Cellular (PoC) service. Each of the individual items are feasible changes that can be incorporated into the ICT, as well as incorporated into the SIP infrastructure.

2.13.3 Dedicated Station

The dedicated station (DS) is a dial telephone (DT) that is customized for a single purpose and has a reduced user interface. Because it is a customized phone, it cannot be purchased as a COTS device. This is not to say that parts of it cannot be purchased as COTS. As with the DT there are two types of base telephone technologies used, one is analog and the other is digital. See the section on DT for more details on the differences, as well as the different features that the phones support. The DS does not have a keypad for dialing out, it is meant to receive calls and allow the user to answer the call. The user interface is limited to an on-hook/off-hook switch, and other selection switches and indicator lamps. It has a single jack that a handset or equivalent can be plugged into or a speaker and/or microphone directly connected to. Because of the limited user interface it lends itself to a phone on a chip solution. This also adds more flexibility since the SIP stack can then be controlled which will allow for added features, if required. If features are added, then the SIP server and possibly the other end devices need to be aware of the changes to the SIP packets. SIP does have the benefit that if a SIP stack (end device) does not understand a header it will negotiate to a common level of understanding. One of the DS is the emergency phone that emergency calls are directed to. In this case the person that occupies this location answers the call by pressing the on-hook/off-hook button and takes the call. Very simple in nature, but it is only used for the single purpose. Another DS is for the dive chamber or Lockout trunk; this device includes an underwater high-pressure speaker as well as a selection switch for the direction of audio. There is no reason that the research found that indicates that this should be an issue to be implemented in SIP.

2.13.4 Sound Powered Telephone interface

This feature is currently done with a circuit that is in the PBX or a custom circuit developed by the integrator of the two systems. This could be done with a media gateway that matches the impedance requirements of the sound powered telephone (SPT) system. There are two types of media gateways to look at. The first is one that supports the Mouth-and-Ear protocol; the other is one that is designed for connection to a radio system, such as the Raytheon ARA-1. [19] If one of these media gateways does not fulfill the requirements then a purchased amplifier or a custom circuit that amplifies the audio signal will need to be developed and then used to feed a media gateway.

2.13.5 Dial Telephone

The Dial Telephone (DT) in many ways is closer to the commercial version than the ICT is. There are two major types of DT, analog (Plain Old Telephone (POT)) and digital phones. The POT is very limited in features and presently connects to the PBX through an analog card. The digital phone is close to the commercial office phone found in many business offices. It connects to the PBX through a proprietary, ISDN, or Centrex interface protocol. The POT may be still required in some cases for intrinsic safety requirements. In those cases a media gateway can be used to connect POT to the IP network. The digital phone solution is the focus of this section. This phone's features are close to the requirements for a corporate office phone. The method used for this phone can be two fold. First is purchasing of a COTS phone, such as a Polycom 301 or 601, and harden the phone to the requirements of the U.S. Navy. This can be done by placing the phone into an enclosure or by removal of the internal circuitry and placing them into a harden phone casing. The other method is to design the phone around a "phones on a chip" and then design the enclosure to meet the U.S. Navy's requirements. Some of the features that are required are Intercom, Push-to-talk and Caller ID that are all handled in the SIP drafts or specifications. See the ICT for a more detailed discussion of the features. With the phone on a chip method you can customize the SIP stack to support the above features and any others that are determined in future requirements. One feature that is new to the specifications is to allow the calling party to control the called party's ability to receive and transmit audio on a hands-free phone, preventing call blocking due to excessive noise. This is a feature that standard COTS phones do not support at this time. In the research, no present phone commercially or in the U.S. Navy was found to support this requirement. In SIP this would require either a separate protocol that the two devices use to signal the microphone or be added to a notify header, that is currently not documented. Another method may be the use of a voice activated switch (VOX) circuit to control the end users microphone. This is outside the scope of this paper.

2.13.6 Recording

Recording on a U.S. Navy vessel falls into two different areas. The first is recording of areas not directly connected to the internal communications of the vessel where the other is recording of telephone calls. The first one is audio that is collected and directed to the recording device. The move to VoIP does not affect this method directly. The hardware that is used for the recording of the telephony must change that may mean that both

recording methods can be effected. The recording of the telephony will change vastly with the move to VoIP. There are two different ways to capture the RTP packets that are on the network. The most common method is to have a server-in-the-middle that has all RTP that needs to be recorded directed to pass through a single server. There are a few disadvantages to this method. This introduces a single point of failure. This method can be done with some vendors PBX, but most vendors use third party products for recording of calls. The other method that some vendors support is promiscuous mode network devices. This network device sits in the network traffic and pulls a copy of the packets that it needs to record and stores them. This method does not have the issue of being a single point of failure, as well as it does not require massive amounts of CPU utilization, since it is not passing all the packets through itself. This method seems to have many benefits over the server-in-the-middle. There is also a draft-sriram-sipping-poc-lip-02 that was developed for lawful intercept to support things, such as CALEA[2], which will also provide a new way to record calls. In the future when the draft becomes a specification it should be re-visited as a method for recording calls.

2.13.7 Conference Bridge

The conference bridge (CB) is very close to the one used in a corporate implementation. Because of this the CB supplied with most IP-PBXs will fulfill the requirements of the derived baseline. Depending on the size of the bridge required and the supplier, the implementation can be done in software or hardware. The monitoring of the CB can be done using a network monitoring tool or a custom application that is designed for only the single purpose of monitoring the CB. Each vendor handles the fail over process differently for the CB. . During the selection process this will need to be discussed and determine if it will fulfill the essence of the requirements.

2.13.8 Electronic Call Accounting System

The Electronic Call Accounting System is commercially referred to as Call Detail Record (CDR). This record is created when a call is made within a PBX. Depending on the manufacturer, it may be only calls that go external of the PBX where other record the station to station calls as well. Traditionally CDR output was directed to an RS232 port

---

2

http://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act 07/24/07

The **Communications Assistance for Law Enforcement Act (CALEA)** is a controversial **United States wiretapping** law passed in 1994 (Pub. L. No. 103-414, 108 Stat. 4279). In its own words, the purpose of CALEA is:

*To amend title 18, **United States Code**, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes.*

The driving force in adopting CALEA was the **FBI**'s worry that increasing use of digital telephone exchange switches would make tapping phones at the phone company's **central office** harder and slower to execute, or in some cases impossible. Since the original requirement to add CALEA-compliant interfaces required phone companies to modify or replace hardware and software in their systems, **U.S. Congress** included funding for a limited time period to cover such network upgrades. CALEA was passed on October 25, 1994 and came into force on January 1, 1995.

that have another piece of equipment/software application running to collect the information that came from the PBX and assemble the record from the individual pieces of information generated by the PBX. In the SIP PBX world, at the highest level it is the same but the method used is different in nature. SIP headers have set messages that can be used to key off of. Even though the INVITE is always there, the BYE is an optional message. Because of this inconsistence, the collection of information has to be gathered from alternate devices that are in the path of the SIP packets. The proxy and session border controller handle the packets and can give detailed information about the call. From the research it appears that the individual vendors each support CDR. The details of the exact information is still unknown for each vendors offering. But the requirements do not seem to be out of the normal requirements that a corporation would require.

2.13.9 Voicemail

All the vendors support a version of Voicemail. With the use of SIP and RFC 3842, presence allows the system to let the user know about the voicemail even when the individual is not at their hard-wired phone. The voicemail can be tied to the individual not a phone, allowing for greater flexibility for the individual sailor, and commanding officer allowing for each to have the mail box customized for their individual needs. The voicemail systems are more in the realm of unified messaging with the different resources combined. The voicemail can be retrieved from a web page or sent to the user by email. Even thou the derived baseline does not address this type of interaction, it does give the U.S. Navy added features even if it is only for a few individuals per vessel. The web interface allows easier management of the voicemails and storage of them, and then the DTMF menu voicemail systems could ever deliver to the end user.

2.14 VoIP GUI Summary

The communication terminal for use onboard surface ships needs to direct the user to the quickest method to achieve his set task within the users' duty station. For the past several years, advances in Graphical User Interface (GUI) design, Human Factures Engineering, and pure processing power have made the development of products more intelligent for the end user. The goal is to leverage this new technology and make the next generation VoIP communication terminal robust and easy to use.

The VoIP communication terminals are used at communications intensive locations. Each VoIP terminal will be capable of supporting four IP phone calls. A typical operator interface will include a colored flat panel display with a touch screen for user selections. The display consists of multiple screen pages, each customized for the intended location of the communication terminal. On startup, the tactical screen will be displayed. The tactical screen provides the essential communications most used for a particular location. The second screen page provides for "quick calls" (speed dial) to other stations often called by terminal location. Both the first and second screens will contain a common area for handling and processing phone calls, status and caller ID information. In addition to a shared common area, utilitarian screens will always be accessible from the tactical and speed dial screens. For example, a single push button will display the dial keypad. The dial keypad will allow the user to dial a specific number or to program the speed dial buttons.

The graphical user interface is the most important interface to the end user. The GUI must provide capabilities for call processing, which includes Call Forward, Call Pickup, Call Drop, Call Transfer, Call Hold, Call Conferences, Call Priority and Call Override or break-in. In addition to call processing, the GUI must provide capabilities for unit configuration. The following list defines Administrative and User configurable options.

Administrative options:

- Customized colors for each call type
- IP-Address configuration
- Retrieve and store user configuration
- Password protected supervisory profiles

User options:

- Speed dial button definition
- Customized ring tones
- Keypad and volume control
- Separate voice volume control for each call
- Separate ringer volume control for each call

The user will have the capability to make various types of phone calls from the Communications Terminal. All calls will use the Session Initiation Protocol (SIP) Stack and communicate through a SIP server via the IP packet network. Specific details

regarding call setup will not be addressed here; rather the types of calls that can be initiated will be addressed.
The communications terminal will be capable of establishing the following types of IP calls:

- Voice calls
- Radio Calls
- Broadcast calls
- Intercom calls
- External Voice calls
- Conferences calls

The development of a new VoIP Communications Terminal requires careful thought from the GUI developers' perspective. The GUI developer must present a user interface that is efficient and functional while attempting to minimize the number of operator actions required to navigate. The developer must see the user interface through the eyes of the user. User controls must also be carefully selected. Many current graphics libraries contain pre-defined user controls for the developer to implement. However, this GUI must utilize a touch screen interface, which makes many pre-defined user controls not usable. User controls that can be operated using a finger instead of a stylus or mouse are desirable.

Considerations must also be given to building portable, reusable code. The developers should refer to reference [20] where the authors explore the benefits of Energy-Efficient GUI Design. In reference [20] the authors categorize GUI design by its purpose, input-centric, content-centric or hybrid. For our purposes, the Communications Terminal is an input-centric design. However, the techniques mentioned in reference [20] make specific recommendations regarding colors, color patterns, and color sequences. Each color handling technique utilizes different amounts of power. This may not be applicable to a fixed communications terminal on board U.S. Navy Ships, however if the GUI is ported to execute on a handheld device, then the power consumption recommendations are highly applicable.

The primary user control on the communications terminal will be the button. The button is a user control that can be programmed to perform different functions. Grouping many buttons together based on functionality determines how the GUI screen layout will be defined. The communication terminal is a touch screen application with the user's finger as the pointing device. With that thought in mind, the developer must analyze the user requirements for the quantity of buttons per screen and create a button that meets those requirements in size and functionality. The common theme is that the buttons are large enough to be pressed/depressed with ease. Sailors must be able to perform their duty under extenuating circumstances. The user must be able to depress any button when wearing fire retardant gloves. This requirement alone limits the size of the button. Button placement goes hand in hand with screen layout. Grouping like functionality creates a very usable display. The new Communications Terminal GUI will also incorporate Color and Audio into its design. Color will be utilized to differentiate what type of incoming call or what call type is programmed on the speed dial screen. Color will also be utilized to differentiate encrypted and un-encrypted IP calls. The intent is to

incorporate as many visual markers to aid the user in the performance of their duty. The Audio portion of an active call is configurable. The user can assign the audio portion to the left, right or both ears of the headset or to the external speaker and can also be muted and/or monitored. The audio voice and volume controls can be individually configured for each active call. This provides greater flexibility and ease of use for the operator at their duty station.

In addition to the Color and Audio requirements, the Communications Terminal GUI must support night mode operation. Night mode operation refers to operating the GUI display in reduced lighting situations. Communication terminals that reside on the bridge of a ship require the terminal to have a dimmer control for the backlight display and the GUI to change to either "Red Text" on a black background or "Blue Text" on a black background. The blue text option is required for night vision goggles. Sufficient thought must be allocated to define the color behavior of Encrypted and Un-encrypted IP calls and for specific call types while in either night mode color.

In summary, the GUI developer has a great many decisions to make in order to define a user friendly, efficient and functional Graphical User Interface for the next generation VoIP Communications Terminal. As previously stated, the developer's role in the GUI development is to present a user interface that is efficient and functional while attempting to minimize the number of operator actions required to navigate. The developer must visualize the user interface through the eyes of the user. That statement demands that the developer completely understand all user requirements and translate those requirements into a modern graphics design. The developer must encapsulate the complexity of the VoIP terminal behind an easy to operate user interface. The next generation VoIP terminal will support four active connections with advanced user controls, which allows for efficient handling of two calls per headset. Allowing two simultaneous users provides dual functionality where each user can be connected to two active calls. This option further improves the efficiency of the next generation Communications Terminal.

2.15 *IAC Security Summary*

VoIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units, and mobile units. In addition to end-user equipment, VoIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Most of these components have counterparts used in data networks, but the performance demands of VoIP mean that ordinary network software and hardware must be supplemented with special VoIP components. Not only does VoIP require higher performance than most data systems, critical services, such as Emergency 911 must be accommodated. One of the main sources of confusion for those new to VoIP is the (natural) assumption that because digitized voice travels in packets just like other data, existing network architectures and tools can be used without change. However, VoIP adds a number of complications to existing network technology, and these problems are magnified by security considerations. [21] VoIP has inherent weaknesses and is vulnerable at multiple points in the network infrastructure. VoIP must be secured in order to ensure the availability of the voice system, and to protect the content value and integrity of voice conversations.

Security is probably the most important part of a converged network consisting of voice and data streams. Aside from the normal security issues revolving around e-mail, network infrastructure and virus scanning, security for the voice must be designed up front. There is no point to deploying a VoIP system without ensuring that the data network is as secure as possible. Adding VoIP to an existing installation requires a robust security analysis prior to making design decisions since security features to lock down the VoIP system can and will have an impact on data throughput.

Security threats are categorized into broad groups that define the type of threat they represent. The major threats to a VoIP network are:

- Theft of Service
- Unwanted Contact
- Denial of Service
- Impersonation
- Eavesdropping
- Interception

Within each threat category, many variations of the threat exist. Theft of service applies to phone services that are stolen, where unwanted contact includes harassment and Spam Over Internet Telephony (SPIT). Denial of service is probably the most disruptive attack where the network resources and bandwidth are exhausted. Impersonation refers to false identities or what rights any individual or group has assigned. Eavesdropping refers to reading or gleaning information from the data packets and packet interception involves actual packet manipulation, packet rerouting and alteration.

Firewalls, gateways, and other such devices can help keep intruders from compromising a network. However, firewalls are no defense against an internal hacker. Additional layers of defense are necessary at the protocol level to protect the voice traffic. In VoIP, as in

data networks, this can be accomplished by encrypting the packets at the IP level using IPSec, or at the application level with secure RTP, the real-time transport protocol (RFC 3550). However, several factors, including the expansion of packet size, ciphering latency, and a lack of QoS urgency in the cryptographic engine itself can cause an excessive amount of latency in the VoIP packet delivery. This leads to degraded voice quality. Careful network design decisions will greatly improve latency.

Remember that VoIP is data and is transmitted in digital packet form. This means that the voice transmissions can be now attacked, hacked, intercepted, manipulated, re-routed and degraded just as any data packet on the data network can. Viruses, worms, Trojan horses, denial of service attacks and hijacking are all possibilities on the VoIP network.

Security must be implemented in a layered approach. This means that security has to involve the entire system. Each component must have a focus on security starting with the End Instrument (IP Phone) by hiding the phone/network parameters. Next the Call Servers, Media Gateways, Session Border Controllers and all Routers, Switches and Firewalls must all be locked down requiring administrative access for management changes and UserId/Password for use. Also, many of the data network precautions, such as virus scan software and an effective patch management system, need to be in place to keep the soft phones, servers and Personal Computers up to date. Next all voice streams and call signaling should be encrypted, ideally end-to-end. Voice should be encrypted with Secure RTP (SRTP) using 128-bit Advanced Encryption Standard (AES) Signaling should use Secure Socket Layer (SSL)/ Transport Layer Security (TLS) wherever possible or alternatively IPSec can be used to encrypt everything.

From a purely network approach; security can be applied by segregation. Each type of VoIP equipment type should be allocated to their own Virtual Local Area Networks (VLANs). VLANs are used to segment voice components and to segment the data network. Softphones that require access to both the voice and data VLANs should be allocated with care. Security studies from National Security Agency (NSA) and Defense Information Systems Agency (DISA) strongly suggest not using softphones or greatly limiting their use.

Physical network security with regards to critical network components, computer rooms, wiring closets, server rooms must have their access controlled at all times. Many network disruptions can be initiated when physical security of the VoIP components has been compromised.

Software management and updating require secure access. The following list outlines some common management recommendations:

- Remote management should only be performed over encrypted connections.
- Proper password management techniques should be used.
- Any default passwords must be changed. Passwords need rotation.
- System actions should be logged with appropriate audit capabilities.
- Only secure connections should be used for web access, i.e., Secure Socket Layer (SSL)/ Hypertext Transfer Protocol Over Secure Socket Layer (HTTPS).
- Set software loads should be encrypted and tamper-proof.
- Network Service providers should run the minimum of services required.

Connection of a set to the system must require an initial authentication and authorization." [22]

To summarize, all VoIP traffic should be encrypted. There are multiple options including VPNs, SRTP (Secure RTP) and IPSec, but making sure that the selected encryption method is efficient and fast is a critical design issue. Otherwise, performance and throughput may be negatively impacted. Segment the network into VLANs that contain like equipment. For example, all softphones belong to their own VLAN as does the data Network. Segmentation provides another form of separation between voice and data traffic. The primary goal is to avoid or greatly reduce the commingling of voice and data traffic on the same network segment. The network must be actively monitored for unauthorized or non-compliant technologies supporting the VoIP network. This includes identifying devices with non-standard configurations. Make VoIP servers physically secure by adopting technologies such as firewalls and intrusion detection. Use firewalls that can handle the unique attributes of VoIP traffic. Require all users to login to access the VoIP network. A VoIP handset should be treated no differently than a user's computer where network access is governed by login and password.

Security policies will differ for each installation. Reference [8] "Network Infrastructure, Security Technical Implementation Guide V6R4" is an excellent resource for guidelines when deploying a security policy across the infrastructure. Reference [7] "IPT & VoIP STIG, V2R2 21 April 2006, Internet Protocol Telephony & Voice Over Internet Protocol, Security Technical Implementation Guide V2R2" provides specific security guidelines for VoIP installations. The Defense Information Systems Agency (DISA) developed references [7] and [8] for the Department of Defense (DOD). The National Security Agency's (NSA) Systems and Network Attack Center (SNAC) have developed additional security configuration guidelines and checklists. Additional information may be obtained from the NSA website outlined in reference [23].

The government and industry have contributed a number of documents for specifying and/or analyzing aspects of VoIP security. This section attempts to identify the some of the most relevant and widely used.

DISA maintains a set of documents, called Secure Technical Implementation Guides (STIGs), that detail how devices need to be designed and configured to meet DISA's requirements for military departments to connect IT assets to the global DoD networks

(specifically to networks connected to the Global Information Grid (GIG) and/or Defense Switched Network (DSN)/ Defense Red Switch Network (DRSN)). These requirements are the basis for DISA's Information Assurance (IA) certification testing. Most devices need to conform to several applicable STIGs. For example, a server on a VoIP network may need to use the VoIP STIG[7], Enclave STIG[24], DSN STIG [25], UNIX STIG[26], etc. Each STIG has an accompanying checklist, which enumerates each requirement in the STIG, instructions to test compliance, and typical steps to remediate non-compliance. Some STIGs, such as the operating system STIGs and some database STIGs, include system readiness review scripts to automate the checklist process. Beyond the DoD, the STIGs can be used as best-practices guides.

The National Institute of Standards and Technology (NIST) has published a few relevant documents. The special publications series SP 800-58 [27] is one of the most comprehensive documents on the subject of securing VoIP systems. It includes a description of security issues affecting VoIP and recommendations (as well as concerns) for deploying COTS VoIP solutions today. NIST is also responsible for the Federal Information Processing Standards (FIPS). FIPS 140-2[28] gives requirements for designing cryptographic modules suitable for protecting sensitive government data. FIPS 140-2 certification is a requirement for any product using encryption to be allowed onto a DoD network.

NIST also plays a role, through the National Information Assurance Partnership, for Common Criteria (CC) evaluations. CC plays a role in Evaluated Assurance Level (EAL) certification, which is a fundamental step for vendors to sell information assurance products to the DoD. The CC framework itself is an ISO/IEC document [29]. It defines the process for building a Protection Profile (PP), which is a set of requirements for a functional device (e.g., a router or firewall). For a product to conform to the PP, the vendor must demonstrate that its product mitigates the threats outlined in the PP.

The best-known requirements document for TDM-based telecommunications systems is Telcordia's GR-815 [30]. Its purpose was to provide requirements for securing the national telephone infrastructure in accordance with the Telecommunications Act of 1996. The document is primarily geared toward securing the core TDM switches (e.g., 5ESS® and tandem switches) and customer premises equipment.

The Alliance for Telecommunication's Industry's baseline security requirements [OAMP] is similar to GR-815, but focus on the management interfaces of IP-based systems (including but not specifically VoIP). Other industry and government specifications and requirements documents commonly cite these requirements.

Telephony requirements tend to use Chairman of the Joint Chiefs of Staff Instruction (CJCSI) instructions instead of DoD instructions. CJCS Instruction 6215.0.B[31] provides policies for DoD voice networks. CJCS Instructions 6510.01D[32] and 6211.02B[33] give requirements for DoD's global telecommunications networks (voice and data) and their interconnections including cross-domain solutions.

2.16 Commercial Off the Shelf

In the past a telephony systems was proprietary and all the parts needed to be purchased from a single supplier. In many ways there were benefits to this model. Individual components worked together and if not you only had a single company to call. The problem was that the company could charge anything it wanted for a part and could force the customer into having to purchase new hardware as the vendor updated their product lines. In many cases the vendor was the only person to support the PBX and new features were slow to evolve. If the manufacturer chose to do a change for the customer they could price it accordingly since there was no competition. The other model was an "Open System" that multiple vendors supported. However, in the telecommunication industry this model was not very prevalent. With the introduction of VoIP and the offshoot of SIP, the "Open System" concept is getting closer to reality. SIP promises to be a standard base protocol that multi vendors will support. See the sections on VoIP Review for more details.
Commercial Off the Self (COTS) is the purchasing of products that are commercially available. The benefits are that the costs of these products are greatly reduced from one-of-a-kind manufactured products. With the mass production also comes the support ability. One issue with COTS is that the product lines change regularly to include new features, but this results in a non-consistence product line. The combining of "Open System" and COTS begins a new direction that should reduce costs in the short term, as well as long-term support.

2.16.1 COTS IP-PBXs

Six vendors were down selected for the focus of this review. In this group there are three influential companies: Alcatel, Avaya and Cisco. The other three companies are all centered on the "open system"; they are: Digium, Pingtel and Sphere. The first two are based on open source products. Each company that was reviewed received a questionnaire that selected key areas that the vendor needed to answer. What was found from the companies is that there are two distinct ways of implementing the VoIP. The first was to implement a proprietary protocol on top of a non-proprietary one, such as Alcatel did with "Universal Alcatel", that runs on top of ITU-T Standard H.323. The other method was using SIP's specifications and drafts to create a system that is developed on the "Open Standards" concept. In many cases they have implemented a feature in a method that is not documented since there is no ratified method. Sphere has taken this approach and has their product JITC certified.
Each vendor that was reviewed had a solution that could be implemented into the U.S. Navy, but had a small deficiency. In most cases the same ones were seen between the different vendors. The area of recording a call is one that a third party product, such as Red Box Recorders, could be used. See the COTs section for more details on different solutions and the methods of recording.
The last question was for each vendor to supply a "recommended solution" that was left open ended to see what kind of responses was received. The resulting responses varied between the different vendors. In many cases a system that was defined around a

corporate design was supplied. The areas that were not covered were connections to the external communications. Several of the vendors have groups that presently deal with the U.S. Navy, so a design focused for the U.S. Navy was expected from those vendors. The overall results of the questionnaires, interviews and research showed that the two types of systems could be acquired, proprietary or open system. In the open system group Sphere stood out; their solution is JITC certified. The proprietary solutions came from the influential companies which needed to have all the features. Alcatel was the most thorough with their responses and displayed a willingness to assist Henschel in their research.

2.16.2 COTS IP-Phones

The area of IP-Phones is very vast in scope. We narrowed the scope by looking at ones that were considered to be mainstream at the time of the research. There were two types of phones found, ones that were proprietary with a firmware update to run SIP or ones that natively ran SIP. In many cases after the firmware update, this became a non-issue. In many cases we found that the phones that are purchased are behind in the firmware level and require updating to the latest version. The phones supported many of the features that are required, with the Polycom line standing out for its native support for SIP. It has features, such as Intercom, that is an interpretation of the draft-ietf-sip-answermode-01 drafts. These phones all had set features and could not be changed by the end user if a new feature was required. Each manufacture supports the RFC 3261 specification and then some limited number of other specifications and drafts. No attempt was made to gather information on how a company would proceed with one of the major manufacturers to support a custom feature. Table 2-6 is a list of the phones that made it into the final selection group:

Table 2-6. Phones Final Selection Group

Feature	Polycom	Polycom	LG-Nortel	Aastra	Snom	Snom	Grandstream	Grandstream
Model	IP601	HD IP650	LIP-6812	9133i	300	370	BudgeTone 200	GXP-2000
SIP	Y	Y	Y	Y	Y	Y	Y	Y
Web Admin	Y	Y	U	Y	Y	Y	U	Y
Micro Browser	Y	Y						
QoS		Y	Y	Y	Y	Y	Y	Y
PoE	Y	Y	Y	Y	N	Y	Y	Y
Hub	Y	Y	Y	Y	Y	Y	Y	Y
#Lines	6	6	11	9	2	12	1	4
Intercom	Y	Y						
G.711	Y	Y	Y	Y	Y	Y	Y	Y
G.723					Y	Y	Y	Y
G.729a			Y		Y	Y	Y	Y
G.729b	Y	Y	Y	Y			Y	Y
G.732.1			Y		Y	Y	Y	Y
G.722	Y	Y			Y	Y	Y	Y

One consistent issue is that the phones will not pass vibration and shock testing. There were also different levels of quality when it came to the casing for the phone. The home office versions were very thin and flimsy, where the executives office phone was a very nicely package phone. The manufacturers do not sell their internal parts as a rule, unless the company wants to buy thousands of them, for repackaging.
Research then was redirected to IP-Phones on a chip to determine how these products will work supporting special features and hardening. These appear to be the direction to take for most phones that are defined in the different ship specifications. These products came with a base line phone code design that could be licensed; a developed version starting from the SIP stack could also be used. Review the open source section for a detailed review of two different SIP stacks. This solution is only good for an IP-PBX that does not use proprietary protocols. In those cases the vendor of the PBX would need to be contacted to determine how their proprietary phones can be repackaged. Further analysis will need to be done to determine the IP-Phone on a chip that is right for the U.S. Navy requirements if an open system IP-PBX is selected. More details can be found in the Embedded section of this paper on the units that were researched from a point of view of specifications and capabilities. Many of the vendors have soft phones that fully support their own feature sets. These phones are installed on a PC and use the audio card for the sound.

2.16.3 COTS Media Gateways

The need for media gateways varies depending on the IP-PBX that is used. Many of the larger vendors have them implemented into their switches where the open system vendors use third party products. The media gateway converts the IP packets to a stream between disparate telecommunications networks. This can be a connection to a radio with the Raytheon ARA-1 that is designed for just that purpose, then a more general connection to typical telephony, such as Analog, ISDN, PRI, or BRI. In some cases an older device can not be updated to a newer design, so the media gateway is used as a converter. The units come in single connection to units that are 48 ports or larger. These larger units are used in many cases to connect to the external PSTN or to support older hardware that can not be updated.

2.16.4 COTS Wireless Products

The concept of wireless frees up the individual from a wire and allows the sailor to be mobile, but still be attached to the network. In many discussions with U.S. Navy and SPAWAR individuals that concept of untethered was very interesting. The technology is being testing in several small pockets in the labs, boat yards and the fleet today. It appears that these pockets are working independently for the most part.
In the past one of the hurdles was the environment of a U.S. Navy vessel that is mainly steel rooms. In this environment the radio waves bounce around causing many issues with the access points. See the section on wireless communications for an expanded review of the subject.

The requirements break up into two separate research projects. The first is the external communications for short distances. The second one is the communications internal to the vessel. From the research it appears that the two types of wireless networks should be developed on different protocols. The external communications for short distances should be developed around WiMAX. An issue that will need to be investigated is the antenna that will be used. The continuous rolling of the vessel will make it hard to direct the signal between another vessel or a land station. The internal communications should be developed around WiFi. New methods of controlling the output of the access points are coming out, so a site plan is not required to tune the system. These new systems from Meru Networks and Alcatel have master/slave configurations that allow the individual access points to appear as a single point of access, as well as control the output power to the individual access points. The benefit of the single point of entry is the end device will not need to authenticate as it moves from access point to access point. The ability of the access points to work together as a single unit allow them to adjust their individual power so there is limited overlap between them, as well as move end devices onto units that have less used bandwidth, resulting in a more load balanced wireless network.

2.16.5 Summary

The individual companies offer several products off the shelf that can be used in the U.S. Navy environment. Most of the products will not meet shock and vibration testing that is required for the harsh environment that they will be exposed to. In some cases the units can be housed in protective cabinets and have isolation from the vibration. In other cases the unit needs to be repackaged. In many cases the unit will not be able to be purchased off the shelf and just installed on the vessel. There are several companies that will take the COTS product and harden it for the environmental requirements.
The technology of the COTS product can be exploited for the U.S. Navy and where the product uses "open system" it should work with other vendor technologies. Even though the proprietary vendors have all the features in a single solution; they limit the ability of the use of other vendor's products in the future. A balance needs to be achieved between the two requirements. The recommendation section will look at balancing this with cost effective methods.

2.17 Open Source

2.17.1 Introduction

This section on Open Source Software (OSS) is meant as a review of the community, and is not meant as a legal analysis. A review of the community at large and who makes up this expanding alternative to proprietary software applications. The Open Source community breaks into two different parts that will be discussed later in this section. Many mainstream products fall under this community like: MySQL, Red Hat, and Fedora. The benefits of Open Source is that it can reduce internal costs of the software and result in faster, development cycles, bug fixes, and collaboration between many developers. Many companies like Google and Amazon have developed their infrastructure around Open Source projects for internal use.

Once the initial investment in source code development has been incurred by the author(s), software can generally be reverse engineered, reproduced and distributed at very little cost. It has become increasingly important to consider upfront and define the rights the author expects to have in the use and distribution of their source code defined in a license agreement. The author is automatically provided certain protection under copyright law, but if the need to defend those rights occurs, it can be very costly. The license agreement is merely a contract between the author and the user(s) on how the source is to be used, if it can be modified, whether derivative works can be created, whether the user can distribute the source alone or combined as a larger program and if royalties are due the author amongst other terms and conditions. These license agreements are put in place to clarify the intent and hopefully insure proper use of the licensed source code (and where necessary, an easier route to stopping misuse of the source code).

2.17.2 Open Source

Open Source in the most general term is software that is distributed with a relaxed license.

2.17.2.1 *The Open Source Definition [34]*

Submitted by Ken Coar

Introduction

Open source doesn't just mean access to the source code. The distribution terms of open-source software must comply with the following criteria:

1. Free Redistribution

The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

2. Source Code

The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of obtaining the source code for no more than a reasonable reproduction cost preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.

3. Derived Works

The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.

4. Integrity of the Author's Source Code

The license may restrict source-code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.

5. No Discrimination against Persons or Groups

The license must not discriminate against any person or group of persons.

6. No Discrimination against Fields of Endeavor

The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

7. Distribution of License

The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

8. License Must Not Be Specific to a Product

The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

9. License Must Not Restrict Other Software

The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.

10. License Must Be Technology-Neutral

No provision of the license may be predicated on any individual technology or style of interface.

Two terms often used when discussing open source. One is the rights given to the developer/author known as "*copyright*" protection, whereby the author's work is protected under patents and trade secret laws from being copied or used in a manner not intended by the author. The second is "*copyleft*", in which the developer/author provides a license to other users whereby the source code is made available for use under certain terms and conditions, in particular the GNU Public License (GPL). the GPL attempts to insure that if derivatives are created, they will be made available under the same terms as the GPL. A review of the various licenses accepted by the Open Source Initiative will find that they vary from very restrictive, such as the Netscape Public License, to the GNU General Public License. The GPL provides that any modified code or code linked to the open source licensed under the GPL also be open source and be made freely available to the license granting free use without restriction. An example of which is the MIT Academic License. When designing if and how a third party source will be used as a part of a product, how the third party's code is licensed and whether their terms and conditions are compatible with the business strategy must be considered.

2.17.3 History

The OSS movement started in 1983 with the name "Free Software" and then in 1998, the name was replaced with "Open Source". In 1997 Eric S. Raymond assembled a group of essays that was called "The Cathedral and the Bazaar". [35] In this work he compared an organized method of development (cathedral) with a development process that contains multiple agendas and approaches (bazaar). He felt that the bazaar method would achieve a better final solution that fulfilled more individuals needs then the structured

development process that was underway in industry at the time. Eric S. Raymond and Bruce Perens formed the Open Source Initiative in 1998. A presentation of Raymond's paper to Netscape convinced the CEO Jim Barksdale to release Navigator source code as Mozilla.

2.17.4 Comparing the Open Source Licenses

There are currently more than 50 licenses that have been accepted by the Open Source Initiative that meet the requirements of the open source community. Of those there are certain licenses that are more widely used and accepted. For reference, see Appendix G "Open Source SIP Whitepaper Phase One" for each of the accepted licenses with active links to the full text. Rather than trying to analyze each license, the components to be conscious of when determining whether or not certain open source is viable for a particular development effort are presented. Note that some open source licenses do not interoperate well with other closed source or open source licenses. It is important to be aware of the compatibility of the licenses when combining or linking source code into a larger program.
The current 50-plus licenses maintained by the Open Source Initiative (OSI) fall into four distinct types. [36]

2.17.4.1 Academic Licenses

Representing the most 'free' of open source licenses, Academic licenses place no requirements whatsoever on the license user. There is not even a requirement for the user to share modifications or redistribute them. Licenses in this category include the BSD (original license from BSD UNIX), MIT Academic license, and Apache licenses. Academic licenses are designed to provide absolute freedom. The only marked restriction is that these licenses prohibit the leveraging of the original licensor's name as an endorsement in marketing efforts. Other than that, these licenses are truly intended for those who seek complete control over the software, its use, modifications, and subsequent re-releases independently or with another software package.
The BSD, granddaddy of open source licensing, originated within the University of California to grant the free use, modification, and distribution of software built within the institution. It has since become a public license available to open source developers.
The MIT was created by the Massachusetts Institute of Technology as a rewrite of the BSD license. The Apache license differs from the BSD and MIT only in its requirement that a notice be included in either documentation or source code of modified works to identify that the new distribution contains software created by the Apache Software Foundation.

2.17.4.2 Reciprocal Licenses

Like other licenses, Reciprocal licenses grant complete rights to the software's use to the developer and end user. The single difference lies in the requirement that any derivatives of the software be released under the same license, and that the source code must be released. The resulting new software must also be free.
The intent of reciprocity is to ensure that a growing universe of free software emerges, and that original works, as well as modified and new efforts, remain free to users. Some

of the most popular software available today remains free and accessible due to its use of the GPL including Linux, MySql, the Bash shell, Mailman, gzip and grep.
The centerpiece of this category is the GPL, by original authors Richard Stallman and Eben Moglen, with input from the open source community at large. The Mozilla Public License also resides in this category.

2.17.4.3 Standards Licenses

Standards licenses seek to create a base standard of software and documentation. Modified and redistributed sources usually have to be distributed as patches, so as to not modify the core.
For example, imagine a situation in which a Web application is created to allow importing and exporting between the various popular blog applications. A Web developer grabs the source of this new software and builds in an additional function to migrate and convert specific design elements along with data. Under a standards license, the core application would be distributed with a plug-in to enable the latter new capability.
The goal of a standards license is to preserve an existing code base so that the originating author can come back to it and evolve it without difficulty. In some cases, plug-ins will not be affected. In others, the original author will update documentation to allow third-parties to update their plug-ins (often also called patches).

2.17.4.4 Content Licenses

Finally, Content licenses cover elements aside from code, such as art, copy and audio/video. Those familiar with Creative Commons (CC) will recognize this license, although a few are listed at OSI, including the Academic Free License.
One caveat with Creative Commons (CC) licenses is that if a Share-Alike attribute is included in a CC license, it makes the license reciprocal, similar to the GPL.

In most instances, in order to comply with the majority of third party licenses, amongst other terms and conditions provided in the individual license agreements, the author must acknowledged and all warranties to the source code be disclaimed unless specific warranties are provided to the user from the author in the license agreement. It is generally a good practice to include the copy right notice and any disclaimers in the installer of the product to ensure that the user is informed.

It is difficult to define a certain process without knowing a specific business model, but an understanding is required that there are critical risks in this arena and diligence processes need to be defined and maintained to limit the risks associated with adoption of open source use.

2.17.5 Open Source Business Model

John Koenig in his paper "Seven Open Source Business Strategies for Competitive Advantage" breaks it into seven different business strategies. Linux has proven how well an Open Source Software (OSS) can benefit companies. HP and IBM derives more then $1 billion in annual service revenue. [37] Oracle is promoting its "unbreakable Linux" guarantee. For the U.S. Navy use of OSS, it does not fall into any of the business models

that Mr. Koenig presents. The U.S. Navy would be using the software internal to their branch of the military. Depending on how it was handled it could be done at the level of the government. The internal use of OSS needs to be evaluated legally to determine how this would work. This evaluation needs to look at the individual OSS license and determine on a license-by-license bases if the government can use it for internal use without violating the licenses.

2.17.6 Giving Back to the Community

The process of giving back to the OSS community sounds very easy at first glance. Again legal evaluation needs to be made to determine if there are reasons that it is not possible. The first area is if the code uses any third party products that are incompatible with the OSS license that it would be released under. Another issue is confidential processes that are added for special reasons, such as security that can not be released. Since after it is release there is no control of the source; this needs to be evaluated. The benefits of releasing changes to the community is that you get the benefit of many more developers than you employ in resolving issues or determining improved logic in solving difficult problems. Since many of the architects of VoIP also participate in the OSS community you are able to get answers on why set specifications were written in particular ways. By using the architect's knowledge you can follow the essence of the specification or draft instead of the interpretation of it.

2.17.7 Overall Conclusion

One of the most important issues you need to define upfront in your product design is whether or not you intend to contribute your source to the open source community or maintain it as proprietary (i.e., commercial). This will impact your decisions to write your own source code or utilized other third party code in your product as you will need to review each third party's license agreement to determine the compatibility of the license agreements. If you intend to sell your software and maintain it as proprietary code than you must take certain precautions in how you design your code around open source code. It is important to not link or combine your proprietary code with open source without careful review of the requirements of the license affiliated with the open source you are seeking to use. Several of the open source licenses intend that you are free to use their source code however you wish, provided, it is for internal use by you as is; should you wish to modify the code in any way or distribute the code, then you need to read the license agreement very carefully to insure compliance. If you have linked your code either dynamically or statically, you are most likely obligated to reciprocate with the open source community and make the closed source you have developed (your proprietary software) available under the same terms as the open source license.

Diligence reviews should occur periodically and not just when the original choice to use the third party software is made as licenses can be updated and or amended without notice in the open source community. The risks under open source licenses are many and must be monitored, not only can the license structure change, but how your developers are using the source may evolve over time;this must be a dynamic process. Inadvertently failing to comply with the license terms can put the U.S. Navy at risk and can hurt the project later in many ways including but not limited to impacting the U.S. Navy's ability

to continue to use the source code. This is not meant to say that there is not effective ways to use open source that will bring tremendous rewards if done right.

If the U.S. Navy goes with OSS, for part of the project the U.S. Navy is not required to have all the application OSS. The limitation is that the U.S. Navy is not able to support proprietary protocols from any of the major vendors. Because of this the U.S. Navy could not use OSS projects for the end devices and expect to be able to use the proprietary protocol from an IP-PBX vendor for extended features. You are able to work with companies that are compliant with the SIP specifications like Sphere or Pingtel.

The end devices will not be able to be purchased from COTS vendor for many reasons, the use of OSS SIP stack may be a good solution to begin from for internal use by the government. There are two other choices: write it from scratch or purchase a SIP stack development tool. Care needs to be taken on the development tool that you will be able to support features, such as special parameters and multiple hooks to the media player that is required for the communication terminal. See appendix OpenSource_SIP_Whitepaper for a detailed review of six OSS projects.

This page intentionally left blank.

3 Technical Detail

3.1 Introduction

This chapter provides a detailed review of the technologies that were researched for this report. This section is intended as a reference to support the initial chapters of this report, as well as the recommendations and conceptual design presented. VoIP is voice packetized and transported over a network; so the base network is the starting point with a detailed review of the infrastructure and different topologies. In this section it supports the use of a mesh of core switches with the edge switches setup in a star topology to achieve the best match between reliability and performance. The next section covers protocols, and codexes that are used for VoIP. This section is limited to only ones that are required to support this VoIP. H.323 and SIP are compared in detail and SIP is determined to be the protocol for VoIP that is becoming the de facto standard in the industry. In the area of codexes it is found that there are several different opinions, but two major ones are ITU-T standards G.711 and G.729 for voice. The G.711 has been in use for many years and has a good Mean Opinion Score (MOS) score. G.729 has a higher compression ratio with almost the same MOS scores. For initial development G.711 has its benefits, but for production G.729 is the one to use if there are bandwidth concerns. The next section goes into more detail about SIP specifications and implementations and using Open Source as a possible development solution. The next several sections address the use of COTS products and how they conform to the requirements of the US Navy physical requirements. Manufactured products, as well as component level devices, are represented. Different mobile communications protocols that are available from COTS manufacturers are reviewed. It was found that for communication internal to the vessel WiFi is a good candidate, where WiMAX is a good candidate for communication external to the vessel. To compliment the COTS products a review of GUI development practices was performed for creating of a communication terminal. This sections ends with a review of security concerns. This section covers vulnerabilities and methods to mitigate them. This covers different protocols, the use of VLANs, and physical protection. This section references several of the appendixes that cover this subject in major detail. The chapter ends with the system integration details that flow into the recommendations and conceptual design for a VoIP solution. The design gives a review of the different components and how they interact with each other.

This page intentionally left blank.

3.2 Network Infrastructure

3.2.1 Topologies

In networking, topology indicates the layout of networking equipment in a logical fashion. Topology provides the logical and virtual structure. Typical topologies are of the following types:

- Bus
- Ring
- Star
- Tree
- Mesh

The following sections discuss each of these topologies.

3.2.2 Bus Topology

Bus networks use a common backbone to connect each and every device. All devices that tap onto the media share a single communication medium. When a device wants to communicate with another device, it broadcasts over the media.

Figure 3-1 illustrates the bus topology.

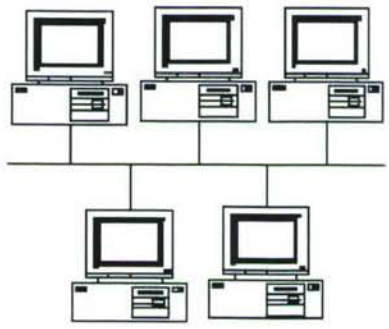


Figure 3-1. Bus Topology

One drawback of this design is that all hosts compete for time on the network media. Only one host can transmit data at any one time on this topology. If multiple hosts attempt to transmit at the same time, a collision condition will exist. This will force each host to stop transmitting for a random period of time before trying the transmission again (from the beginning). The probability of collisions occurring increases with the number of hosts on the network and also their individual need for bandwidth. Performance will be degraded as each host is forced to stop and then restart its transmission. Also, a failure at any point along the bus will cause the entire network to fail.

This topology is not suitable for the ship-wide network of devices for scalability, resilience, performance, and security reasons.

3.2.3 Ring Topology

In a Ring topology each device has exactly two neighbors and messages travel in one direction until it reaches the intended destination. Figure 3-2 illustrates the ring topology.

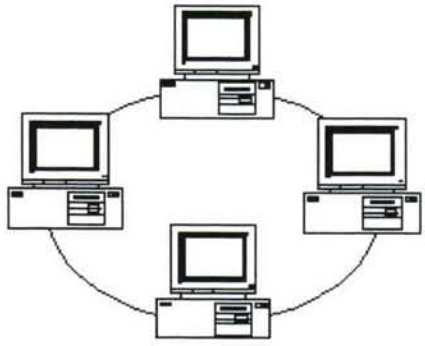


Figure 3-2. Ring Topology

Because a ring topology provides only one pathway between any two nodes, ring networks may be disrupted by the failure of a single link. A node failure or cable break might isolate every node attached to the ring. This topology is not suitable for the ship-wide network for reasons of scalability, resilience, and performance.

3.2.4 Star/Distributed Star Topology

The Star topology features a hub and spoke architecture and is suitable for client-server applications and traffic flows. It is a simple architecture and can be used with modifications or enhancements to enable distributed client-server applications with several hubs (distributed-star). Depending on performance and specially reliability requirement, multiple hubs and multi-homing of the edges to the hubs can result in a highly robust and well performing network. The disadvantage of star topologies is that when the hub fails all devices attached to the hub are affected. Distributed star with hub backups solves that issue to some degree. Figure 3-3 illustrates the star topology.

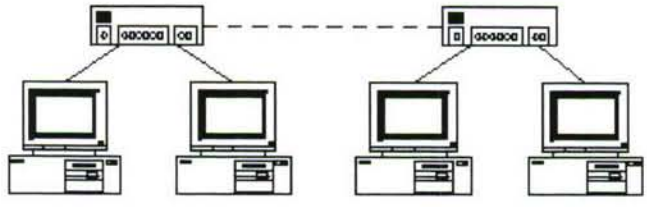


Figure 3-3. Star Topology

Since the Navy applications include such client-server applications like access to Global Command and Control System (GCCS) and other servers from user devices, this topology is worth investigating. From a topological view, it also suits teletraining and bridged conferencing applications.

3.2.5 Tree Topology

Tree topologies can be viewed as multiple ad-hoc stars joined together, in most cases on a bus. The leaves of the trees connect to the edge hub devices, and only the trunk of the tree connects the hubs, which can be a bus. There can be several hierarchical levels in the tree. This hybrid approach leads to a very scalable architecture and works well for large number of devices. Figure 3-4 illustrates the tree topology.

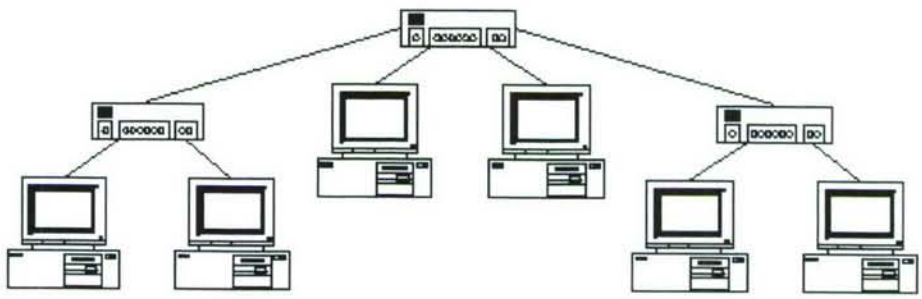


Figure 3-4. Tree Topology

It supports the client-server and computing-cluster types of application flow models. Additionally it suits applications that require communication and interaction with multiple servers attached to different edge hubs, since the tree trunk bus will connect the edge-hubs. Trees can also support peer-to-peer, although the performance will depend on the levels of hierarchy and interconnectivity of the edge-hubs. The disadvantage of the tree topology is that if the backbone trunk or a trunk node fails, entire segments suffer disruptions.

3.2.6 Mesh / Partial Mesh Topology

Mesh networks provide the most connectivity by interconnecting the devices directly. Hybrids like where the end devices are star-connected to the edges and edges are meshed or partially meshed, can be designed based on the traffic flow and performance requirements. Figure 3-5 illustrates the mesh topology.

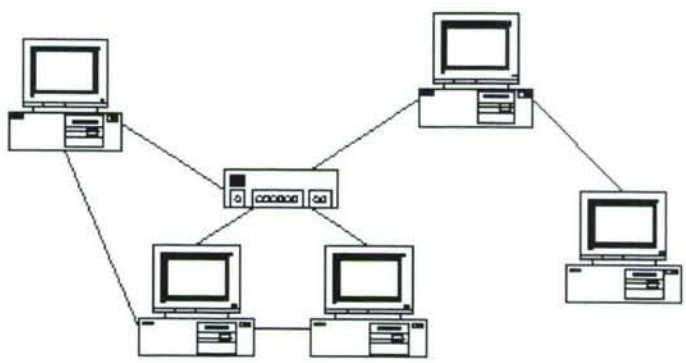


Figure 3-5. Mesh / Partial Mesh Topology

This topology suits well with peer-to-peer traffic flows where communication is primarily from any end-device to any end-device as in case of VoIP. It is also very scalable as adding or disconnecting a device does not alter the topology and the interconnectivity.

3.2.7 Topology Summary

In summary, the bus topology is going to be contention-constrained because of multiple applications and different user communities within the Navy vessel. Bus topology is limited for scalability, resilience, performance, and security reasons. It suits well in relatively small location with specific users and application needs.

The ring topology suits in areas of directional communication among devices, which is not the case here. It is also not well suited for reasons of scalability, resilience, and performance.

The tree topology was considered as a possible candidate as it supports the client-server and computing-cluster types of application flow models and because it suits applications that require communication and interaction with multiple servers attached to different edge hubs. However, tree topologies are primarily architected for reasons of geographic conformity with user communities as in cable networks. Once some of the nodes in the tree's trunk require higher levels of interconnection due to traffic flow requirements or for additions of network and application level functions, the tree essentially becomes a partial mesh topology. Due to the requirements of numbers and types of traffic flows in a multi-application network, it is envisioned that a partial mesh topology is better suited than a true tree topology.

The basic single-star topology features hub and spoke architecture and is suitable for client-server applications and traffic flows. It is a simple architecture and can be used with modifications or enhancements to enable distributed client-server applications with several hubs (distributed-star). Depending on performance and specially reliability requirement, multiple hubs and multi-homing of the edges to the hubs can result in a highly robust and well performing network.

The mesh topology provides the most connectivity by interconnecting the nodes directly. In this case all the edges are meshed then each edge is only one hop away from each other. This provides better performance, especially for peer-to-peer traffic (like VoIP), since traffic between edge switches does not have to pass through the core routers. The trade-offs will be in terms of added links, complexity in configuration when adding nodes, and operations. In most network designs, depending on the performance requirements (e.g., maximum number of hops, latency, jitter, network reliability) instead of a full mesh a partial mesh suffices. The full network is again a hybrid where the end devices are star-connected to the edges and the edges are meshed, based on the traffic flow and performance requirements.

3.2.8 Network Design

Figure 3-6 is a simplified diagram of the network architecture. The network consists of network switches that are used to connect the users (and devices such as Dial Phones, Communications Terminals and IP Speakers) to the network. These are referred to as edge switches. The edge switches are arranged to form a distributed star topology. They support 10/100/1000Base-TX and are capable of providing power to the end-devices (using Power-over-Ethernet) that simplifies end-device installation since there is no need to provide a separate power connection to these devices.

The edge switches are connected to core switches in a meshed topology in a way that the number of hops between edge networks is optimized. The core switch connection is by way of two 1 Gigabit multimode fibers, which provide a high-speed, redundant link to the network backbone (and thus the servers). The core switches are interconnected in a mesh configuration to provide load balancing for increased performance and also to increase the resiliency of the network in the event that one of the core switches fail. The connection between core switches is 10 Gigabit

multimode fibers, which provide ample bandwidth for even the most demanding of applications (i.e. VoIP and Video).

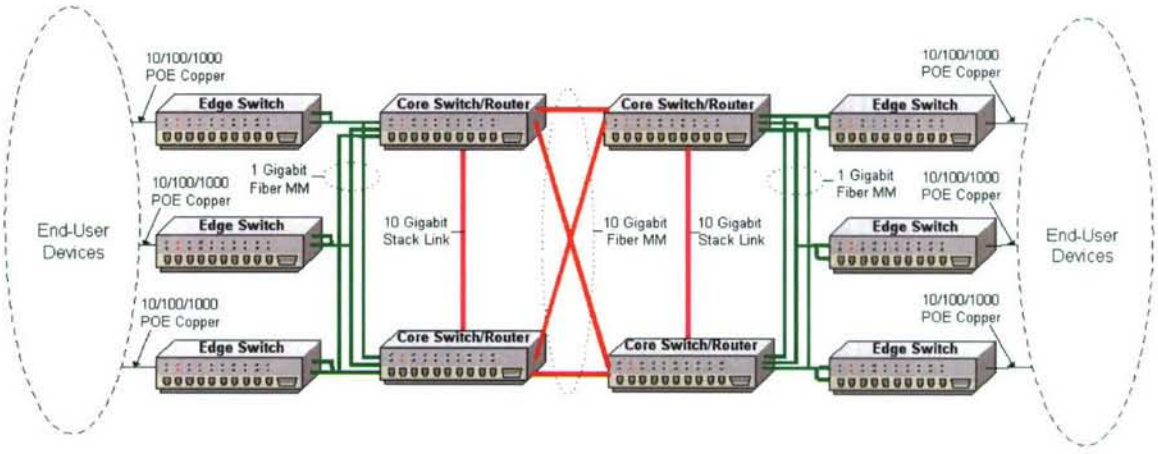


Figure 3-6. Network Diagram

The edge and core switches are managed switches that provide a mechanism for the administration and maintenance of the switches. The switches are configurable remotely through a web-based interface. Network management software will also be implemented to monitor the state of the network, measure performance, and provide alerts should a problem occur such as a failed switch.

VLANs are implemented within the network design for load balancing network traffic between the applications. VoIP traffic is routed over its own VLAN to keep it away from the data traffic going to and from the servers (which are on there own VLAN). This will improve the quality of the voice communication (reduced voice-jitter). Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) are used for enabling loop free topologies with sub-second restoration in case of edge failure. Additional VLANs may be implemented on an as-needed basis.

Support switches are also used in the design within some of the nodes and racks were small switches are required to connect "like" data types together. These will not be managed switches.

Virtual Private Network (VPN) is implemented within the network infrastructure. A VoIP VPN combines Voice over IP (VoIP) and Virtual Private Network (VPN) technologies to offer a method for delivering secure voice. Because VoIP transmits digitized voice as a stream of data, the VoIP VPN solution accomplishes voice encryption quite simply, applying standard data-encryption mechanisms inherently available in the collection of protocols used to implement a VPN such as IPSec (Internet Protocol Security) and TLS (Transport Layer Security).

3.2.9 Network Switch Requirements

3.2.9.1 Edge Switches

The edge switches are 48-port "managed" switches that connect the end devices to the network. The end devices may be, but are not limited to, Dial Phones, Communications Terminals and IP Speakers distributed throughout the vessel and where the runs to the individual end devices are short CAT 5 copper cables. Each edge switch will connect to two core switches through 1 Gigabit multi-mode fiber, resulting in survivability if a single core switch or connection is damaged or fails. This will also allow for load balancing. The edge switches also support Power-over-Ethernet (PoE). The minimum requirements for the edge switches are listed in Table 3-1.

Table 3-1. Edge Switch Minimum Requirements

Requirement	Comment
48 10/100Base-TX auto sensing ports	For user-device connections
Type = Managed	Remotely managed through a web-based and/or command line interface
2 Gigabit Ethernet multi-mode fiber uplink ports	Provides path redundancy to the core switches.
Supports routing (IPv4 and IPv6)	Routes IP Packets
Supports protocols RIP, OSPF, VRRP, DVMRP	Unicast and multi-cast routing protocols
Provides port-based VLAN support	
Implements SSH, SSL, and Syslog	Security features
Supports Spanning Tree protocols STP, RSTP, MSTP, and PVST	Support for single and multiple VLANs
Local console port	Used to administer the switch if remote connectivity is lost.
Supports Power-over-Ethernet (PoE)	To power end-devices (if applicable)
Supports IGMP protocol	Used by hosts and adjacent multicast routers to establish multicast group membership.

3.2.9.2 Core Switch/Routers

The core switches are 24-port "managed" switches that connect to the different major sections of the vessel and maintain multiple connections between themselves in a full mesh configuration for survivability. The core switch/routers will support Power-over-Ethernet (PoE) even though it is meant for support work and they are not expected to be used for end devices or access points. These switches will also implement a 10 Gigabit Stack Link and two 10 Gigabit Fiber Multi-Mode interfaces for redundancy. The minimum requirements for the core switch/routers are listed in Table 3-2.

Table 3-2. Core Switch/Router Minimum Requirements

Requirement	Comment
24 – Gigabit Ethernet auto sensing ports	For connection to edge switches
Type = Managed & Stackable	Remotely managed through a web-based browser and command line interface.
3 – 1 Gigabit Multi-mode Fiber ports	For connection to edge switches
2 – 10 Gigabit Multi-mode Fiber uplink ports (min.)	Provides path redundancy to implement mesh topology.
1 – 10 Gigabit Ethernet stack-link port	
Supports routing (IPv4 and IPv6)	Routes IP Packets
Supports routing protocols RIP, OSPF, VRRP, DVMRP	Supports unicast and multi-cast routing protocols
Provides port-based VLAN support	
Implements SSH, SSL, and Syslog	Supports security
Supports Spanning Tree protocols STP, RSTP, MSTP, and PVST	Supports single and multiple VLANs
1U Rack mountable form factor	
Local console port	Used to administer the switch if remote connectivity is lost.
Supports Power-over-Ethernet (PoE)	Used for support, not for end-devices

Requirement	Comment
Supports IGMP protocol	Used by hosts and adjacent multicast routers to establish multicast group membership.

3.2.9.3 Support Switches

Support switches will be included in some nodes and racks were small switches are required to connect "like" data types together. These switches will be non-managed and will only support a single VLAN. The minimum requirements for the support switches are listed in Table 3-3.

Table 3-3. Support Switch Minimum Requirements

Requirement	Comment
8 – 10/100Base-TX auto sensing ports	For local device connections
Type = Un-managed	
Provides port-based VLAN support	

3.2.10 VLAN

The network has plenty of spare bandwidth so we do not need to add VLANs for performance reasons. We will, however, add VLANs to the network for *load balancing* and *reliability*. VLANs are used to load balance traffic and improve application performance. This is accomplished by keeping VoIP traffic away from the traffic flowing to the servers. The choices for VLAN design are port-based, MAC-based, or protocol-based. A port-based design is typically used since MAC-based and protocol-based VLANs are difficult to administer because of the necessity to install MAC address tables, or protocol policies on each switch.

An access port to an end-device (PC, printer, server, IP phone, etc.) is associated with a VLAN number. Traffic from a VLAN access port is "tagged" with that VLAN number as it is forwarded through the switched network. One can associate a VLAN with a specific type of equipment, such as a PC or VoIP phone, or (more commonly), one can make the port-based VLAN geographical-based, meaning that all ports in one section of the ship will be in the same VLAN. Usually administrators will use both schemes, for example, make the VLANs geographic-based, except for the VoIP phones, which will be on their own VLAN.

Along with a VLAN design, we will also create a spanning tree for each VLAN – using MSTP or PVST – so that the VLANs do not have a common spanning tree root. Utilizing MSTP requires careful design so that the spanning tree will cut off appropriate links to balance traffic through the network. This will require setting bridge priorities on the switches, and if necessary, link weights.

Figure 3-5 shows the network model for the meshed topology. This figure also shows the spanning tree for this network. The main purpose of this network design is to decentralize the network, which improves peer-to-peer performance, such as VoIP, yet maintains the performance of client/server applications. Two roots (each for VoIP and Data) are shown in Figure 3-7. Each root handles separate sides of the network.

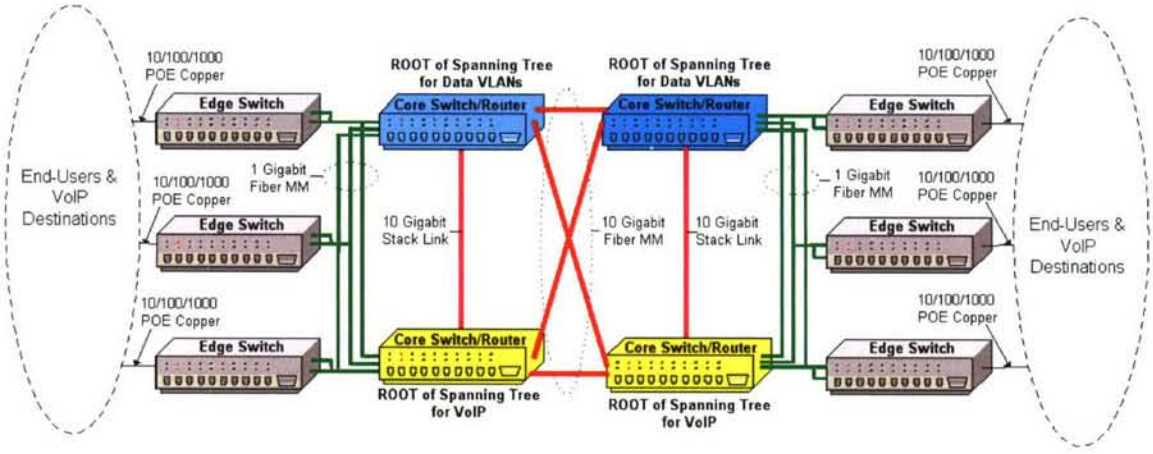


Figure 3-7. VLAN Diagram

3.2.11 Network Management

3.2.11.1 Switch Management

Managing the configuration of network switches can be a daunting task on medium to large scale networks. A means of centrallized management is a neccessity.

Listed below are management features typically found in a managed switch:

- Turning on and off a particular port range
- Setting link speed and duplex mode
- Setting port priority
- Filtering MAC addresses – and other types of "port security" features which prevent MAC flooding
- Use of Spanning Tree Protocols (STP and MSTP)
- SNMP monitoring of device and link health
- Port mirroring (also named: Port monitoring, spanning port, SPAN port, Roving Analysis Port, link mode port)
- Link aggregation (also called: bonding/trunking)
- Setting and managing VLAN configurations.

The switch should provide a serial console to allow the administrator to configure the switch in the event that the switch is not reachable remotely because of either a network failure or unintential misconfiguration of the switch. Management through a command-line interface via Telnet and SSH should also be supported. More recent devices also provide a web interface. Limited functions, such as a complete reset by pushing buttons on the switch are usually also provided.

3.2.11.2 Network Management

Network management refers to the maintenance and administration of large-scale computer networks and telecommunications networks at the top level. Network management is the execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network, including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing,

cryptographic key distribution authorization, configuration management, fault management, security management, performance management, bandwidth management, and and accounting management.

Data for network management is collected through several mechanisms, including agents installed on the infrastructure, synthetic monitoring that simulates transactions, logs of activity, sniffers and real user monitoring.

At minimum, the network management software should have the following features:

1. Performance Monitor – Monitors and alerts on availability, bandwidth utilization, CPU load, memory and disk space utilization.
2. Device Monitor – Monitors the availability of devices and provides alerts the moment a router, circuit or server becomes unavailable.
3. Network Discovery – Performs a detailed discovery on one device or scans a range of subnets.
4. Real-time Interface Monitor – Displays statistics from routers and switches such as packet loss count, response times, and total packet counts processed.
5. Port Scanner – Allows testing for open TCP ports across IP Address and port ranges or selection of specific machines and ports.
6. Network Mapping – Automatically maps the network and provides a graphical view of the network infrastructure (devices and connections) to reduce the burden of network troubleshooting.

3.2.12 Protocols

This section describes the Layer 2 through Layer 4 network protocols used on an IP based network with the exception of SNMP, which is a Layer 7 protocol.

3.2.12.1 Routing Protocols

- **RIP**
  The Routing Information Protocol (RIP) is used by routers to dynamically adapt to changes of network connections by communicating information about which networks each router can reach and how far away those networks are.

OSPF
The Open Shortest Path First (OSPF) protocol is a hierarchical interior gateway protocol (IGP) for routing IP packets. OSPF uses path cost as its basic routing metric. In practice, it is determined by the speed (bandwidth) of the interface addressing the given route, although that tends to need network-specific scaling factors.

- **VRRP**
  The Virtual Router Redundancy Protocol (VRRP) is used to add additional resiliency to increase the availability of the routers servicing hosts on the same subnet. This increased reliability is achieved by advertising a "virtual router" (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router.
- **IGMP**
  The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. Spanning Tree Protocols.
- **STP**
  The Spanning Tree Protocol (STP), creates a spanning tree within a mesh network of connected Layer-2 switches, and disables the links which are not part of that tree, leaving a single active path between any two network nodes. The purpose of this is create a loop-free infrustructure within the mehed network.
- **RSTP**
  This protocol provides for faster spanning tree convergence after a topology change then STP.
- **MSTP & PVST**
  A VLAN design requires replacing the single spanning tree (running RSTP) with multiple spanning trees (running MSTP or per-VLAN Spanning Tree (PVST)) in order to improve the performance and resiliency of the network and applications. These protocols are used for enabling loop free topologies with sub-second restoration in case of router failure, switchover, or the addition of routers to the network

3.2.12.2 Network Management Protocols

- **SNMP**
  Simple Network Management Protocol (SNMP) is used as the transport protocol for network management. Network management consists of network management stations communicating with network elements such as hosts, routers, servers, or printers. The agent is the software on the network element (host, router, printer) that runs the network management software. The agent stores information in a management information base (MIB). Management software polls the various network devices and gets the information stored in the MIB.

3.2.12.3 Network Supporting Protocols

- **IP**
  The Internet protocol (IP) suite is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run. It has also been referred to as the TCP/IP protocol suite, which is named after two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were also the first two networking protocols defined. Today's IP networking

represents a synthesis of two developments that began in the 1970s, namely LANs (Local Area Networks) and the Internet, both of which have revolutionized computing.

- **TCP**
  The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol (IP) suite, often simply referred to as TCP/IP. Using TCP, applications on networked hosts can create *connections* to one another, over which they can exchange streams of data using Stream Sockets. Unlike the UDP protocol this protocol guarantees reliable and in-order delivery of data from sender to receiver. TCP also distinguishes data for multiple connections by concurrent applications (e.g., Web server and e-mail server) running on the same host.
- **UDP**
  User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as *datagrams* (using Datagram Sockets) to one another.

  UDP does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order, appear duplicated, or go missing without notice. Avoiding the overhead of checking whether every packet actually arrived makes UDP faster and more efficient, at least for applications that do not need guaranteed delivery. Time-sensitive applications often use UDP because dropped packets are preferable to delayed packets. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients. Unlike TCP, UDP supports packet broadcast (sending to all on local network) and multicasting (send to all subscribers).

- **ARP**
  The Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address when only its IP address is known.

- **ICMP**
  The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol (IP) suite. It is mainly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

3.2.13 Multicast

To support functionality required by, for example, an announcing system, IP Multicasting is needed to handle the many-to-many communications over an IP infrastructure. It scales to a larger receiver population by not requiring prior knowledge of who or how many receivers there are. Multicast utilizes the network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers. The nodes in the network take care of replicating the packet to reach multiple receivers only where necessary.

A multicast address is associated with a group of interested receivers. According to RFC 3171, addresses 224.0.0.0 to 239.255.255.255 are designated as multicast addresses. This range was formerly called "Class D." The sender sends a single datagram (from the sender's unicast address) to the multicast address, and the routers take care of making copies and sending them to all receivers that have registered their interest in data from that sender. The 224.0.0.0 to 224.0.0.255 range is assigned to multicasting on the local LAN only. Well known examples are RIPv2 which

uses 224.0.0.9 and OSPF which uses the 224.0.0.5 address. Multicast addresses in IPv6 all have the prefix ff00::/8. Address assignments from within this range are specified in RFC 2373.

The implementation of the multicast concept on the IP routing level, is where routers create optimal distribution paths for datagrams sent to a multicast destination address spanning tree in realtime.

3.2.14 VPN

A virtual private network (VPN) is a communications network tunneled through another network, and dedicated for a specific network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

A VoIP VPN combines Voice over IP (VoIP) and Virtual Private Network (VPN) technologies to offer a method for delivering secure voice. Because VoIP transmits digitized voice as a stream of data, the VoIP VPN solution accomplishes voice encryption quite simply, applying standard data-encryption mechanisms inherently available in the collection of protocols used to implement a VPN.

Security is not the only reason to pass Voice over IP through a Virtual Private Network, however. Session Initiation Protocol (SIP), a commonly used VoIP protocol is notoriously difficult to pass through a firewall because it uses random port numbers to establish connections. A VPN is one solution to avoid a firewall issue when configuring remote VoIP clients. The VPN virtually moves users inside the same network local as the VoIP server.

Encryption algorithms perform many, highly complex, operations on individual bits or small blocks of bits. This makes them very computationally intensive. Even though both symmetric and asymmetric cryptosystems can be implemented in hardware or in software there are a number of things that must be taken into account. Although either system could be implemented in software with the intent of running on a general purpose CPU (i.e. a PC) the result would not be particularly efficient. First, general-purpose processors are not particularly suited for the type of mathematical operations required for encryption. In addition, encryption is also normally very CPU intensive. This type of implementation would quickly consume the resources of the CPU in question. It is therefore highly desirable to "offload" encryption operations to separate hardware. This would allow the general-purpose processor to continue its normal duties without adversely impacting its performance.

In addition to the performance benefits, implementing encryption systems in hardware also brings security benefits. Depending on the environment and the secrecy level of the information in question, it may be necessary to take additional precautions. Hardware is self-contained and can be made tamper-proof. It can also be further isolated from potential snooping by shielding and TEMPESTing the hardware to prevent electromagnetic leakage. Software implementations, on the other hand, suffer the potential of modification while in memory without warning to other users.

It is therefore, highly recommended that any systems that will be involved in encryption and decryption have separate hardware encryption modules. This will prevent the crypto functions from interfering with the normal operating functions of the system. In the case of VoIP systems this means handsets and communications servers/gateways. If the system in question is to be a pure VoIP system where no calls are made via the PSTN, then the handsets must support

hardware-based cryptosystems. In this case, the communications server/gateway is used purely for signaling while the voice content is sent handset-to-handset via SRTP and the encryption/decryption is being performed only at the handset. Note that routers, switches, and other network gear need not support encryption mechanisms because they are being used purely as transports. However, if the system is to involve encrypted tunnels between networks then some network gear will require hardware-based encryption support. In general, any system that will perform the actual encryption/decryption should do so in hardware. Systems that merely transport encrypted sessions need not support it in any way [10].

One common way of implementing a VPN is by using IPSec, which is a set of IETF standards for securing Internet traffic. IPSec operates at Layer 3 (the network layer) and hence protects any type of Internet traffic, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP), regardless of the application. Commercial Virtual Private Network (VPN) solutions commonly use IPSec for secure remote access.

IPSec can operate in either of two modes, transport mode or tunnel mode. In transport mode, the original IP header is unmodified (passed as clear text). In tunnel mode, a new outer IP header encapsulates the original IP header, such that the original IP header can be encrypted and protected end-to-end. Tunnel mode may be used between routers (or VPN gateways) to protect the privacy of the end hosts behind each router or gateway. [38]

This page intentionally left blank.

3.3 Protocols/Codeces

3.3.1 Introduction

The infrastructure and topology is very important to the design of the IP packet based network and is discussed in another section. After these two elements are defined, then how it will be transported will be the next major piece. The last complimenting component of the IP network is how will it be packaged and transported on the IP network. Without these decisions being made upfront the network will be disjointed and very hard to converge and have the ability to expand as the utilization requirements changed overtime. Some of these decisions will be influenced by the selection of IPv6 or IPv4; what will also impact security. The next couple sections will review different VoIP, video and data protocols' features and capabilities. The last sections will concentrate on the codexes for VoIP and video and their characteristics and bandwidth requirements. To begin this discussion, a review of the Open System Interconnection Server Layer Model will be examined.

3.3.2 Protocol Reference Architecture

The reference models for communications among distributed computing systems is a framework or standard that helps organize functionally separate functions in hierarchical layers and leads to an overall architecture. This architecture is then used for designing the network with interoperable components that provide functions specific to each layer. As networking applications grew, the architectures were put forth to help developers so applications can be developed easily and to ensure interoperability so that multi-vendor products specific to a layer will work with each other as well as with vendor products designed for other layers. Two major reference models are of importance and they are discussed below.

3.3.3 International Organization for Standards (ISO) Open System Interconnection (OSI) Seven Layer Model

As data communications applications took hold in the mainstream and soon concurrence became important for global communications companies and equipment manufacturers, the ISO organization took the task for building a standard reference model and developed the OSI networking suite [40]. It has two major aspects (1) a functional networking model, also called the Basic Reference Model or the 7-Layer Model, and (2) a set of protocols between corresponding layers. The reference model has become the defacto standard followed by the computing and networking industry worldwide and is roughly followed by all, while the protocols in the OSI standard are not accepted to that extent any more as new technologies and more efficient, optimized, and function-specific protocols have been constantly developed. In this model, a networking system is divided into seven hierarchically organized layers. Distinct functions for each layer and the interfaces between the layers are specified. Within each layer, one or more entities implement its functionality. Each entity interacts directly only with the layer immediately beneath it, and provides facilities for use by the layer above it. Protocols enable an entity in one host to interact with a corresponding entity at the same layer in a remote host. The whole idea is interoperability, i.e., products targeted for a single layer by many vendors should be able to interoperate with other vendor products at the same layer or layers directly above and below. Note in the 7-Layer Model described below that OSI 7-layer model is now taken as a guideline. In reality, "protocol stacks" are implemented by combining one or more of the OSI layers into a single layer. Ethernet and Frame Relay (FR) provide functions for both Layer1 and Layer 2, and in the Internet suite Layer 7 through Layer 5 are combined.

By the late 1980's, ISO was recommending the implementation of the OSI model, but by that time, TCP/IP had been in use for years in ARPANET and other networks that evolved into and worked with Internet.

Layer 7

The Layer 7 **Application Layer** provides a means for the user to access information on or from the network through applications working with the operating system (OS) of the computer. Obviously, the same application protocols mentioned in DoD 4 or 5-layer model also apply here.

Layer 6

The Layer 6 **Presentation Layer** describes how the application layer data is wrapped, i.e., the syntax of data being transferred. Protocol or format conversion, encryption / decryption, or any manipulation of application data before passing it to the network is modeled for this layer. Example protocols for this layer will be American Standard Code for Information Interchange (ASCII), Moving Pictures Expert Group (MPEG), etc. Very few applications actually used it as prescribed in reality.

Layer 5

The Layer 5 **Session Layer** function is to establish, manage, synchronize, and terminate the sessions between the local and far end applications. An example of a Session Layer protocol is Session Description protocol (SDP). Very few applications actually used it as prescribed either and were rarely supported.

Layer 4

The Layer 4 **Transport Layer** deals with reliable data transfer, end-to-end error recovery, and flow control functions ensuring that packets are transmitted properly. Both connectionless and connection oriented sessions may be set up requiring different treatments for these functions. Typical protocols in this layer are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Stream Control Transmission Protocol (SCTP), etc.

Layer 3

The Layer 3 **Network Layer** provides the routing function for transporting packets from source to destination devices via one or more networks involving various data links. The packets may have to be fragmented/segmented, sequenced, and rebuilt. It also tracks and reports errors, may inform about congestion, and is responsible for maintaining quality of service as can be managed at the packet level. Typical protocols are Internet Protocol (IP), Internet Control Message Protocol (ICMP), X.25 Layer 3 (obsolete), etc.

Layer 2

The Layer 2 **Data Link Layer** encodes/decodes the packets from Network Layer into bits and vice versa. The bits are organized into logical aggregates called frames. The functions here include handling errors by using checksums, flow control, and frame synchronization. This layer may be split further into Media Access Control (MAC) and Logical Link Control (LLC) sub-layers. Bridges, and Switches operate at this layer and typical protocols are Point-to-Point protocol (PPP), High level Data Link Control

(HDLC), Address Resolution and Reverse Address Resolution Protocols (ARP/RARP), and X.25 Layer 2 (obsolete).

Layer 1

The Layer 1 **Physical Layer** defines the functions necessary to connect, control, and disconnect physical equipment and media necessary for communications, the signaling used, and the associated protocols. All electrical impulse, optical or radio signals, physical specifications for devices such as pins, voltages, radio and coaxial and fiber specifications, etc., are part of this Layer. The functions at this layer include establishment and termination of connections to the physical medium, contention resolution if multiple devices are accessing the medium, flow control, and modem functions. Examples of typical specifications for this layer are RS232, X.21, and X.25 Layer 1 (obsolete).

3.3.4 TCP-IP Model / DoD Four (or Five) Layer ARPANET Reference Model

Some historical background of VoIP, the Defense Advanced Research Projects Agency (DARPA) funded the research to start building the packet switching communication model and infrastructure. One of the results was the DoD Four-Layer Model. Also known as Advanced Research Projects Agency Network (ARPANET) reference model, or the TCP-IP model, the communications between geographically distributed computers was developed in early 1970s for the DARPA Internet project that eventually grew to today's Internet. The structure of the Internet reflects the DoD model closely. So, it is important to note that this model was developed even before the OSI 7-Layer Model. Unfortunately there is no official documented version of this model and sometimes it is shown as a four-layer and sometimes as a five-layer model. Although the ARPANET Working Group disbanded without any official document, a very lucid, fun-to-read request for comments (RFC) [39] is written by M. A. Padlipsky, one of the ARPANET developers, describes the conceptual framework for the ARPANET protocol suite. The document also compares and contrasts the ARPANET Reference Model with the ISO Reference Model.
The four layers in ARPANET reference model are:

- Layer 4 - **Process Layer or Application Layer**, where the "higher level" application protocols, such as SIP, Real Time Protocol (RTP), Dynamic Host Configuration Protocol (DHCP) / Domain Name Server (DNS), Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Secure Shell (SSH), Transport Layer Security (TLS), Secure Socket Layer (SSL), etc. operate.
- Layer 3 - **Host-To-Host (Transport) Layer** deals with opening and maintaining connections, and ensuring that packets are in fact received. Flow-control and connection protocols such as TCP, UDP, SCTP, etc. operate in this layer.
- Layer 2 - **Internet or Internetworking Layer** defines the routing schemes for navigating packets from one IP address to another, using protocols like IP, ICMP, and IP Security (IPsec).
- Layer 1 - **Network Access Layer** - This layer describes the physical equipment necessary for communications, the signaling used on that equipment, and the associated protocols.

Splitting Layer 1 into a Physical layer and a Network Access layer or Data Link Layer derives the five-layer model.
The hierarchical nature of the layers and the interrelationship among them approximately follows the same description and processes as in the OSI 7-layer model described in the section above and so is not repeated needlessly.

3.3.5 VoIP, Video, Data, and Multimedia Applications Enabling Protocols

VoIP, video, data, as well as multimedia applications are enabled at present by two major application layer protocol suites: SIP and H.323. Both of these protocols provide different approaches to the problem of signaling over IP networks. H.323 first appeared around 1996 and was adopted by most manufacturers as a signaling protocol over which to carry their proprietary voice and video protocols. SIP, in concept, appeared in 1998 but was not fully ratified until 2000. Additional specifications and Requests for Comment (RFCs) have been appearing since then and both protocols continue to evolve today. However, SIP is rapidly becoming the signaling protocol of choice for VoIP. For more information on SIP and H.323, and the features and benefits of each, please see appendix "Network Infrastructure Part 1a-SIP vs. H323 Comparison": A Comparison of SIP and H.323 for Internet Telephony by Henning Schulzrinne (Columbia University) and Jonathan Rosenberg (Bell Labs).
It should be noted that regardless of the signaling protocol used for multimedia applications, some form of QoS must be used alongside. Protocols such as 802.1p, Differentiated Services (DiffServ) or Resource Reservation Protocol (RSVP) are used to guarantee packet delivery in a timely and jitter-free manner. These guarantees are necessary in order to deliver high quality voice and video.

3.3.6 Feasibility/Applicability Issues for Use by the Navy

Besides the inherent pros and cons of both SIP and H.323 there are no known issues related to use of VoIP, video, and data in a converged networking infrastructure that would prevent either's use in naval communications, be it on-board, ship-to-shore or on navy bases.

3.3.7 Product Support of Features/Capabilities

Because both H.323 and SIP operate at the applications layer above layer 3 there is no need for support of the protocols themselves as it relates to network infrastructure. In other words, they are presented to switches, routers, firewalls, etc. purely as payload. They need only be supported by related infrastructure such as handsets and communications server/gateways. Most manufacturers today support SIP as a signaling protocol. They support SIP natively with a restricted subset of features but also use it purely as a signaling protocol over which their own proprietary protocols are run. Cisco's "skinny" protocol provides a good example of this. Alcatel-Lucent, on the other hand supports both SIP and H.323. H.323 is used as a transport for its proprietary protocol "Universal Alcatel" or "UA". SIP is supported natively with a subset of basic telephony features and also as a signaling protocol in combination with HTTP and Voice eXtensible Markup Language (VxML) in the case of softphones. In the meantime the Internet communities along with the Internet Engineering Task Force (IETF) are working towards expanding SIP's functionality in order to support a larger set of telephony features natively.

3.3.8 Characteristics of Voice and Video Codecs

This section includes our findings on characteristics of different voice and video codecs utilizing industry standard specifications (such as, G.711, G.722, G723.1, G.726, G.728, G.729, internet Low Bitrate Codec (iLBC), Speex, H.261, H.263, and H.264). The characteristics covered in this section, pertain to the areas of algorithm, bandwidth used for sound, overhead, bitrates, and Mean Opinion Scores (MOS).

3.3.8.1 G.711 Voice Codec

G.711 is an international ITU-T standard [46] for encoding and decoding speech. The standard was developed in the 1960s and was published in 1972.

Sampling/Encoding: 711 employs the simplest form of waveform coding, an approximately logarithmic pulse code modulation (PCM) scheme for sampling signals of voice frequencies. G.711 encodes frequencies in the range of 0 to 4 kHz (kiloHertz), which is effective for normal speech. The sampling rate is then 8kHz or 8000 samples per second by Nyquist theorem. Each sample is coded in 8 bits, yielding a 64 kbps (kilobits per second) coding. Because of the low complexity, the codecs are very fast and result in low delay and excellent quality.

MOS published for G.711 through Perceptual Speech Quality Measure (PSQM) testing indicates a range of 4.45 in ideal condition to 4.13 in stressed condition. A comparative table for MOS scores is given later in this section.

A-law and μ-law: There are 2 variant schemes within G.711, the A-law and the μ-law. μ-law is used in the US and A-law is used in most other countries internationally. Both use a roughly logarithmic scheme in which the lower the signal, the more is the granularity. μ-law uses 16 segments (8 each in both positive and negative directions) where the range doubles from one segment to the next. In μ-law, there are 16 intervals in each segment, yielding 256 intervals coded in 8-bits. A-law also has 256 intervals coded in 8-bits, but it uses 14 segments, while using the lowest 2 segments with 32 intervals and the rest with 16 intervals each. Thus A-law is skewed towards greater fidelity for smaller frequencies at the expense of higher ones. G.711 includes algorithms for Packet Loss Concealment (PLC) in G.711 Appendix I, and Voice Activity Detection (VAD) and Comfort Noise Generation (CNG) in G.711 Appendix II.

3.3.8.2 G.726 Voice Codex

G.726 is an international ITU-T standard [VOC2] encoding/decoding scheme. It was published in 1990 as it superseded previously introduced standardized coding schemes, G.721 (a 32 Kbps coding) and G.723 (24 and 40 kbps coding), based on the same Adaptive Differential Pulse Code Modulation (ADPCM) coding scheme.

Sampling/Encoding: G.726 employs ADPCM, a variation of waveform coding. Instead of coding the speech samples directly like in G.711 PCM, ADPCM quantizes the difference between the actual speech signal and a prediction of the sample. The predictions are based on correlations present in the samples due to the effects of the vocal tract and the vibration of the vocal chord. If the model of the vocal tract and its vibrations is good, then the error between the actual speech and the predicted sample is minimal and the differences can be quantized in fewer bits than what is needed in quantizing actual samples as in G.711. The decoder employs a reverse process of adding the predicted sample to the quantized difference to reconstitute the actual speech sample. So, there are the two major components that affect the ADPCM coding – adaptive predictor and quantizer and how well they adapt to the changing characteristics of the speech being coded.

The sampling frequency in G.726 is 8 kHz, encoding audio frequencies in the range of 0 to 4 kHz, same as in G.711. However, in the ADPCM coding, an adaptive 31, 15, 7, or 4-level quantizer is used to assign 5, 4, 3, or 2 bits respectively to the value of the difference signal (actual minus predicted). This results in the bit rates of 40, 32, 24, and 16 Kbps respectively. Obviously the G.726 is more complex than G.711 and adds typically a delay of 125 μs, quite imperceptible. The most commonly used mode of G.726 is 32 Kbps. The rate doubles the usable network capacity as it is half that of the G.711 rate. MOS published for G.726 through PSQM testing indicates a range of 4.3 in ideal condition to 3.79 in stressed condition. A comparative table for MOS scores is given later in this section.

3.3.8.3 G.722 Voice Codec

G.722 is another international ITU-T speech coding standard [48] based on ADPCM and published also in the 1980s.

Sampling/Encoding: Speech coding for bandwidths wider than 4 kHz (as used in G.711 and G.726) results in better represented speech quality and clarity. In G.722 coder, a wider frequency range (roughly 7 kHz) of speech is sampled by 16 kHz sampling rate. G.726 is a wideband ADPCM-based speech coder that uses sub-band splitting. Sub-band splitting, based on two identical band pass filters, divides the 16 kHz ADPCM samples into two 8 kHz sub-band samples. The coding of the sub-band samples is based on a modified version of the G.721 (or G.726) ADPCM speech coder.

G.722 complexity adds typically a delay of around 3 ms (milli-second). The codec provides acceptable performance (a MOS score of 3.0) for transmission BER up to 10^{-3}. A University of Maryland Institute for Advanced Computer Studies show MOS for G.722 ranging from 4.3 at BER=0 to 3.0 at BER=10^{-3} for 64 Kbps codec and 3.8 at BER=0 to 3.0 at BER=10^{-3} for 48 Kbps codec. A comparative table for MOS scores is given later in this section.

There are later variants of G.722, such as the G.722.1 [49] and G.722.2 [50] that offers lower bit-rate compressions.

3.3.8.4 G.728 Voice Codex

G.728 is an international ITU-T speech coding standard [51] published in 1992. It is based on Low-Delay Code Excited Linear Prediction (LD-CELP) algorithms developed at the Bell labs.

Sampling/Encoding: The quality of speech rendered by the waveform codecs previously discussed deteriorate sharply at bit rates of around 16 kbps. For lower bit rates, the hybrid codecs, especially CELP and its derivatives are useful, given that their relative high delays due to forward look-ups are acceptable. G.728 LD-CELP uses backward adaptation of past speech frames rather than buffering a typical input speech frame of 20 ms or so. It enables the G.728 codec to use a much shorter frame length than previous CELP codecs.

G.728 uses a frame length of 5 samples giving it a total delay in order of a ms. G.722 complexity adds typically a delay of around 3 ms. There are other algorithmic improvements that led to this codec at 16 kbps bit rate with speech comparable to that of G.726 and a good robustness to bit error rate (BER). MOS values for G.728 range from 3.61 to 4.0 at 0% packet loss. A comparative table for MOS scores is given later in this section.

There are later variants of G.722, such as the G.722.1 [49] and G.722.2 [50] that offer lower bit-rate compressions.

3.3.8.5 G.723.1 Voice Codec

G.723.1 is an international ITU-T speech coding standard [52] that was first adopted in 1995.

Sampling/Encoding: G 723.1 is a low bit rate coder used for compressing speech or audio component of multimedia services as part of H.323 and H.324. G.723.1 coder operates with a digital signal obtained by first performing bandwidth filtering of the analogue input, then sampling at 8 kHz sampling rate and then converting to 16-bit linear PCM for the input to the encoder, just as in waveform coding. The output of the decoder should be converted back to analogue by similar means. The difference in this codec is that the coder is based on the principles of linear prediction analysis-by-synthesis coding and attempts to minimize a perceptually weighted error signal. The encoder operates on blocks (frames) of 240 samples each. That is equal to 30 msec. at an 8 kHz sampling rate. G.723.1 offers a dual rate of 6.3 kbps based upon a Multi-Phase Maximum Likelihood Quantization (MP-MLQ) codebook search, and 5.3 kbps based on Algebraic Code Excited Linear Prediction (ACELP®) platform developed at the Université de Sherbrooke. Both are advancements to Code Excited

Linear Prediction (CELP) algorithms previously introduced. It was optimized to represent speech with high quality at low bit rates using a limited amount of complexity. Music and other audio signals are not represented as faithfully as speech but can be compressed and decompressed using this coder. The higher bit rate has greater quality compared to more flexibility by the lower bit rate algorithm. Both rates are mandatory parts of the encoder and decoder. It is possible to switch between the two rates at any 30-ms frame boundary. G.723.1 can perform full duplex compression and decompression functions for multimedia, visual telephony, and videoconferencing products. G723.1 may not transport DTMF or fax or musical tones reliably, causing issues with services requiring media resources.
G.723.1 uses a frame size of 30 ms (240 samples) and look-a-head of 7.5 ms (60 samples) giving it a total delay of 37.5 ms. As can be expected, G723.1 codec is processing intensive. A VoiceAge implementation indicates 20-25 MIPS (Million Instructions Per Second) and about 3K Random Access Memory (RAM) for the codebooks for its implementation. MOS values for G.723.1 are quoted in a range from 4.1 to 3.8 for the 6.3 Kbps codec and from 4.0 to 3.62 for the 5.3 Kbps codec at zero packet loss. A comparative table for MOS scores is given later in this section.

3.3.8.6 G.729 Voice Codec and Annexes

G.729 is an international ITU-T speech-coding standard [53] that was first adopted in 1995. It was developed through a collaboration of Université de Sherbrooke, France Telecom, and Nippon Telegraph and Telephone Corporation (NTT).

Sampling/Encoding: G 729 is also based on the CELP coding model as the G728 and G723.1. The algorithm used in G.729 is called Conjugate Structure Algebraic CELP (CS-ACELP). It offers high quality speech performance at the expense of complexity. G729 uses 10 ms input frames and generates 80-bit frames. Each 80-bit frame contains linear prediction coefficients, excitation code book indices, and gain parameters that are used by the decoder in order to reproduce speech. The inputs/outputs of this CS-ACELP algorithm are 16 bit linear PCM samples that are converted from/to an 8 kbps compressed data stream. G.729 is mostly used in VoIP applications for its low bandwidth requirement. Standard G.729 operates at 8 kbps but there are extensions, which provide also 6.4 kbps and 11.8 kbps rates for marginally worse and better speech quality respectively.
G.729 uses a frame size of 10 ms and look-a-head of 5ms giving it a total algorithmic delay of 15 ms. G.729 operates at 8 kbps, and still delivers speech quality comparable to 32-kbps ADPCM but at one-quarter the bit rate. As can be expected, G729 codec is complex and processing intensive. A VoiceAge implementation indicates 20-25 MIPS for its implementation with 4K RAM requirement for the codebooks. MOS values for G.729 are quoted from 4.0 to 3.7 at zero packet loss. A comparative table for MOS scores is given later in this section.
G.729a [54] is compatible with G.729, requires less computation, but produces slightly worse speech quality. G.729b [55] incorporates silence compression scheme, a VAD module, and CNG. G.729.1 [56] is another extension of G.729 now in progress. G729.1 will provide support for wideband speech and audio coding covering the frequency range from 50Hz to 7 kHz. The bit rate and associated quality are adjustable by simple bit stream truncation in G729.1.

3.3.8.7 Speex Voice Codec

Speex [57] is a free software speech codec from non-profit Xiph.org (licensor of the Ogg family of formats, the most known being the Ogg Vorbis audio coding format). Speex-coded audio is in Ogg bitstream format and it can be transmitted with Xiph's Ogg container format or over TCP/UDP. The latest version is 1.2 released in Aug-Sept, 2006 and internet drafts were published.

Sampling/Encoding: Speex uses CELP encoding scheme and can encode in a wide range, from 2 Kbps to 44 Kbps bitstream. With the narrowband codec used for VoIP application, typically Speex frames will be between 6 to 70 octets. The total number of Speex frames in the payload should be limited by the path maximum transmission unit (MTU) to prevent fragmentation.
Speex uses 20 ms frames and a variable sampling rate clock. For VoIP the clock rate used generally is 8 kHz. With 20 ms frame and a 10ms look ahead the algorithmic delay is 30 ms. MOS published for Speex through PSQM testing with 8kbps stream is around 3.84 in ideal condition to 3.59 in stressed condition (5% packet loss). A comparative table for MOS scores is given later in this section.

3.3.8.8 ILBC Voice Codec

The internet Low Bit rate Codec (iLBC) is a free but not open-source codec [58] from Global IP Sound. iLBC encoded frames are transported within Realtime Transport Protocol (RTP) packets.

Sampling/Encoding: iLBC algorithm is a version of block independent linear predictive coding (LPC). iLBC uses fixed frame sizes of either 20 ms. or 30 ms. with sampling frequency at 8KHz. The 20ms frames are coded in 304 bits (38 octets) and 30 ms frames are coded in 400 bits (50 octets). These yield bit rates of 15.2 Kbps for 20 ms frames and 13.33 Kbps for 30 ms frames. The iLBC speech codec is robust in the sense that it handles the case of lost frames through graceful speech quality degradation. Standard low bit rate codecs exploit dependencies between speech frames, which result in error propagation when packets are lost or delayed. In contrast, iLBC encoded speech frames are independent and the errors are confined. This gives iLBC robustness against packet loss and delay.
CPU load or the computational complexity and speech quality or MOS value from iLBC is similar to those of G.729a. MOS published for iLBC through PSQM testing is around 3.81 in ideal condition to 3.74 in stressed condition (5% packet loss). A comparative table for MOS scores is given later in this section.

3.3.9 Composite Table Describing Voice Codec Characteristics

Below, a table (Table 3-4) is provided with some of the information given above for comparing the codecs side by side.

3.3.9.1 Bandwidth Requirement Per Call

The table provides the coding algorithm, bit rate, frame size, bundled frame size, and the corresponding frame length as can be derived from the codec information. This information is then incorporated into the header overheads from link layer (Frame Relay, Asynchronous Transfer Mode and Ethernet), and Layer 3 headers to arrive at the bandwidth required per voice call. Note that when multiple values are possible, the value that is most commonly used is indicated by bold lettering.

3.3.9.2 MOS value

Table 3-4 also indicates collected MOS values for the codecs as derived from industry research and is from different sources. The sources include articles from Department of Computer Science at the Columbia University, University of Maryland Advanced Computer Studies, Cisco Systems Inc., and Vocal Technologies Ltd. Note that the values given are under no congestion or no packet loss scenarios. With 5% packet loss or under congestion, the MOS values typically go down by 0.1 to 0.8 depending on the algorithm employed in the codec.

Table 3-4. Bandwidth Requirements Per Call and other Characteristics for Codecs

Codec	Encoding Algorithm	Bit Rate (kbps)	Frames/ Samples (ms)	Bundled Frame Size (ms)	MOS	Frame Length with 40 byte RTP+UDP+ IP Headers (bytes)	Required bandwidth in Kbps (including L2 and L3 headers)		
							L2 Encapsulation protocol		
							PPP or Frame Relay (6 bytes)	ATM	Ethernet (14 bytes)
G.711	**PCM**	64	.125	20	4.1 – 4.5	160+40 = 200	**82.4**	**90.0**	**85.6**
G.726	**ADPCM**	40/**32**/ 24/16	.125	20	3.8 – 4.3	80+40 = 120	**50.4**	**54.0**	**53.6**
G.722	**Sub-band ADPCM**	**64**/56/ 48/32/ 24/16	.125	20	4.3	160+40 = 200	**82.4**	**90.0**	**85.6**
G.723.1	**MP-MLQ ACELP**	**6.3**/5.3	30	30	4.08 – 3.8	20 + 40 = 60	**17.6**	**18.7**	**19.7**
G.728	**LD-CELP**	16	.625	20	4.0	40 + 40 = 80	**34.4**	**36**	**37.6**
G.729	**CS-ACELP**	8	10	20	4.0 – 3.76	20+40 = 60	**26.4**	**28**	**29.6**
iLBC	**LPC**	**15.2** / 13.33	**20**/30	20	4.1 – 3.8	38 + 40 = 78	**33.6**	**35.2**	**36.8**
Speex	**CELP**	**8**/16/ 32/48	2.15 – 44.2	20	3.84 – 3.78	20 + 40 = 60	**26.4**	**28**	**29.6**

3.3.10 Video Codecs

3.3.10.1 H.261 Video Codec

H.261 is the first practical digital video-coding standard [42] published by ITU-T in 1990. The latest published recommendation in-force is as of March 1993. Note that none of the standards (e.g., H.261, H.263, MPEG, and H.264) explicitly define a codec but defines the syntax of the encoded stream and methods of decoding the stream. Still H.261 was a great step forward as the functions (prediction, transform, quantization, entropy encoding) introduced first in H.261 were used and enhanced by all subsequent standards. H.261 was designed to support videoconferencing over ISDN and as such operates with data rates that are multiples of 64 kbps, the basic channel rate for ISDN. It can also send still picture graphics. H.261 transports video streams using RTP. It has been pretty much obsolete due to standards that have been introduced in later years (e.g., H.263) with significant improvements in compression capability for the same quality.

Sampling/Encoding: H.261 coding algorithm uses a hybrid of motion compensated inter-picture prediction, spatial transform coding, zigzag scanning, and entropy coding. This codec was not designed for packet networks and does not work well over FR and TCP/UDP/IP networks. H.261 supports two resolutions – Common Interchange Format (CIF) with 352x288 pixels and Quarter CIF (QCIF) with 176x144 pixels. The data rate for H.261 can be set between 64 kbps and 2 Mbps (Megabits per second).

3.3.10.2 H.263 Video Codec

H.263 is an international ITU-T speech coding standard [43] originally designed by the ITU-T Video Coding Experts Group (VCEG). The first version was published in 1995. The latest published recommendation in-force is as of January 2005. Although the codec was originally designed to support PSTN based videoconferencing and video-telephony, it is used with H.323,

H.320, Real Time Streaming Protocol (RTSP) and SIP. It is used for desktop conferencing, video over Internet, surveillance and monitoring, and teletraining applications. H.263 improved upon H.261, works better with packet networks, supports more data rates and image sizes and as a consequence, pretty much replaced H.261. It was enhanced once in 1998 (H.263v2) and again in 2000 (H.263v3).

Sampling/Encoding: H.263 is variable wide-range data rate codec, although it started its life as a low bit rate codec. The coding is similar to that used by H.261, with improvements for performance such as half pixel precision for motion compensation, and configurations for lower data rate and better error recovery. In addition to the CIF and QCIF resolutions, H.263 added 3 other resolutions Sub-Quarter CIF (SQCIF) with 128x96 pixels, 4-times CIF (4CIF) with 704x576 pixels, and 16-times CIF (16CIF) with 1408x1152 pixels. Generally speaking, H.263 provides video coding with bit rates starting from about 20-30kbps and up and provides the same quality video as in H.261 for half the bit rate.

3.3.10.3 H.264/MPEG-4 Part 10/AVC Video Codec

H.264 is an international standard [44] jointly sponsored by ITU-T Video Coding experts Group (VCEG) and the ISO / International Electrotechnical Commission (ISO/IEC) Moving Picture Experts Group (MPEG). The standard is known by H.264 at ITU-T, or MPEG-4 Part 10 by ISO/IEC [41] or by Advanced Video Coding (AVC). The first version was completed in 2003. After the first version, H.264 added Fidelity Range Extension (FRExt) to enable higher quality coding through extended features. FRExt was added in H.264 second version in March 2005. There is an amendment [45] approved in June 2006 that introduces support of additional color spaces and deprecates the use of a profile (High 4:4:4) that was in previous versions of H.264.

Sampling/Encoding: The objective of H.264 was to build a standard that enables good video quality at substantially lower bit rates than previous standards (e.g., H.263, MPEG-2, MPEG-4 Part 2). Additionally, the standard should provide flexibility to work with different applications requirements and work on a variety of networks. Some of the major features that enable such flexibility in H.264 are: multi-picture inter-picture prediction, improvements with spatial prediction, lossless macroblock coding, new transforms, quantization design, entropy coding, resiliency from loss, and switching slices, to name a few. In other words, the important changes in H.264 are in the details of the functional elements defined for all video codecs - prediction, transform, quantization, and entropy encoding. H.264 defines six profiles, 1) baseline - for low-cost videoconferencing and mobile applications, 2) main - for broadcast and storage applications, 3) extended – uses high compression and robustness for streaming video application, 4) high – higher end broadcast and storage (used in High Definition Digital Versatile Disk or HD-DVD and Blu-ray), 5) high 10 – adding to high profile, and 6) high 4:2:2 – for professional applications for interlacing video. One other profile, high 4:4:4, was deprecated in Amendment 1. With these features and enhancements, H.264 covers a broad range of applications with all forms of compressed rates- from low bit-rate streaming applications to High Definition Television (HDTV) broadcast and Digital Cinema. The transport protocol for H.264 video is RTP.

3.3.11 Bandwidth Requirements For Video Conference Calls

Bandwidth requirement for video calls vary depending upon many factors, including screen resolution, encoding schemes, frame rate, underlying transport network capability, error corrections, amount of motion in the content etc. Therefore it is virtually impossible to predict a specific bandwidth requirement for a video call. The Table 3-5 below provides a guideline for approximate bandwidth requirements with H.264 encoding for various resolutions and frame rates:

Table 3-5. Typical Mid-range Bandwidth Requirement per Videoconferencing Call with H.264 Codecs for Dfferent Resolutions

Resolution	Horizontal pixels	Vertical Pixels	Frame Rate (fps)	Typical Bitrate (kbps)	Typical throughput with P headers (kbps
QCIF	144	176	15	57.0	64
CIF	288	352	15	228.1	256
QVGA	240	320	10	115.2	128
VGA	480	640	30	1382.4	1.5 Mbps

H.264 codecs provide the best picture quality for the same bandwidth or throughput compared to other video codecs. For example, in comparison to the Table 3-5 numbers, the range for typical throughput for H.263 codecs for QCIF resolution is 64-128 kbps and for CIF resolution the range is 192 – 512 kbps.

3.3.12 Voice and Video Codecs

Voice and Video codecs are constantly being improved to make existing applications perform better and also to incorporate new applications. In general, choice of codecs is a trade-off analysis between equipment cost and the user-perceived quality of the session, i.e., MOS for voice and resolution with frame rate for video. The bandwidth requirement is taken as an input to network capacity planning and engineering and as such is considered separately. It should also be noted that most Customer Premises Equipment (CPE) such as IP phones and softphones are built to support multiple codecs so that at the session initiation phase, the choice is negotiated between the two ends.

Therefore the traffic engineering is best performed by considering the default codecs in the user devices. It is recommended that for voice, multiple codecs should be tested for quality at both normal (no packet loss) and stressed (3-10% packet loss) conditions, since MOS values go down at different rates with packet loss depending on the algorithms used in the codecs. G.711 and internet Low Bitrate Codec (iLBC) are two commonly used codecs. Code Excited Linear Prediction (CELP) based codecs should be tested for theaters with bandwidth constraints. For video, H.264 codecs should be tested with different resolutions in support of different services.

This page intentionally left blank.

3.4 Session Initiation Protocol (SIP) Feasibility

3.4.1 Introduction to SIP

This will examine the use of Session Initiation Protocol (SIP) for a number of telephony features within the context of DoD needs and requirements. The primary goal is to define the feasibility of implementing these features using native SIP as the signaling protocol. This paper assumes that the term "native SIP" refers to the SIP protocol standards as defined by the Internet Engineering Task Force (IETF). In this way, we hope to determine whether these features can be implemented when using standard COTS SIP-based devices in a multi-vendor environment without modification. For any given feature that cannot be implemented as described above, a workaround solution is investigated. We strive to suggest workaround solutions that are themselves based on accepted IETF or IEEE protocol standards.

3.4.2 What is SIP?

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants without dependency on the type of session that is being established. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP itself does not participate in the sessions themselves but merely enables and controls them. There are several other protocols that have been developed to do the actual work of carrying the session data.

In recent years the community has chosen SIP as the de-facto signaling protocol for Voice over IP (VoIP) applications. It was designed specifically to be simple and highly extensible. It is this simplicity that makes it the perfect signaling protocol, as it is highly scalable and independent of media and session type. However, the protocol is still evolving today as the technology matures. As it stands today, not many extensions have been standardized. Several proposals have been introduced that would provide additional functionality for telephony applications but as of yet they have not been ratified.

Because only a few extensions have been ratified, SIP on its own can only perform a few basic functions as it relates to telephony. It is for this reason that vendors have had to develop their solutions to this problem while they wait for the protocol to mature. However, this does not prevent the use of SIP today. Most solutions available today use SIP for signaling but rely on other protocols, both proprietary and standard, to complement SIP and thereby achieve the more complex features.

SIP is a request-response protocol that closely resembles two other Internet protocols, HTTP and SMTP (the protocols used for the world wide web and email); consequently, SIP sits comfortably alongside Internet applications. Using SIP, telephony becomes another web application and integrates easily into other Internet services. SIP is a simple toolkit that service providers can use to build converged voice and multimedia services. It is crucial to understand that other protocols must be used alongside SIP in order to provide complete telephony services.

This report provides only a vague description of the protocol's workings. This description is provided only to place the work into context. A complete description of the components, specific extensions, and modes of operation of SIP is beyond the scope of this paper. For more information please see the protocol standard as defined by the Internet Engineering Task Force (IETF) in RFC3261. This RFC obsoletes RFC2543, which was the original SIP specification. RFC3261 defines SIP itself and 6 extensions or methods. The RFC is

extended or amended by RFC3265, RFC3853 and RFC4320. These RFCs define additional extensions including SUBSCRIBE, NOTIFY, MESSAGE, INFO, SERVICE, NEGOTIATE and REFER. There are a number of additional RFCs related to SIP but the basic protocol is described by these four.

3.4.3 Core SIP Specifications

These are the specifications that impact almost every session requested by an agent for which the extension is relevant, such as, SIP session management, SIP registrations and SIP subscriptions
The specifications in this area are:

3.4.3.1 Fundamental SIP Protocol Related

- RFC 3261 – is the basis of SIP protocol.
- RFC 4320 – describes modifications to SIP RFC 3261 [2] to address issues with SIP non-INVITE transactions.
- RFC 3263 – describes DNS procedures for taking a SIP URI and determining the IP address, port, and transport protocol for the SIP server that is associated with that SIP URI and may be in a different IP domain.
- draft-ietf-sip-connected-identity – The identity of the party answering a call, i.e., the connected user can differ from that of the initial called party (given in the 'To' header) in many services requiring forwarding and retargeting. This ID extends the use of the 'From' header field to allow it to convey the identity of the connected user. This is used in conjunction with authentication of the UA identity.

3.4.3.2 SDP Related

- RFC 4566 - Session Description Protocol (SDP), describes the format of multimedia sessions (e.g., VoIP conferences, voice and video streaming) for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. It is independent of transport layer protocols. SDP conveys media details, transport addresses, and other session description metadata to the participants.
- RFC 3264 – defines an Offer/Answer model with the SDP, that is primarily used in unicast sessions with SIP to negotiate session parameters
- RFC 3605 – defines an extension of SDP to explicitly signal the IP address and port # for RTCP within an SDP message, rather than deriving from base media port in RTP. It is specially needed for NAT/NAPT, where mapped port numbers may have no relationship to the order of original port numbers.
- RFC 3388 – defines two SDP attributes, "group" and "mid" that allow grouping of media streams in SDP messages. This enables binding between different media streams from a single flow encoded in different formats (e.g., audio associated with a video feed) on different ports and host interfaces.

3.4.3.3 SIP Requests Related

- RFC 3840 – Indicating User Agent (UA) Capabilities in SIP for example, in INVITE or REGISTER or OPTIONS requests, extend the capabilities in RFC 3261 by providing a general framework to indicate the characteristics and capabilities of SIP UA.

- draft-ietf-sip-outbound-07 – proposes changes to SIP registration mechanism to allow requests to be delivered across NAT bindings between Servers and User Agents (UA)
- draft-ietf-sip-gruu-11 – This SIP extension defines a mechanism (e.g., by SIP REGISTER) for obtaining and communicating an unique globally routable URI that can direct requests to a specific UA. This is usable for features like transfer.
- RFC 3265 – defines a general event notification framework in SIP with SUBSCRIBE and NOTIFY requests.

3.4.3.4 SIP Headers Related

- RFC 3325 – introduces a new header field, "P-asserted-identity", that enable a network of trusted SIP servers in a trust domain to assert the identity of end users/systems and convey privacy indications, as in secure caller-id services
- RFC 4474 – introduces two new SIP header fields: 1) "Identity" to convey signatures in a cryptographic hash s and "Identity-Info" for conveying a reference to the certificate of the signer for securely identifying originator UAs. It is an alternative to the mechanisms in RFC 3325 [59].
- RFC 3327 – introduces the PATH header field, used in conjunction with REGISTER requests and responses to REGISTER, to accumulate and transmit the list of proxies that have to be transited by inbound requests sent to the UA.
- RFC 3581 – introduces a new 'rport" parameter field for the VIA header field that allows a UA to request that the server send the response back to the source IP address and port from where the request originated. It is an essential part of getting SIP through NAT
- RFC 3326 – defines the 'Reason' header field. It provides the reason for initiating the request or to include a final status code in provisional responses.
- RFC 4412 and RFC 4411 – RFC 4412 introduces two new header fields "resource-priority" and "accept-resource-priority" to indicate request for priority treatment during emergencies. RFC 4411 defines an extension to the REASON header to be included in the BYE requests to allow a UA to know that it's session is torn down (preempted) to allow a higher precedence session.

3.4.4 SIP Infrastructure Extensions (General Uses)

These extensions to SIP, SDP and MIME are general purpose extensions introduced for various applications.

3.4.4.1 Fundamental Protocol Related

- draft-ietf-mmusic-ice-13 – defines a method for NAT traversal of media sessions for protocols using offer/answer model, like SIP media streams.
- RFC 3262 – in addition to final responses, SIP defined provisional responses (100-199) for informational purposes only. These are not sent reliably. RFC 3262 defines the Provisional Response ACKnowledgement (PRACK) method and an option tag (100rel) to provide reliable provisional responses.
- RFC 4028 – defines a keep-alive mechanism for SIP sessions by requiring the UAs to send periodic re-INVITE or UPDATE requests. This helps the Stateful Proxies keep the call-state status of all sessions current even in the event of improper terminations.
- RFC 4168 – specifies a mechanism of using SCTP as a transport protocol between SIP entities.

3.4.4.2 SDP Related

- RFC 4145 – defines an extension to SDP for setting up TCP based media sessions between UAs.
- RFC 4091 – defines a mechanism for including alternative types of network addresses (e.g., both IPv4 and IPv6) in SDP for a specific media session.

3.4.4.3 SIP Requests Related

- RFC 2976 – introduces the INFO message to carry mid-call application level signaling information along the session signaling path.
- RFC 3311 – defines a new UPDATE method for SIP to update session parameters (e.g., media stream characteristics) codecs, during "early media" or before the initial INVITE has been answered.

3.4.4.4 SIP Header Related

- RFC 3323 – defines the Privacy Header field for SIP. This RFC defines the roles and messages to be used by UAs and Intermediary Servers when the users choose not to divulge personal identity information.
- RFC 3841 – defines three new request header fields - Accept-Contact, Reject-Contact, and Request-Disposition. The Request-Disposition header allows UAs to express preferences as to how their requests are handled by the servers and the Accept-Contact and Reject-Contact headers allow the UAs to express a preferred feature set for target UAs.
- RFC 4244 – introduces a new header field, "History-Info", to capture the history of requests from a UA that arrive at a particular application server or user.
- RFC 3420 – introduces a new header field "Service-Route", that records a path of proxies and is included by a registrar server in its response to a REGISTER request from a UA. The UA then could use this service-route when requesting service through the specific service proxy.

3.4.5 SIP Limitations

SIP was designed to solve only a small set of problems and to allow interoperability with a broad spectrum of existing and future IP telephony protocols. To this end SIP provides four basic functions:

- User Location: mapping a user's name to their current network address (similar to DNS)
- Feature Negotiation: Allows User Agents (UA) to negotiate a common set of features
- Call participant management: adding, dropping, or transferring participants
- Modifying session features while a call is in progress
- Any other functions must be performed by other protocols.
- Its simplicity means that SIP is not a Session Description Protocol (SDP) nor is it able to perform Conference Control functions. It is also not a Resource Reservation Protocol (RSVP) and it has nothing to do with guaranteeing quality of service (QoS), e.g., IEEE 802.1p, Type of Service (ToS). SIP can work within a framework with other protocols to insure these roles are played out - but SIP does not perform these functions itself. SIP is regularly deployed alongside SOAP, HTTP, XML, VXML, WSDL, UDDI, SDP, RTP and a variety of other protocols.

Because of the simple nature of SIP many of the functions described in this report are not achievable with native SIP alone. Standard methods for deploying these features have not yet been ratified due to the myriad different potential methods to deploy any given feature. Vendors have independently chosen varying methods to solve these issues, which, in turn create a non-interoperable or proprietary situation. Due to this current situation where vendors have not reached agreement and the lack of standards it will be many years, if ever, before multi-vendor solutions with "plug-and-play" advanced features are available to the marketplace. This leads to an environment today where COTS SIP products cannot be guaranteed to interoperate or even have similar feature sets.

3.4.6 Basic Flows

There are a few SIP transactions that must always occur in any SIP interaction. The examples below show state diagrams of SIP flows for User Registration and a basic phone call between two users (UA). The flows discussed below are described in RFC3665 *SIP Basic Call Flow Examples.*

3.4.6.1 SIP Client Registration

Client registration is not absolutely necessary in order to complete a session (see Figure 3-8). If User A knows the network address of User B it can simply call it directly. However, in a network with large groups of users this becomes unfeasible. In these cases a registration server is required. Registration either validates or invalidates a SIP client for user services provided by a SIP server. Additionally, the client provides one or more contact locations to the SIP server with the registration request. Registration is used by a Proxy to route incoming calls in an IP Telephony network. Registration is shown with authentication in these call flows. If authentication is not used, an imposter could *hijack* someone else's calls.

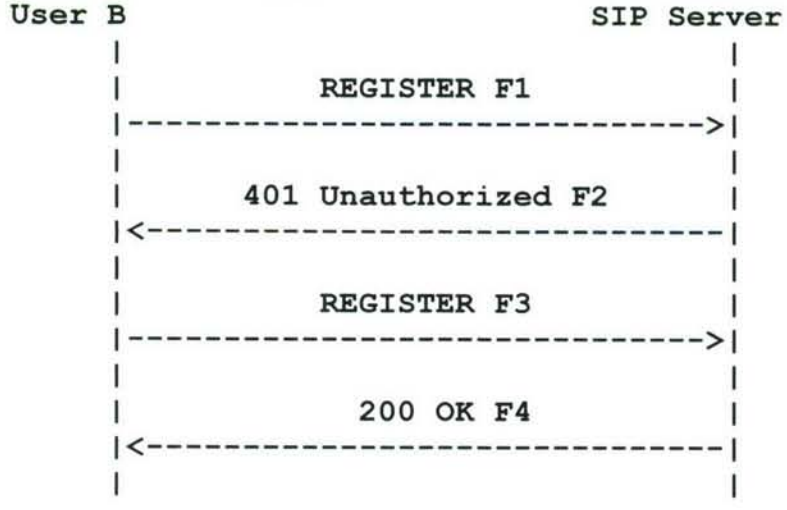


Figure 3-8. SIP Client Registration

User B initiates a new SIP session with the SIP Server, i.e., the user "logs on to" the SIP server. User B sends a SIP REGISTER request to the SIP server. The request includes the user's contact list. Contact list refers to the *Contact* field in the REGISTER header and contains all the caller's potential URL's. The SIP server provides a challenge to User B. User B enters her/his valid user ID and password. User B's SIP client encrypts the user information according to the challenge issued by the SIP server and sends the response to

the SIP server. The SIP server validates the user's credentials. It registers the user in its contact database and returns a response (200 OK) to User B's SIP client. The response includes the user's current contact list in Contact headers. The format of the authentication shown is SIP digest as described by RFC2543. It is assumed that User B has not previously registered with this Server (see Figure 3-9).

Assuming User B's name is Bob, the SIP message details are as follows:

```
F1 REGISTER Bob -> SIP Server

REGISTER sips:ss2.biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS
client.biloxi.example.com:5061;branch=z9hG4bKnashds7
Max-Forwards: 70
From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl
To: Bob <sips:bob@biloxi.example.com>
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 1 REGISTER
Contact: <sips:bob@client.biloxi.example.com>
Content-Length: 0


F2 401 Unauthorized SIP Server -> Bob

SIP/2.0 401 Unauthorized
Via: SIP/2.0/TLS
client.biloxi.example.com:5061;branch=z9hG4bKnashds7
 ;received=192.0.2.201
From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl
To: Bob <sips:bob@biloxi.example.com>;tag=1410948204
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="atlanta.example.com", qop="auth",
 nonce="ea9c8e88df84f1cec4341ae6cbe5a359",
 opaque="", stale=FALSE, algorithm=MD5
Content-Length: 0


F3 REGISTER Bob -> SIP Server

REGISTER sips:ss2.biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS
client.biloxi.example.com:5061;branch=z9hG4bKnashd92
Max-Forwards: 70
From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH
To: Bob <sips:bob@biloxi.example.com>
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 2 REGISTER
Contact: <sips:bob@client.biloxi.example.com>
Authorization: Digest username="bob", realm="atlanta.example.com"
 nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",
 uri="sips:ss2.biloxi.example.com",
 response="dfe56131d1958046689d83306477ecc"
Content-Length: 0
```

```
F4 200 OK SIP Server -> Bob

SIP/2.0 200 OK
Via: SIP/2.0/TLS
client.biloxi.example.com:5061;branch=z9hG4bKnashd92
 ;received=192.0.2.201
From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH
To: Bob <sips:bob@biloxi.example.com>;tag=37GkEhwl6
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 2 REGISTER
Contact: <sips:bob@client.biloxi.example.com>;expires=3600
Content-Length: 0
```

Figure 3-9. Example of Registration

3.4.7 Basic SIP Call

SIP is used to provide signaling for a call between two users. RTP (Real Time Protocol) is then used to carry the voice payload after the call is setup. SIP is then used to tear down (hang-up) the call (see Figure 3-10).

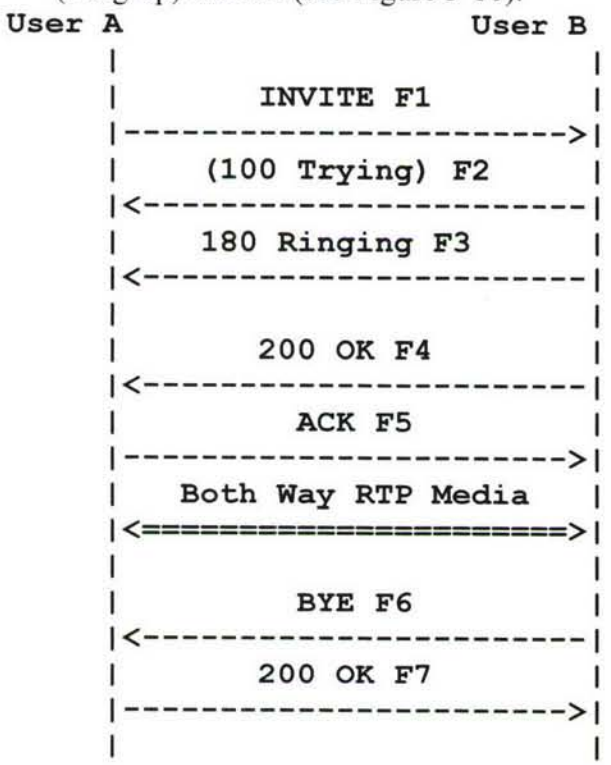


Figure 3-10. Basic SIP Call

In this scenario, User A completes a call to User B directly. User A sends an `INVITE` message to User B. This message indicates to User B that User A would like to set up a dialog. User B sends back a `100 TRYING` to acknowledge the `INVITE` request followed by a `180 RINGING` message to provide a ring-back tone to User A. Once User B decides to accept the call it returns a `200 OK` message to User A, who in turn accepts the call by

responding with an ACK message. The call is now setup and RTP is used to carry the actual conversation or payload. Once the conversation is concluded, User B terminates the call by sending a BYE to User A, who in turn responds with a 200 OK message. Assuming User A's name is Alice and B's name is Bob, the SIP message details are as follows (see Figure 3-11):

```
F1 INVITE Alice -> Bob

INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP
client.atlanta.example.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
 Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 151

v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000


F2 180 Ringing Bob -> Alice

SIP/2.0 180 Ringing
Via: SIP/2.0/TCP
client.atlanta.example.com:5060;branch=z9hG4bK74bf9
 ;received=192.0.2.101
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:bob@client.biloxi.example.com;transport=tcp>
Content-Length: 0


F3 200 OK Bob -> Alice

SIP/2.0 200 OK
Via: SIP/2.0/TCP
client.atlanta.example.com:5060;branch=z9hG4bK74bf9
 ;received=192.0.2.101
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>;tag=8321234356
```

```
    Call-ID: 3848276298220188511@atlanta.example.com
    CSeq: 1 INVITE
    Contact: <sip:bob@client.biloxi.example.com;transport=tcp>
    Content-Type: application/sdp
    Content-Length: 147

    v=0
    o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com
    s=-
    c=IN IP4 192.0.2.201
    t=0 0
    m=audio 3456 RTP/AVP 0
    a=rtpmap:0 PCMU/8000
    F4 ACK Alice -> Bob

    ACK sip:bob@client.biloxi.example.com SIP/2.0
    Via: SIP/2.0/TCP
client.atlanta.example.com:5060;branch=z9hG4bK74bd5
    Max-Forwards: 70
    From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
    To: Bob <sip:bob@biloxi.example.com>;tag=8321234356
    Call-ID: 3848276298220188511@atlanta.example.com
    CSeq: 1 ACK
    Content-Length: 0

    /* RTP streams are established between Alice and Bob */

    /* Bob Hangs Up with Alice. Note that the CSeq is NOT 2, since
       Alice and Bob maintain their own independent CSeq counts.
       (The INVITE was request 1 generated by Alice, and the BYE is
       request 1 generated by Bob) */


    F5 BYE Bob -> Alice

    BYE sip:alice@client.atlanta.example.com SIP/2.0
    Via: SIP/2.0/TCP
client.biloxi.example.com:5060;branch=z9hG4bKnashds7
    Max-Forwards: 70
    From: Bob <sip:bob@biloxi.example.com>;tag=8321234356
    To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
    Call-ID: 3848276298220188511@atlanta.example.com
    CSeq: 1 BYE
    Content-Length: 0


    F6 200 OK Alice -> Bob

    SIP/2.0 200 OK
```

```
    Via: SIP/2.0/TCP
client.biloxi.example.com:5060;branch=z9hG4bKnashds7
    ;received=192.0.2.201
    From: Bob <sip:bob@biloxi.example.com>;tag=8321234356
    To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
    Call-ID: 3848276298220188511@atlanta.example.com
    CSeq: 1 BYE
    Content-Length: 0
```

Figure 3-11. SIP Message Details

3.4.8 Implementation of Selected Features

Below we examine a set of selected features and the feasibility of implementing them using native SIP. Where the feature is achievable in native SIP, state flow diagrams and explanations are provided. Where they cannot be implemented in native SIP, an explanation is provided along with potential workarounds and/or problems that may arise if implemented in SIP.

3.4.8.1 Conference Call

A conference call is the creation of a group of end devices coupled together so all participants can hold a conversation. It requires action of the end user to pick up their end device or call into a conference number.

SIP was defined to allow for the establishment, maintenance, and termination of calls between one or more users. However, despite its origins as a large-scale multiparty conferencing protocol, SIP is used today primarily for point-to-point calls. This configuration is the focus of the SIP specification and most of its extensions. As a result, there is a lot of confusion about how SIP supports multi-party conferencing.

There are a number of conferencing models supported by native SIP. These models range from Three-Party Calling with end system mixing to large multicast conferences, to dial-in or dial-out conferences servers, to ad-hoc centralized conferences, to conferences using centralized signaling and distributed media. Most conference calls involving more than a dozen or so participants have the need for more advanced features such as the ability of the moderator to mute all phones, set the length of time for the conference call, record and display the participants of the conference call, etc. However, there is no ratified standard for any of these models as of yet. A draft exists by Rosenberg, titled *draft-rosenberg-sip-conferencing-models-00* which describes all of these models in detail.

Standard native SIP cannot provide conferencing capabilities without the help of some form of SIP Proxy or IP-PBX for mixing the voice signals. The simplest example of conferencing is accomplished by first initiating a basic call between two users (A and B) as described in the previous section above. Once the call is in progress, B initiates a second, separate call to User C. Once the second call is in progress, B will then mix the streams and send B+C to A, and send A+B to C. In this example, User B is acting as the mixer/IP-PBX. This method of conference calling is how many IM (Instant Messaging) clients function. The number of participants is usually limited to a few participants. A separate server or PBX could just as easily perform the *mixer* function without affecting the SIP flow in any significant manner.

Changes Needed to SIP Protocol

No changes or modifications of SIP are required to implement this feature, however, a User Agent Server (UAS) or mixer is required.

State Diagrams

The example below (see Figure 3-12) describes the simplest form of conference calling with SIP. All other models are variations of the same.

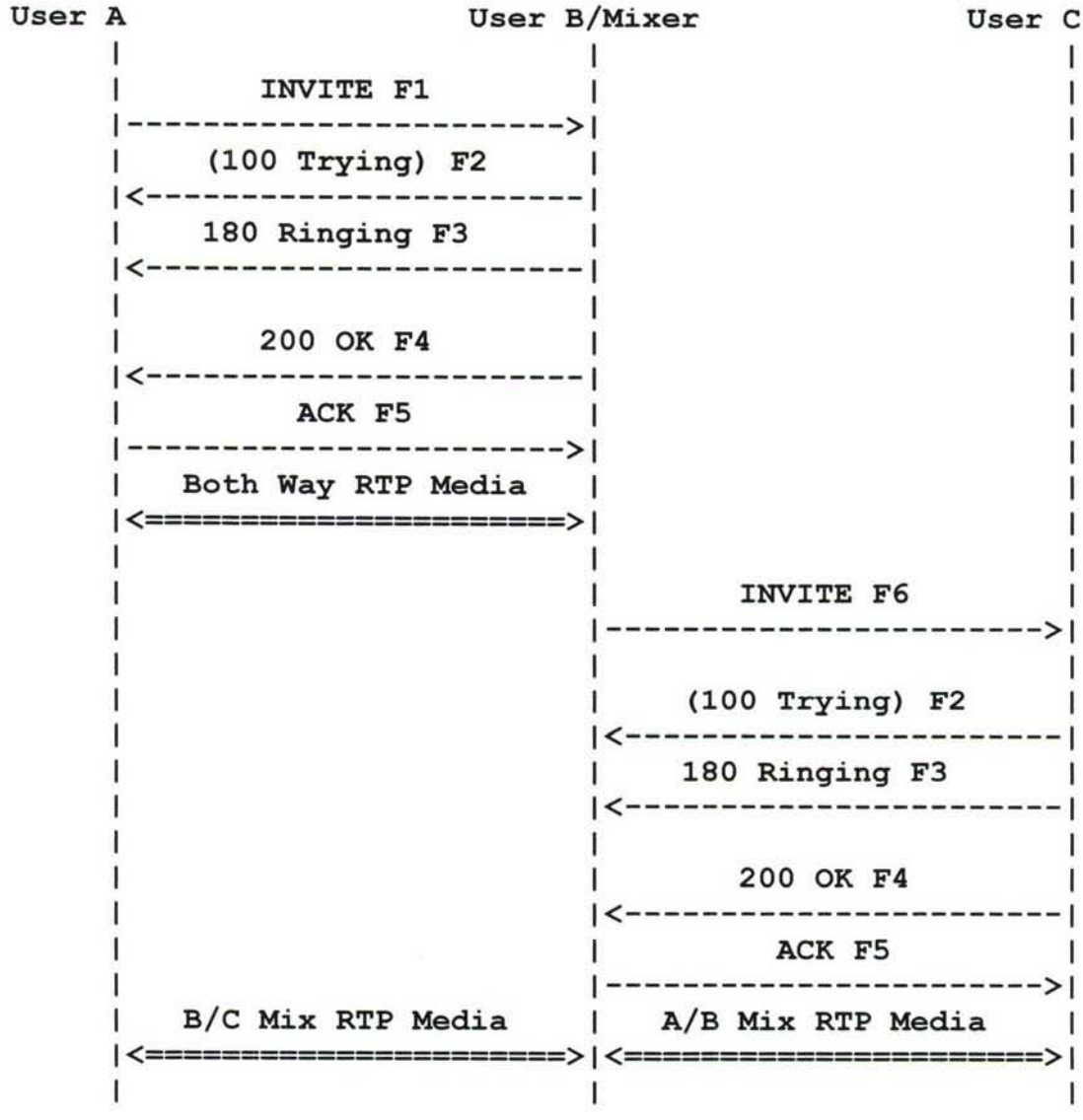


Figure 3-12. Simple Conference Call With SIP

See previous example for descriptions of SIP message details.

This next example (see Figure 3-13) assumes that users A, B and C are already in conference using a proxy. The example describes how User D would be added to the conference. Only one addition is shown for the sake of simplicity. It should be remembered that any other additions would follow the same flow.

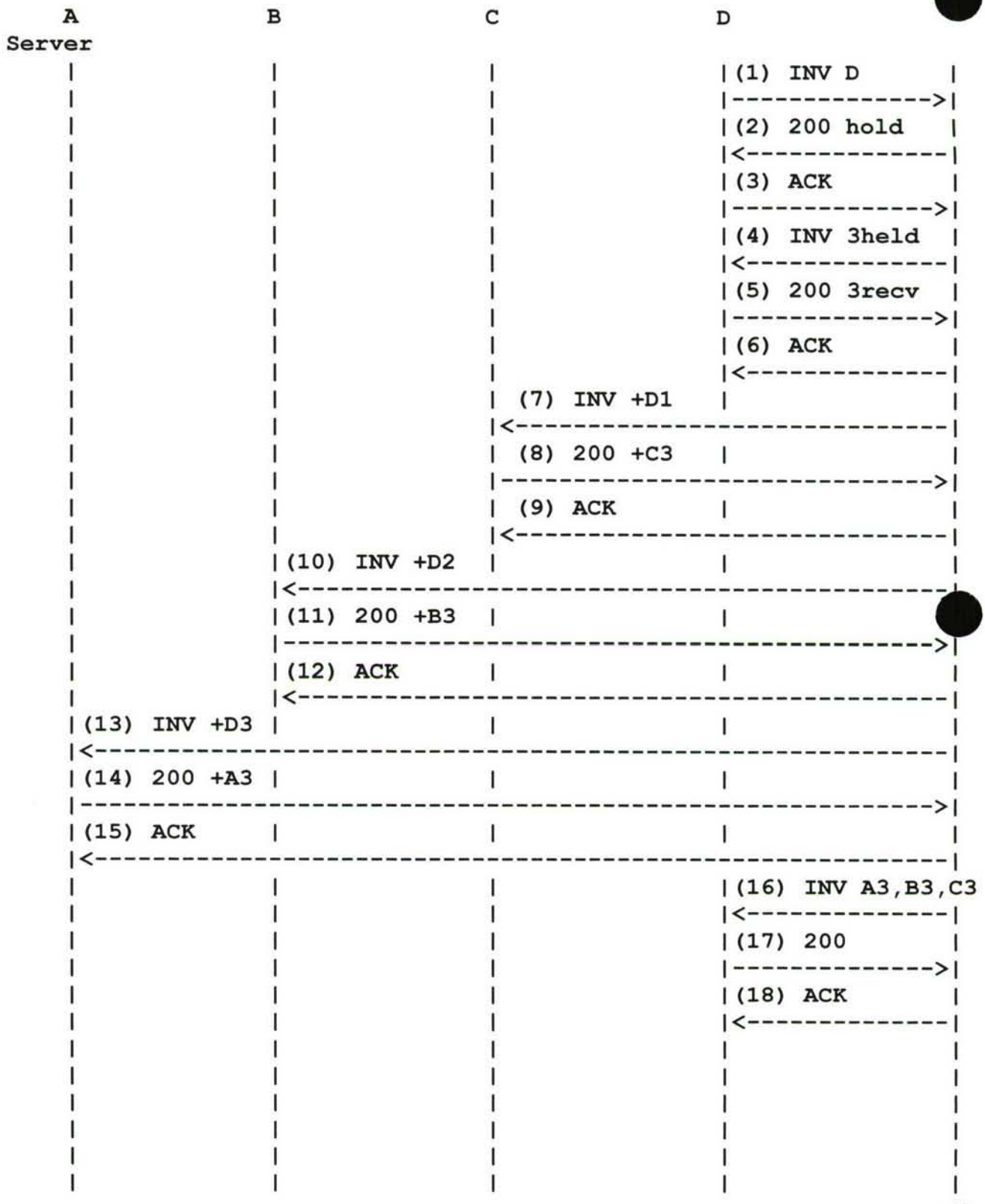


Figure 3- 13. Example Conference Using a Proxy.

As described in draft-rosenberg-sip-conferencing-models-00, users joining is easily done. The participant that wishes to join simply sends an INVITE to the conference server, with the conference ID in the request URI (1). The conference ID (which is a SIP URL) can be learned by any number of means, including having it on a web page, receiving it in an email, etc.

For example, if D wishes to join sip:conference34@servers.com, D would send the following request:

```
INVITE sip:conference34@servers.com
From: sip:D@example.com
To: sip:conference34@servers.com
```

3.4.8.2 Intercom

This feature involves the creation of a group of end devices coupled together so all participants can hold a conversation. It doesn't require the end user to pick up their end device or hang it up. The end device goes off-hook automatically and then returns to on-hook after the intercom is completed.

The Session Initiation Protocol does not currently provide a mechanism to force the UA (User Agent) to go *off-hook*. A UA could be configured to *auto-answer* incoming calls. However, this method has some security implications. In particular, there may be problems with potentially having an open-microphone when auto-answering a call. Other parties within the vicinity of the end device may over hear conversations they are not meant to. It could be an appropriate method for one-way announcements in some circumstances.

It is possible, and some manufacturers have implemented this method, to add a field to the standard INVITE header that would cause the receiving UA to go off-hook automatically with or without mute. In essence, the called device must understand this field or flag and it must be programmed to act on it. A device that does not support this field will simply ignore the flag and continue with normal operations. A number of manufacturers have successfully implemented this feature. Some with the method described here but most have done it with proprietary methods such as using proprietary protocols running over SIP. It goes without saying that until this method is ratified in an IETF RFC, there is no way to guarantee that any given SIP UA will support this feature. There is an Internet draft called "draft-ietf-sip-answermode-00" but it expired in June of 2006 with no action taken.

The creation of a group of end devices so all participants can hold a conversation is in essence a form of Conference Call. There are multiple methods of Conference Calling but two major types: dial-in and invite-based. A dial-in conference is one in which users must explicitly request to join the group. In an invite-based Conference, however, a user is invited (using the INVITE message) to join the group. The specific requirement here would be a basic invite-based conference and can be implemented as described above in the Conference Call section.

Changes Needed to SIP Protocol

Methods to extend SIP have been implemented by some manufacturers but an Internet draft must be proposed, discussed and ratified in order to provide this function in a standard manner and guarantee availability in any given SIP device.

State Diagrams

The state diagram would be identical to a basic call. A minor variation in the SIP message detail would be the only change. No State diagram provided.

3.4.8.3 Group Page

The creation of a group of end devices coupled together so a one-way announcement can be done. The end device goes off-hook automatically and then returns to on-hook after the announcement is completed

This feature has similar issues to the Intercom feature described above in that it involves calling a group of users simultaneously. Like the Intercom feature above, it would also be an invite-based conference call. The basic difference between these features is that the Intercom feature calls for a two-way conversation and Group Page calls for a one-way conversation but the mechanics are identical.

Changes Needed to SIP Protocol

An auto-mute function must be added to SIP.

State Diagrams

This feature has a state diagram flow identical to a conference call where a user is invited in rather than calling-in. See state diagram for Conference feature above. No state diagram provided.

3.4.8.4 Priority Calls

The ability for an individual to break into a call that is in progress by use of a feature code and supervisor login. (Busy Verify in Avaya's PBX)

SIP, as a signaling protocol, does not have the ability to break into ongoing calls. The problem is similar to the auto-answer issue described above.

Changes Needed to SIP Protocol

Extensions to SIP would need to be drafted and ratified in order to provide this function. The SIP protocol would need to have the ability to signal the UA and have the UA duplicate the incoming and outgoing voice streams and mirror them to UA , SIP Proxy, IP-PBX.

State Diagrams

Not possible within the framework of SIP. No State diagram provided

3.4.8.5 NCS Voice Precedence System

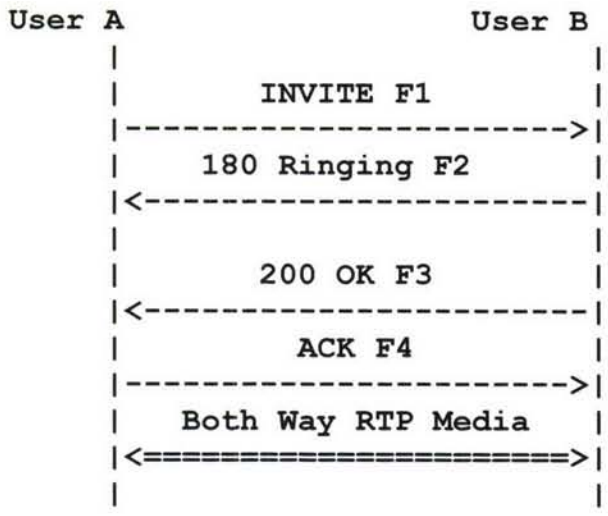
Also known as Multi-Level Precedence and Preemption or MLPP gives individuals the ability to override a call that is in progress between two or more other parties. This feature is presently not being used onboard U.S. Navy vessels. Instead, Priority Calling is being used.

Priority Calling differs from MLPP in that it is a method of inserting a third-party into an ongoing call without notification to the original parties. Also known as Busy Verify (Avaya) or Barge-In (Alcatel) and was traditionally used to check the status of line by an operator or similar person. MLPP on the other hand, is a priority-based call override system. This system may affect all SIP elements in a network. However, this paper will only discuss it within the context of the end-user point of view.

MLPP notifies the called party with a tone prior to overriding the existing call. For example:

- Users A and B are having a conversation
- User C must communicate with A
- User C calls A using a priority level higher than the ongoing call between A and B
- Both A and B are presented with a tone warning them of an incoming higher priority call
- The call between A and B is dropped
- A new session between A and C is immediately started

This feature is a SIP standard and is defined in RFC4412. The RFC adds two new fields to standard SIP messages. These fields can potentially appear in all types of SIP messages. It is mandatory only for handful of messages including INVITE, REFER, UPDATE, PRACK and ACK but optional in others.
No changes needed to SIP. At a minimum, support of RFC4412 is required by the UA's. Preferably, all SIP elements should support this RFC.
The state flow for this feature looks identical to a basic call with the addition of the *Resource-Priority* field in the INVITE message (see Figure 3-14).



The relevant message headers are:

F1 INVITE User A -> User B

```
INVITE sip:UserB@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP
client.atlanta.example.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: BigGuy <sip:UserA@atlanta.example.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Resource-Priority: dsn.flash
Contact: <sip:UserA@client.atlanta.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: ...

...
```

F2 180 Ringing User B -> User A

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP
client.atlanta.example.com:5060;branch=z9hG4bK74bf9
  ;received=192.0.2.101
From: BigGuy <sip:UserA@atlanta.example.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.example.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:UserB@client.biloxi.example.com;transport=tcp>
Content-Length: 0
```

F3 200 OK User B -> User A

```
    SIP/2.0 200 OK
    Via: SIP/2.0/TCP
client.atlanta.example.com:5060;branch=z9hG4bK74bf9
    ;received=192.0.2.101
    From: BigGuy <sip:UserA@atlanta.example.com>;tag=9fxced76sl
    To: LittleGuy <sip:UserB@biloxi.example.com>;tag=8321234356
    Call-ID: 3848276298220188511@atlanta.example.com
    CSeq: 1 INVITE
    Contact: <sip:UserB@client.biloxi.example.com;transport=tcp>
    Content-Type: application/sdp
    Content-Length: ...

    ...
```

Figure 3-14. Invite Message

3.4.8.6 Call Park

The ability to park a call onto a virtual extension and then have a third-party or the same individual, retrieve the call. To the caller, the call appears to be on hold and is presented with "music on hold".

This feature, like many others, can be implemented with SIP in several ways. It is defined RFC 4240 and in the *draft-procter-sipping-call-park-extension-00* draft document. Several different methods are also described in books and SIP-related sites on the Internet. For this reason, this paper will describe the most basic and simple version of these methods. The method described below appears in *draft-procter-sipping-call-park-extension-00* and a similar method is described in *draft-ietf-sipping-service-examples-06*.

The only requirement is a "Park Server". Other methods may require modifications and/or additional servers.

This method adds an *orbit* tag to the REFER message. This tag is user defined provides a basic extension that can be used later to retrieve the call. It provides a way to avoid two callers being parked simultaneously in the same place (see Figure 3-15).

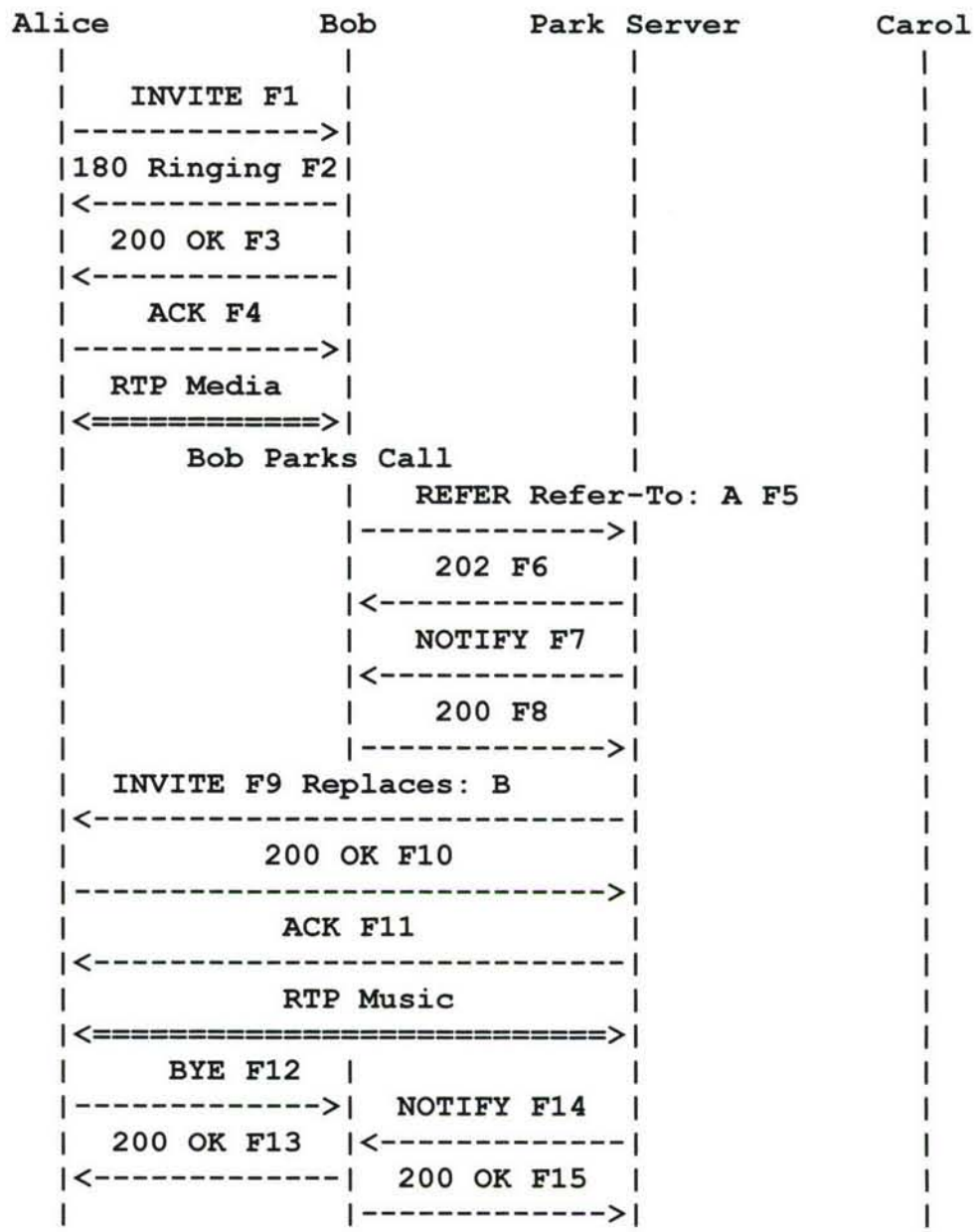


Figure 3-15. Call Park

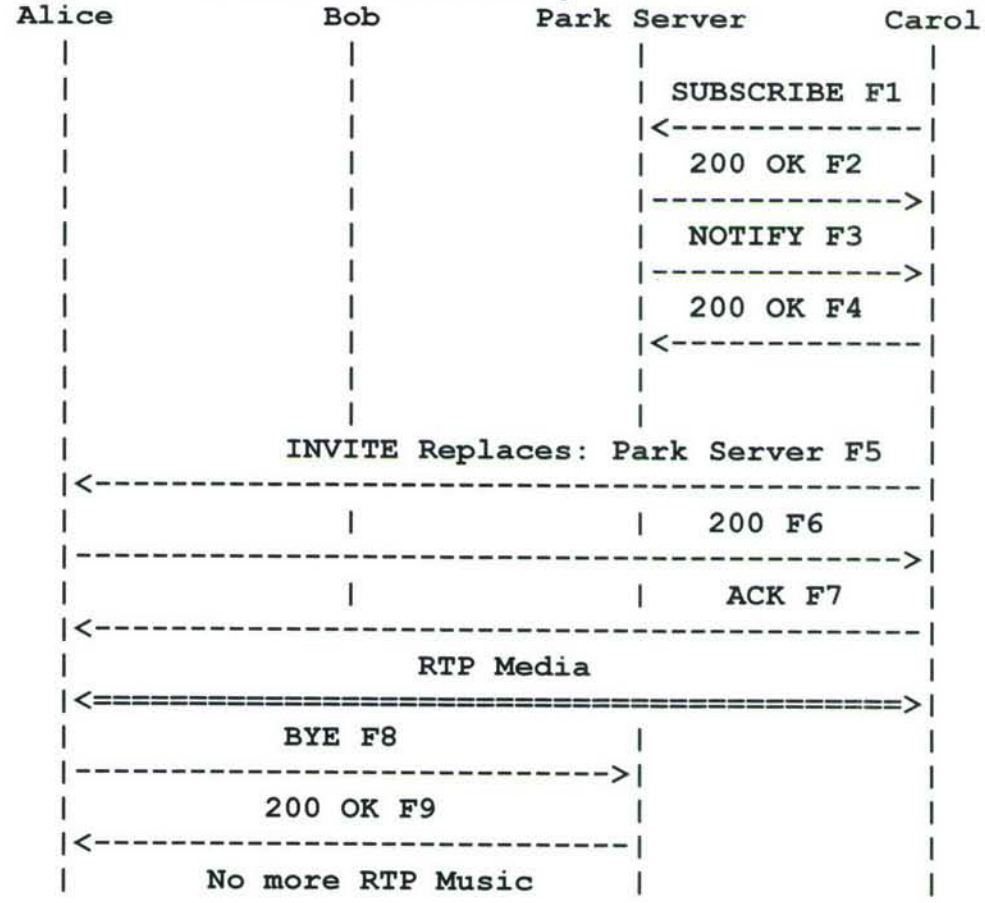
The URI <sips:park@server.example.com;orbit=1234> is used instead of directing the request to the URI <sips:park@server.example.com>. The addition of the orbit parameter effectively tags the parked call with a short memorable code entered by the user see Figure 3-16 and Figure 3-17).

```
F5 REFER Bob -> Park Server

REFER sips:park@server.example.com;orbit=1234 SIP/2.0
Via: SIP/2.0/TLS
client.biloxi.example.com:5061;branch=z9hG4bKnashds9
Max-Forwards: 70
From: Bob <sips:bob@biloxi.example.com>;tag=02134
To: Park Server <sips:park@server.example.com;orbit=1234>
Call-ID: 4802029847@biloxi.example.com
CSeq: 1 REFER
Refer-To: <sips:alice@client.atlanta.example.com?Replaces=
12345601%40atlanta.example.com%3Bfrom-tag%3D314159%3Bto-
tag%3D1234567>
Referred-By: <sips:bob@biloxi.example.com>
Contact: <sips:bob@client.biloxi.example.com>
Content-Length: 0
```

Figure 3-16. Park Server 1

Alice is now *parked* at the Park Server. In order to retrieve the call, Carol calls the Park Server. The Server notifies Carol of the URI required to retrieve the call in the NOTIFY message. Remember that the URI contains the *orbit* tag.



```
F1 SUBSCRIBE  Carol -> Park Server

SUBSCRIBE sips:park@server.example.com;orbit=1234 SIP/2.0
Via: SIP/2.0/TLS chicago.example.com:5061;branch=z9hG4bK92bz
Max-Forwards: 70
From: Carol <sips:carol@chicago.example.com>;tag=8672349
To: <sips:park@server.example.com;orbit=1234>
Call-ID: xt4653gs2ham@chicago.example.com
CSeq: 1 SUBSCRIBE
Contact: <sips:carol@client.chicago.example.com>
Event: dialog
Subscription-State: active;expires=0
Accept: application/dialog-info+xml
Content-Length: 0


F2 200 OK  Park Server -> Carol

SIP/2.0 200 OK
Via: SIP/2.0/TLS chicago.example.com:5061;branch=z9hG4bK92bz
 ;received=192.0.2.114
Max-Forwards: 70
From: Carol <sips:carol@chicago.example.com>;tag=8672349
To: <sips:park@server.example.com;orbit=1234>;tag=1234567
Call-ID: xt4653gs2ham@chicago.example.com
CSeq: 1 SUBSCRIBE
Content-Length: 0


F3 NOTIFY  Park Server -> Carol

NOTIFY sips:carol@client.chicago.example.com SIP/2.0
Via: SIP/2.0/TLS chicago.example.com:5061;branch=z9hG4bK93ca
Max-Forwards: 70
To: Carol <sips:carol@chicago.example.com>;tag=8672349
From: <sips:park@server.example.com;orbit=1234>;tag=1234567
Call-ID: xt4653gs2ham@chicago.example.com
CSeq: 2 NOTIFY
Contact: <sips:park@server.example.com;orbit=1234>
Event: dialog
Subscription-State: terminated
Content-Type: application/dialog-info+xml
Content-Length: ...

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info"
   version="0" state="full"
   entity="sips:park@park.server.example.com;orbit=1234">
<dialog id="94992014524" call-
id="12345600@atlanta.example.com"
```

```
          local-tag="3145678" remote-tag="1234567"
direction="recipient"
          remote-uri="alice@atlanta.example.com"
          remote-target="alice@client.atlanta.example.com">
        <state>confirmed</state>
        </dialog>
        </dialog-info>


        F4 200 OK  Carol -> Park Server

        SIP/2.0 200 OK
        Via: SIP/2.0/TLS chicago.example.com:5061;branch=z9hG4bK93ca
        To: Carol <sips:carol@chicago.example.com>;tag=8672349
        From: <sips:park@server.example.com;orbit=1234>;tag=1234567
        Call-ID: xt4653gs2ham@chicago.example.com
        CSeq: 2 NOTIFY
        Contact: <sips:carol@client.chicago.example.com>
        Content-Length: 0
```

Figure 3-17. Park Server 2

3.4.8.7 Directed Call Pick-up

This feature provides the ability to pick-up a call that is ringing on another end device. Call Pickup is described in the IETF draft called *draft-worley-sipping-pickup-02*. This document states:

"There are several different schemes for implementing call pickup. The basic method is the one specified in the Sylantro "SIP-B" specification, which despite its proprietary air, uses standard SIP features in an end-point call control (EPCC) style. All other methods are variations on the same theme, usually by using an agent process (in a proxy or communications server) to provide a feature that the user agents are lacking.

Like call transfer, effecting call pickup requires some support from the caller's end. These caller-end features will, therefore, soon come to be considered necessary for any "quality" SIP implementation."

As there are so many variations and possible implementation methods (none of them standard) for this feature, this paper will focus on the simplest of them and refer the reader to *draft-worley-sipping-pickup-02*, *draft-ietf-sipping-service-examples*, and *draft-procter-sipping-call-park-extension* for more in-depth discussion of the more complex methods.

The basic method involves calling the ringing extension and polling it for status of it's current calls. The ringing extension responds with, among other things, the caller URI. The calling UA can then be sent an INVITE thereby "picking-up" the call.

The basic SIP-B pickup sequences are as follows. (Only principal messages are shown.) Suppose the incoming call is to the callee phone, extension 123, and the phone executing the pickup is extension 456 (see Figure 3-18):

```
Caller                    Callee                    Executing
```

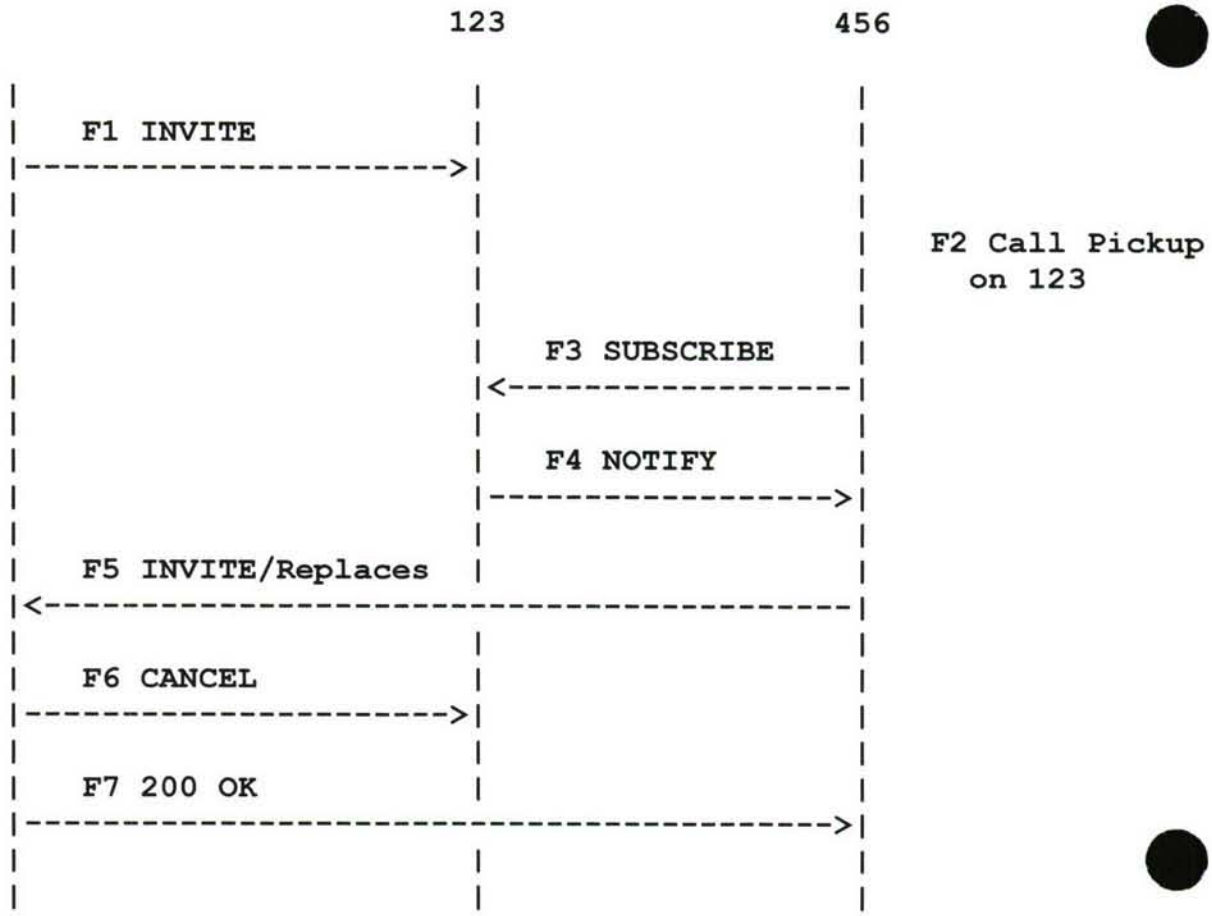


Figure 3-18. Directed Call Pick-up

F1 - The caller (AOR Caller@example.com) sends an INVITE with URI 123@example.com to phone 123.
F2 - The user of phone 456 activates the call pickup feature for extension 123.
F3 - Phone 456 sends a SUBSCRIBE with URI 123@example.com to phone 123, requesting "Event: dialog" and "Expires: 0".
F4 - Phone 123 sends one NOTIFY to phone 456 giving the status of its current dialogs for AOR 123@example.com, which includes the early dialog of INVITE 1 from Caller, and gives the "remote identity" and "remote target" of the dialog (which are the From: and Contact: of INVITE 1), one of which is "Caller@example.com".
F5 - Phone 456 sends INVITE 5 to Caller@example.com. It has a Replaces: header specifying the dialog parameters sent in the NOTIFY. The Replaces: header contains the "early-only" option, so that the pickup operation fails if extension 123 answers the call.
As a consequence of executing the INVITE/Replaces, the caller sends a CANCEL of its INVITE 1 to phone 123.
The caller sends a 200 response to the INVITE 5 from phone 456.
At this point, Caller is talking to phone 456.

3.4.8.8 Group Call Pick-up

The SIP flows for this function are identical to the flows required for Directed Call-Pickup (above). The exception being that the called extension is a conference URI. In other words, the group of end-devices must be in a conference. You may then poll the conference URI to obtain the ringing party's URI.

3.4.8.9 Recording of Calls

This feature would provide the ability to record calls from a set of pre-defined end devices as soon as they are off hook. This would be used for all calls that the bridge handles. There are a number of ways in which this feature might be implemented. The community has discussed this subject extensively since the year 2000. Several ideas have been bandied about but no drafts or standards have come of it. The potential implementations would all require the creation of a Conference Call and the automatic addition (or INVITE) of a *recorder*. The *recorder* would simply act as a standard UA and store the mixed streams it receives.

This can be achieved in a number of different ways but this paper will only describe the simplest of these methods, as no standard yet exists. Let's assume that the bridge UA is A, the *recorder* is B and the called/calling party is C. The simplest method would be to program the user's UA (A) to automatically INVITE the *recorder* (B) and conference it in along with C every time it goes off-hook.

The *recorder* device (B) could be implemented in any number of ways as well. It could implemented in:

- The UA itself: allowing the placement of recorders anywhere they are needed.
- A "Black Box": this could be placed throughout the ship and be able to service multiple UA's simultaneously and providing redundancy in case of failure.
- A PBX: in this manner, the PBX could be programmed with all the extensions requiring this service.

Changes Needed to SIP Protocol

No changes to SIP need be implemented. However, a standard should be proposed and ratified that defines the methodology for achieving this functionality. Until a standard is available there is no guarantee any two vendors will implement this feature in the same way.

State Diagrams

SIP state flows for this feature would be identical to that used in Conference Calling. See Conference Call section above for diagrams.

Summary

After much research, the salient point to be made is simple: all of the above features could be implemented with SIP. However, for any given feature there are myriad ways to achieve it. This is, coupled with SIP's simplicity, we believe, the reason for the current state of confusion with regards to SIP standardization. Some of these features can be implemented today with the standards that already exist. Others could be achieved in a proprietary manner, yet using SIP, through some creative thinking and development of private extensions to the protocol. This, however, creates a situation where only devices explicitly created to support said features would actually work.

In addition, we can envision that eventually the SIP protocol standard will be completed in such a manner as to provide standard methods of implementation for these and other telephony features. The real question is: when?

3.5 SIP Servers

SIP, unlike H.323, does not require any server and can be utilized phone-to-phone, if the caller know the other person's IP address and is able to reach it from their network location. In a real world installation, SIP is installed with at least one server that may contain one or more different functional servers. In this section functional servers will be reviewed with their functional requirements and as to how they are used. First, we will review common names of the parts that would be included in a SIP network. Each individual component in a SIP system is called a Node, which would include a SIP-based phone, as well as the registrar and proxy servers.

SIP defines three logical entities that are the building parts for all the SIP servers, User Agent (UA), the User Agent Client (UAC) and the User Agent Server (UAS).
The User Agent is either a client or server device that maintains state for the session and dialog. It initiates or responds to transactions during the sessions or dialog. This is the lowest level that the next two logical entities are subsets of.
The User Agent Client (UAC) is a logical SIP device that initiates or responds to transactions. It could be a SIP phone on behalf of a human or a proxy forwarding a request on.
The UAC opposite is an User Agent Server (UAS), which is a logical SIP device that accepts and sends back responses. An example of this is a SIP phone accepting an INVITE and responding with an ACK. Many devices have both UAC and UAS in the same device.

The RFC 3261 specification defines three servers, the Proxy Server, the Redirect Server and the Registrar Server. The Proxy functions as an intermediate step in a SIP transaction. It can provide several different functions such as authentication, enforcement of policy, and primary routing. A Proxy can be stateless or stateful of the session depending on the INVITE's parameters. The Redirect Server is a UAS device that redirects the UAC request to other URI in order to contact an individual at a different location. It does this with the response of 3XX class responses to requests. It uses the information that the Registrar Server puts into its databases. The Registrar Server is a UAS that accepts REGISTER requests from a UAC, and stores the information into a database for other UAS to use, as required. The UAC will send updates to the Registrar Server at set intervals so the record is kept up to date. If a record expires, it is deleted. RFC 3261 and its related drafts also define some supporting servers. The server that is used for IP-PBX is Back-to-back User Agent (B2BUA). B2BUA is a UAS device that receives requests and then generates a request from a UAC. It has to stay inside the transaction and maintain dialog-state for all transactions in the dialog. Examples of B2BUAs are IP-PBXs and IP-Mixers. A Presence Server provides information about a SIP device on a network. In SIP Specific Event Notification (RFC 3265) is defined a Events Server, that acts as a "notified" of events like registrations and message waiting indicators.

In the RFC 3261, the authors never state how these servers are to be created. There were separated in the specification and drafts, but only for the reason of clarity to the reader. It was never meant as a guideline for how they were to be implements in a production system. These servers can be combined in any method that makes sense for the applications that is being created. In many cases they are combined. You can find More information about the operations of the SIP Servers is provided in RFC 3665 "SIP Call Flow Examples" document draft-ietf-sipping-call-flows-01.txt.

3.5.1 Proxy Server

The definition of Proxy Server is "elements that route SIP requests to User Agents Servers (UAS) and SIP responses to User Agents Clients (UAC). A request may transverse several proxies on its

way to a UAS. Each will make routing decisions, modifying the request before forwarding it to the next element. Responses will route through the same set of proxies traversed by the request in the reverse order." Even though the proxy server forwards the SIP requests, it has the ability from the specification to do much more, such as validate requests, authenticate users, fork requests, resolve address, cancel pending calls, record-route and loose-route and deal with looping issues. Proxies deploy complicated routing logic that is more complicated then just forwarding the requests to the next element.

There are two types of proxies define in the specifications: Stateless and Stateful. The easiest one is the stateless one; it saves no transaction context. Because of this it scales and has better performance than a Stateful proxy. With the benefits, there are consequences to using a stateless proxy. It can't associate responses with requests that it has forwarded, since it retains no knowledge of the past requests. It is not able to retransmit requests and respond, because every time it gets a message it is for the first time. The high performance of the stateless proxy lends it to be used for high-throughput capability in the core of carriers and service providers. They are also used for load balancing in networks that have high utilization requirements. The only exception to this is if the proxy returns a non-2xx response. Then it is required to retain a transaction state that is Stateful. The Stateful proxy server does not have the limitations of the stateless proxy, but with this comes several drawbacks. The proxy must retain memory for each processed message for a long duration of time, resulting in heavy memory usages. There are code optimizations specific to SIP that reduces the memory usage required for high-capacity installations. Throughput is reduced since the CPU has to process each message, mapping messages to transactions. Then it needs to manage the transactions, in a state machine as well as processing transaction timers associated with client and server transactions. The Stateful proxy does a lot more then just forward the request. Logic needs to be added to handle forking (parallel or sequential), CANCEL, recursion of 3xx responses, and handling 2xx responses. Many special cases that are hard-to-deal with have been added by the different specifications and drafts. The SIP stack that is required for a Stateful proxy needs to be more flexibility that is not required in a UA. It has to be able to deal with transport and transaction layers as well as expose application-programming interface (API) that allows for conformance with the requirements.

Proxy and Redirect servers need to validate the requests as they pass into the server. The first validation is for reasonable syntax. This validation examines if the request is well formed for the fields that the server needs to process and that the other fields are not evaluated. The url scheme are checked to make sure that they are understood and supported by the server.
The max-forward field is checked to make sure that the request has not had too many hops before reaching this server. An optional way of dealing with the max-forward is the loop detection that uses an algorithm on the via list contained in the message. If it has processed the request before it validated the fields that influence the routing of the request, it makes sure they have changed and are not looping. It also has to validate the field that contains the extension for the proxy to make sure that it can successfully handle the request. The final validation is to determine if the request requires authentication from the originator of the message. If it does, it will return a 407 response that contains the challenge.

A specialized type of proxy is the outbound proxy. This type of proxy receives requests from all the clients regardless of the destination. This way the client software doesn't have to complicated by the process of doing address lookups. The server will accept all requests even if they are not leaving the domain.

The Proxy Core Object (ProxyCoreObj) has the responsibility of managing the overall state of the request. The ProxyCoreObj chooses the destination address (es) and instantiates one or more client transaction objects (see Figure 3-19). It also collects the transaction responses and determines the best response to send upstream. This is when an UAC has multi-registered locations that needs to be pooled in order to contact the UAC.

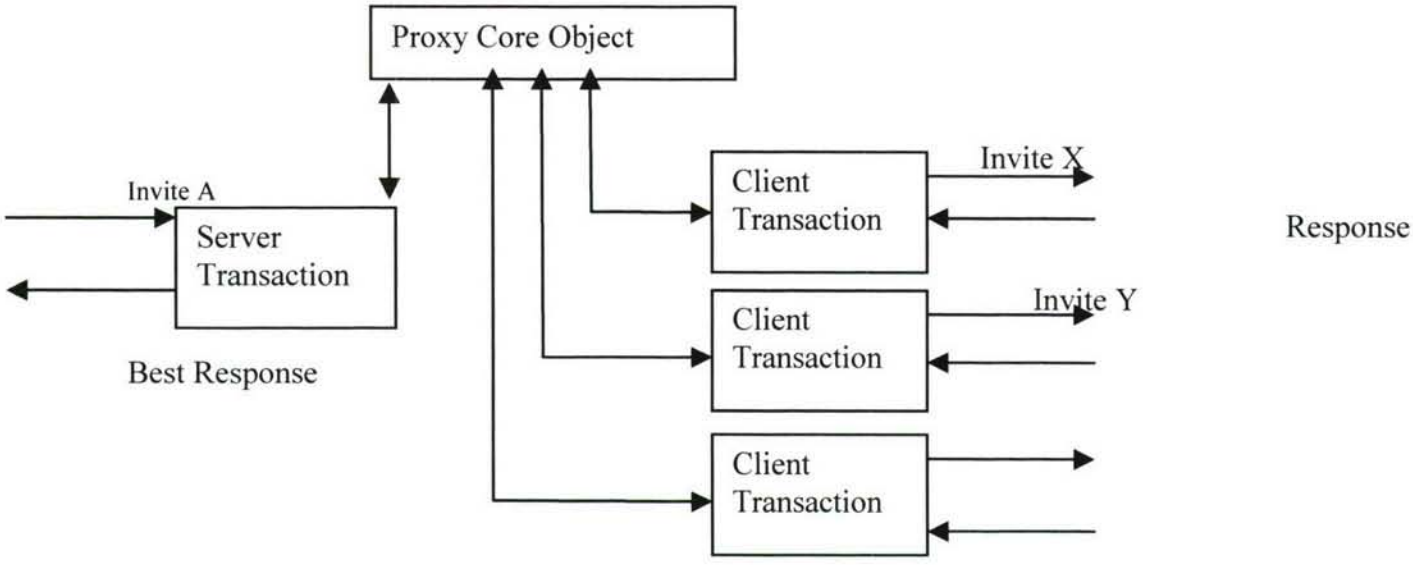


Figure 3-19. Proxy Core Object

The proxy server must determine the destination address to which the message is to be forward to. This can be done using two different methods. The proxy server uses the SIP destination address contained in the "Request URL" to create a target-set. The other method is to use Domain Name System (DNS) resolution to resolve the SIP destination address into the form: transport protocol, IP Address, port. During this process the proxy server may have to resolve multiple addresses if the destination address is registered in multiple locations. The target-set can be obtained using two different methods. The easiest of the two is when the "Request URL" is defined so the proxy has to forward the message to the defined address. If this is not the case, the proxy must determine the address using different methods. It can access the location service on the network that is maintained by the SIP Registrar. A database that is located on the network for address resolution can interact with the Presence Server to determine if the address is present and is logged into the network. The final method is using an algorithmic substitution on the destination address to resolve a new one that will be used to forward the message. The DNS resolution follows the standard process for DNS look-ups. The use of an advanced DNS scheme is recommended for different reasons. The DNS scheme can be used for resilience in the case of a server failing or in the area of load balancing. This can be done through dynamic adjustments in the DNS tables.

In Figure 3-20, the simplest process of a proxy is shown. The request is forwarded from proxy to proxy until it reaches the recipient. The recipient then responds and the response is forwarded back to the initiator.

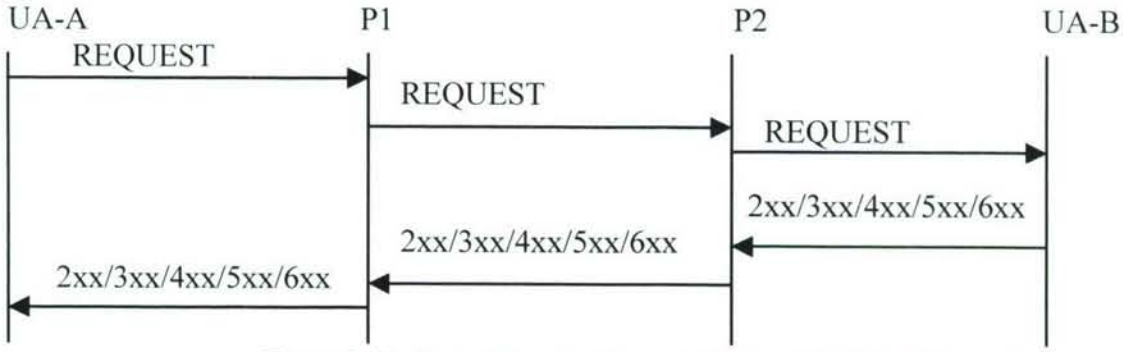


Figure 3-20. Proxy Diagram Request Forward/Recipient Response

Figure 3-21 shows an invite, that receives a non-2xx response. Each proxy server responds back that it is trying and then forwards on the request. When the recipient responds back, the response is forwarded back through each step with acknowledgment along the way.

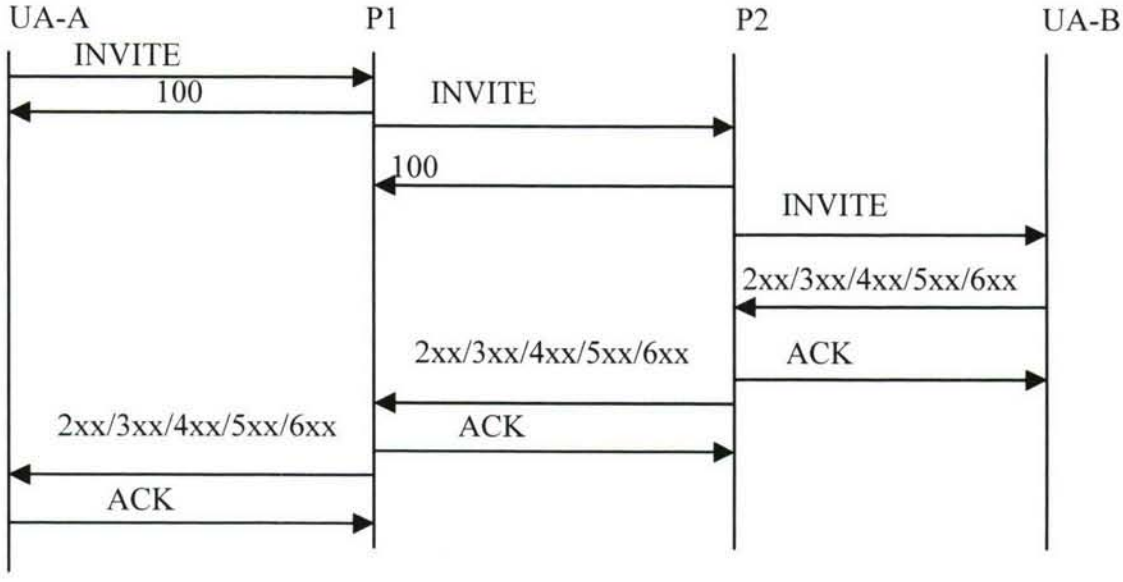


Figure 3-21. Proxy Diagram, Non-2xx Response

In Figure 3-22 the only change is that the recipient is accepting the call so the 180 Ringing of the phone response is shown, then the 200 OK that shows the recipient picking up the call.

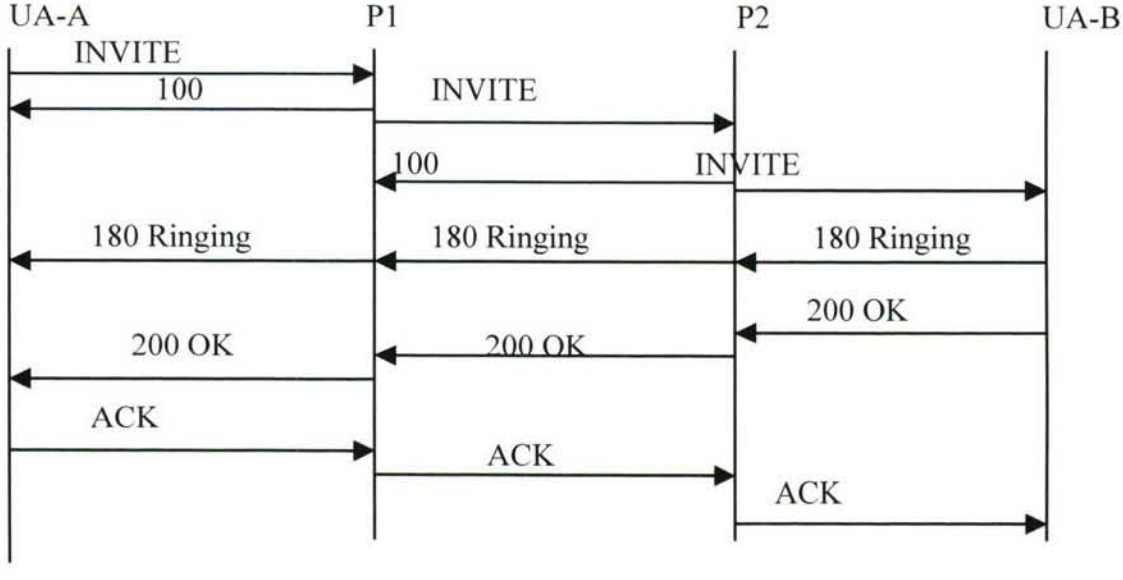


Figure 3-21. Proxy Diagram, Recipient Accepting Call

In Figure 3-23 an INVITE is sent which the proxy requires authentication of the initiator before it will forward the request on. The proxy responds with a 407 that challenges the initiator to send its credentials. After the authentication is complete it has no change from one that did not require authentication.

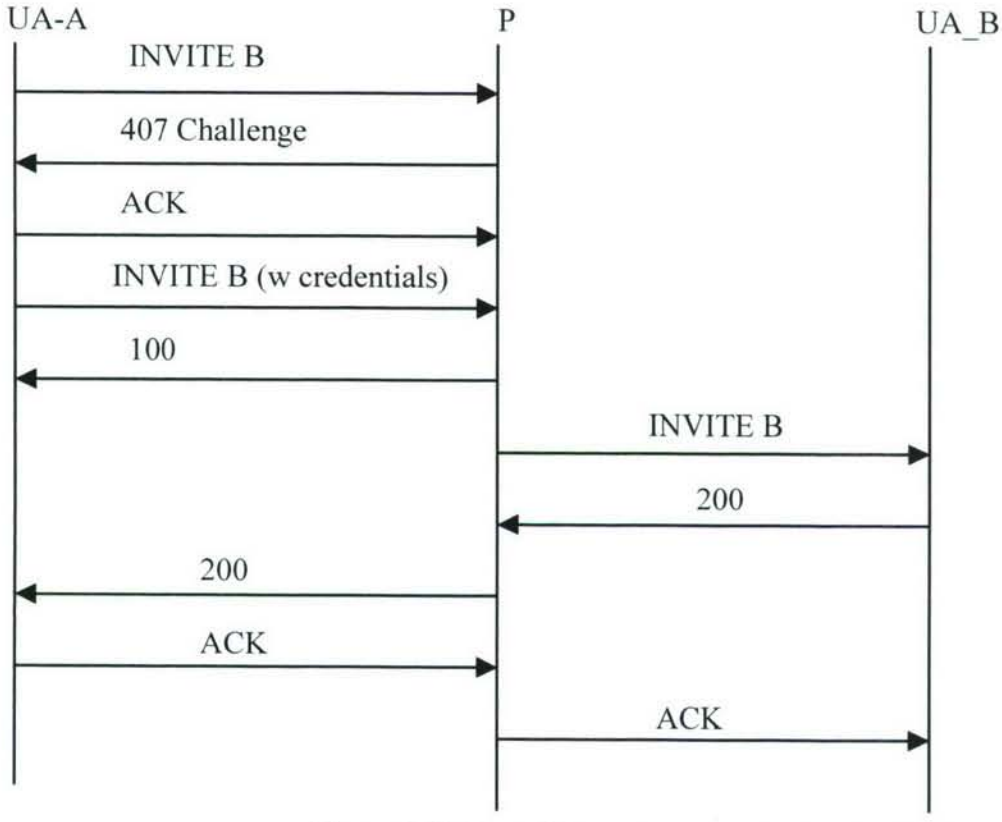


Figure 3- 22. Proxy Diagram, Authentication Required

In Figure 3-24 the proxy parallel forks the request because the recipient has two addresses that it can be reached at. After UA-C sends its 200 OK, the proxy cancels the request to UA-B; UA-B responds with a 200 OK to acknowledge the CANCEL.

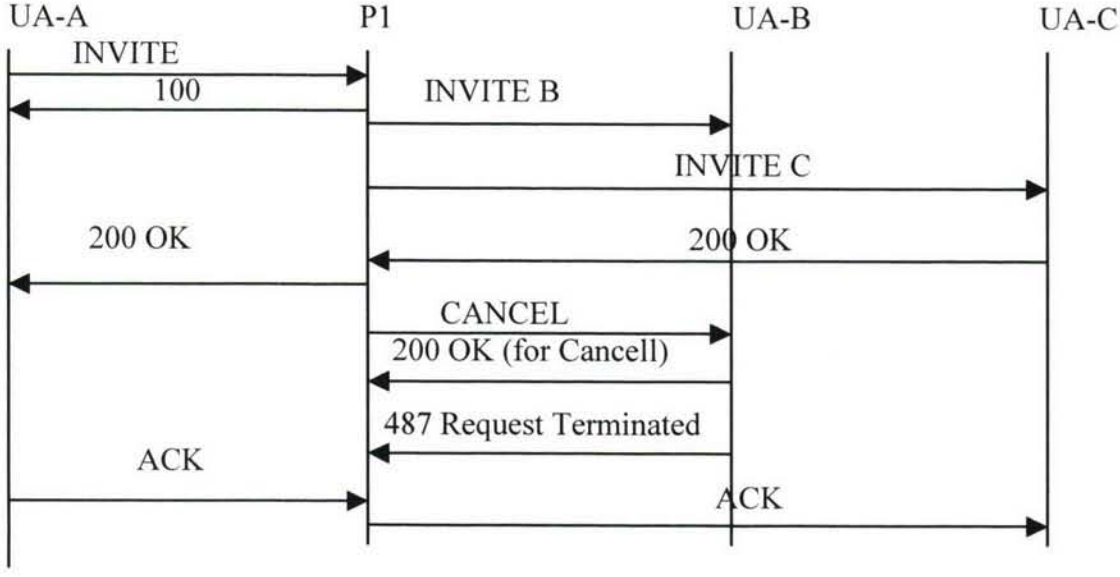


Figure 3-23. Proxy Diagram, Parallel Forks Request

In Figure 3-25 the proxy performs a sequential forking of the request, so it must wait for a response from UA-B before it can do the INVITE to UA-C. After that, it is a standard processing of the 200 OK and the ACK.

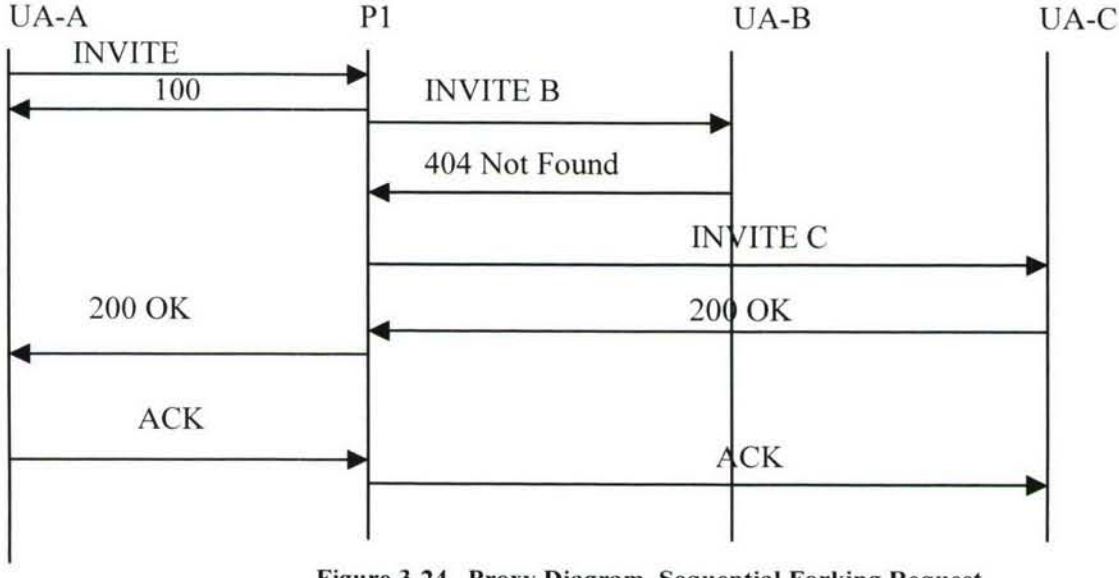


Figure 3-24. Proxy Diagram, Sequential Forking Request

3.5.2 Registrar Server

The RFC 3261 defines a registrar server as: " a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles". This server takes in a register request from a client and adds the information to a location service database. The server and the database may be located in the same server or different servers; the implementation is not defined in the specification itself. The purpose for this is to connect the external address for a client to the internal address of where the client is located. In many environments the Registrar server will require the client to authenticate before adding the information into the location service. This is done by issuing a 401 (unauthorized) response, and challenging the client to authenticate with a name and a password.

In Figure 3-26 the process of registration is very simple. It can be complicated by the additional authentication being required by the register server.

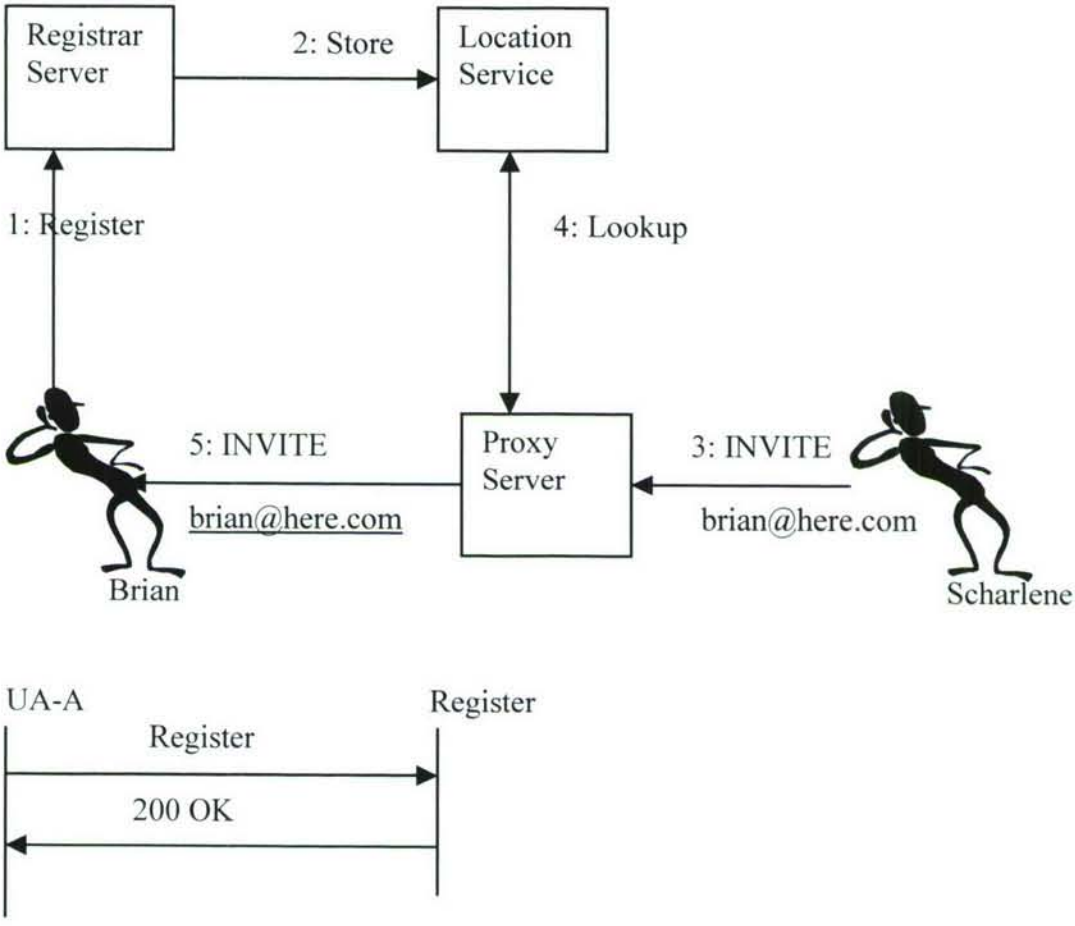


Figure 3-25. Registration Server Diagram

3.5.3 Redirect Server

In RFC 3261 the definition states: "Is a user agent server that generates 3xx response to requests it receives, directing the client to contact an alternate set of URIs." The new addresses are returned in the Contact header of the response message (see Figure 3-27). This is the simplest of the different servers.

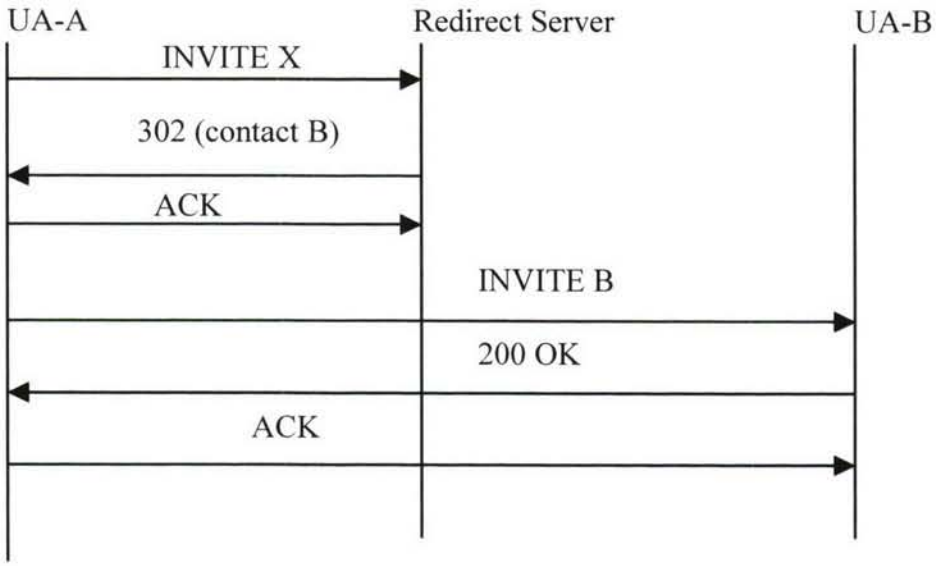


Figure 3-26. Redirect Server

Redirection is designed to be low process utilization that allows the server to be highly scalable. It may also require authentication and uses the same method as the Registrar server. Table 3-5 is a list of the responses that are returned from the server.

Table 3-5. Responses From Redirect Server

Response	Meaning
300 Multiple Choices	The address resolved to multiple addresses that are for the user. Can return multiple records.
301 Moved Permanently	The user no longer is found. The requesting client should try the new address. Can return multiple records.
302 Moved Temporarily	The user is temporarily located at a different address that the client should contact. Can return multiple records.
305 Use Proxy	The requested user must be contacted through the proxy that is contained in the Contact field
380 Alternative Service	The use of this response code is not defined in the SIP specification. The purpose is for the user to try to contact the client through a alternative service.

3.5.4 Back-to-Back User Agent (B2BUA)

The definition that the RFC 3261 gives to it is: "is a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request would be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS no explicit definitions are needed for its behavior."

In many ways the B2BUA can be compared to the H.323 gatekeeper in routed mode. By being the UAS and UAC, it hides the identity of the initiator of the message, and is enabled to make modifications to the header and SDP manipulations. In draft "draft-ietf-sipping-3pcc-06.txt"; Third Party Call Control (3PCC), the B2BUA is capable of disconnecting and initiating dialogs on a single end of the dialog. With this functionality, the B2BUA added many benefits to the environment by adding these features:

- PBX features
- Initiate or modifying dialog states
- Supporting Third Party Call Control (3PCC)
- Can edit messages in ways forbidden to Proxy Servers
- Hiding the initiator from the rest of the network
- Tracking dialog state, can be used for billing

With these features the B2BUA can support several different applications like IP-PBX, Call Center Application, and Firewall transferal. These applications take full use of the above features to manipulate the messages, but this results in heavy processing that leads to issues with scalability on a single system. Because the B2BUA is in the middle of the dialog, it is a single point of failure, which is not the case of a proxy server. The establishment and tear down of calls is complex, so the calls per second are reduced. To add to these problems is that it retains state of all the calls in process resulting in memory consumption. B2BUA should be implemented in a high-availability configuration using the different methods discussed in other sections of this report.
In Figure 3-28 the B2BUA server is in the middle of the communications between UA-A and UA-B. As UA-A makes a request to B2BUA, it then creates its own request and sends it to UA-B. In this way UA-A never talks directly to UA-B.

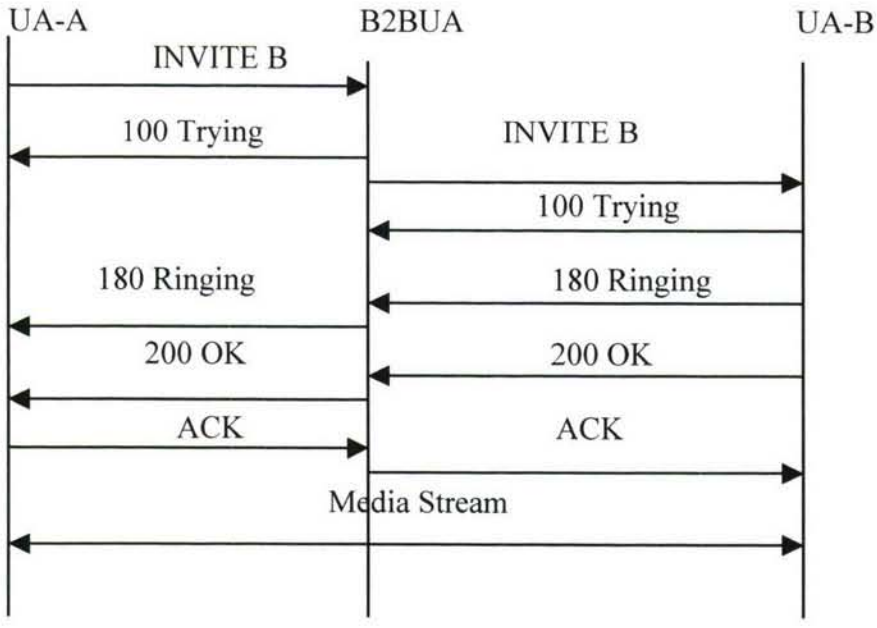


Figure 3-27. Back-to-Back User Agent Diagram

3.5.5 Notification Server

The concept of a Notification server is described in RFC3265, but it never defines a specification for it. It defines a general implementation of an event notification that is used to notify UA of events that happen. In this SIP-extension framework it allows an entity to subscribe to be notified of events that are happening on the network. The Notifier in this architecture is responsible for receiving the SIP SUBSCRIBE requests to determine the validity of the request and create the subscription object. It is also responsible for sending out notification to the scribers of events that happen that the individual has subscribed to receive. Depending on the authentication requirements of the application that the Notifier is located in, it may require UA to authenticate before proceeding with the request. The communications of the events are contained in Event Packages that are defined in several of the RFC and drafts, such as Presence and Winfo. The "presence" gives the willingness of a user to communicate with other uses. The Winfo is called watcher information. This is when a subscriber requests to be notified of a set event. These can be combined so when an individual sets their presence, the Notifier will send out an event package to any user that has subscribed to see the presence of the user when he changes his presence setting.

3.5.6 Presence Server

The Presence Server is a kind of Notification Server that only deals with presence. Presence is how a user lets other users know their willingness to be contacted, even before the user attempts a call. It is presently be defined by the IETF SIMPLE workgroup. They are working in the framework of presence and instant messaging called: Common Presence and Instant Messaging (CPIM). In the design it is composed of these components:

- Presence User Agent (PUA) – This is the user that collects the presence information and is referred to as Presentity User. This data maybe phone, cell-phone, PDA, soft-phone and geo-location system; each of these would supply presence data.

- Presence Agents (PA) – This is a new entity for SIP that is responsible for receiving and handling presence subscriptions from the watchers. Receiving the presence information from the PUA, through SIP or other means, and composing presence status from the fragmented data. From this data then notifying all the subscribed watchers for that presence information.
- SIP Proxy – Forward the presence information from the watcher and PUA without knowing the contents of the message.
- Presence Server – A UA that processes the SUBSCRIPTION requests locally or as a proxy by just forwarding them along to another Presence Server (see Figure 3-28).

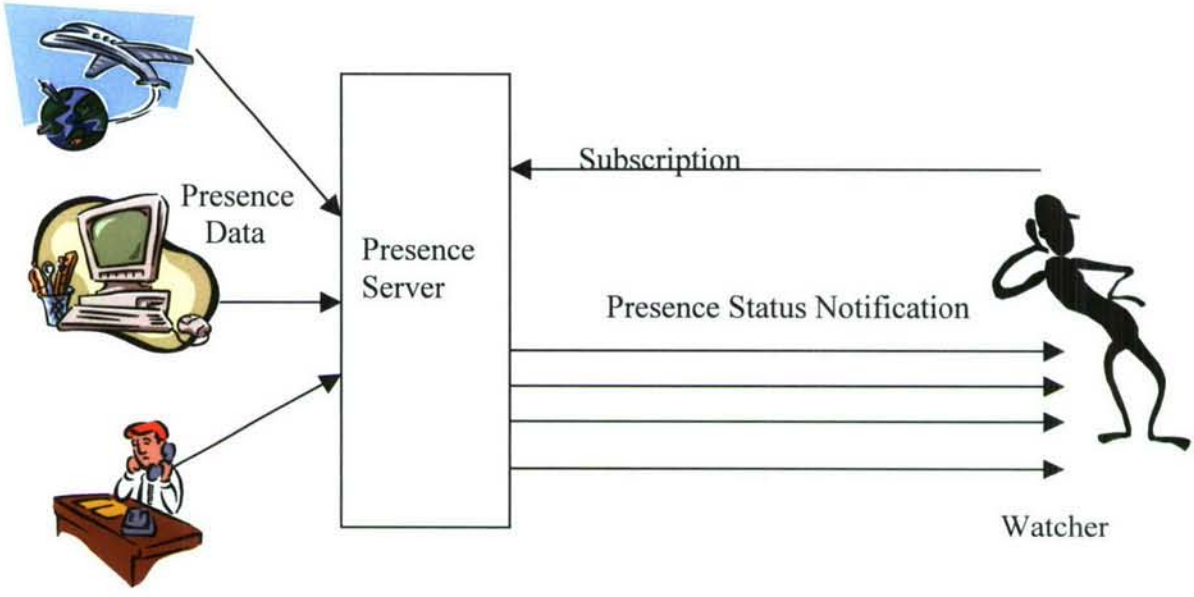


Figure 3-28. Presence Server

In Figure 3-29 the Watcher is showed to subscribe to the Presence Agent. As the Presentity changes its status, the Presence Agent sends notification to the Watcher of the change.

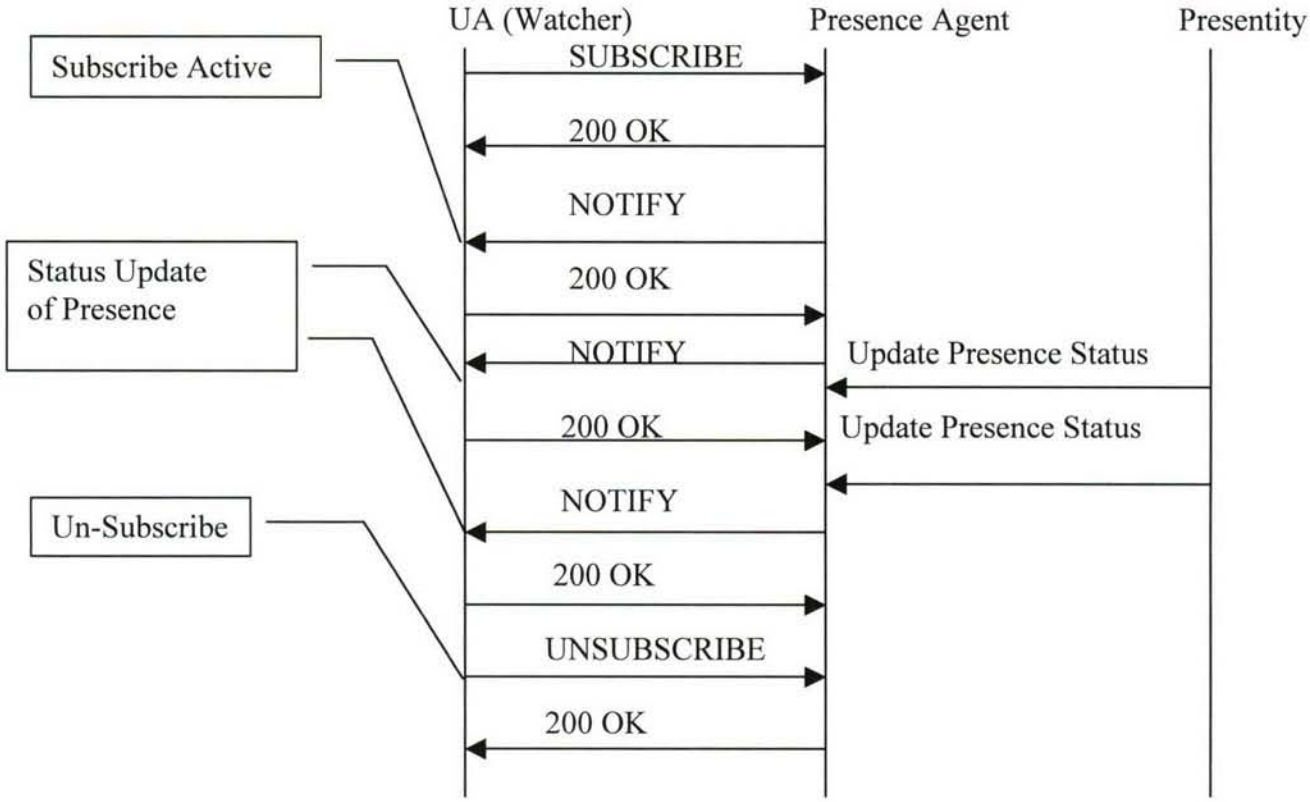


Figure 3-29. Presence Agent Diagram

3.5.7 SIP Server Error Codes

SIP, like its predecessor in the Internet world, all have errors that are from the same standards baseline. In many cases, such as authentication, the returned error is not a problem; it just requires the entity to authenticate itself before the server will process its request. The errors are broken into three major sections:

- 4xx – Method Failures
- 5xx – Server Failure
- 6xx – Global Failure

From this each group of 100 is broken down into individual errors (see Table 3-6). A client only needs to know the group that the error is in to handle it, but if the client knows the full meaning of the error, it can handle the cause gracefully.

Table 3-6. SIP Server Err`or Codes

SIP event	Cause
400 Bad request	Interworking, unspecified
401 Unauthorized	Bearer capability not authorized
402 Payment required	Call rejected
403 Forbidden	Bearer capability not authorized
404 Not found	Unallocated (unassigned) number
405 Method not allowed	Interworking, unspecified
406 Not acceptable	Interworking, unspecified
407 Proxy authentication required	Call rejected
408 Request timeout	Recover on Expires timeout
409 Conflict	Temporary failure
410 Gone	Unallocated (unassigned) number
411 Length required	Interworking, unspecified
413 Request entity too long	Interworking, unspecified
414 Request URI (URL) too long	Interworking, unspecified
415 Unsupported media type	Service or option not available
420 Bad extension	Interworking, unspecified
480 Temporarily unavailable	No user response
481 Call leg does not exist	Interworking, unspecified
482 Loop detected	Interworking, unspecified
483 Too many hops	Interworking, unspecified
484 Address incomplete	Address incomplete (invalid number format)
485 Address ambiguous	Unallocated (unassigned) number
486 Busy here	User busy
487 Request cancelled	Interworking, unspecified
488 Not acceptable here	Interworking, unspecified
500 Internal server error	Temporary failure
501 Not implemented	Service or option not implemented
502 Bad gateway	Network out of order
503 Service unavailable	Service or option unavailable
504 Gateway timeout	Recover on Expires timeout
505 Version not implemented	Interworking, unspecified
580 Precondition Failed	Resource unavailable, unspecified
600 Busy everywhere	User busy
603 Decline	Call rejected
604 Does not exist anywhere	Unallocated (unassigned) number
606 Not acceptable	Bearer capability not presently available

3.5.8 Features of a Typical IP-PBX

Table 3-7 is a list of features that are supported by Sphere's Sphericall IP PBX in release 5.[1] The list is very extensive, compared to the few items that were determined to need to be implemented in SIP Feasibility section and appendix. Joint Interoperability Test Command (JITC)-certified Sphericall IP PBX delivers assured connectivity via MLPP for special C2 (command and control) users including strategic leadership and those who manage strategic assets.

Table 3-7. Features Supported Sphericall IP PBX Release 5

General Telephony Services
Call Announce
Call Transfer
Call Coverage: Multi-Level, Follow Me, Conditional
Call forward
Call Hold
Call Waiting
Music-On-Hold
On-Hold Reminder
Dial-Out Authorization Codes
Direct Inward Dial
Direct Outward Dial
Inbound Routing Schedules (Automatic)
Message Waiting Indicators
Multi-Party Conferencing
Park Zones
Pickup Groups
Class Of Service Profiles
Permission Lists: Allow / Disallow Specific Numbers
Trunk Hunt Groups: Directional
User Access Authorization Codes
Automatic Route Selection (ARS)
Call Recording (Optional)
Call Admission Control
Multi-Level Precedence and Preemption for Emergency / Critical Communications
Call Accounting
Call Detail Reporting
Data Export: Originator ID, Receiver ID, Intended Receiver ID, Time, Duration, Outcome, Reason
Key Industry Standards Support
SIP - RFC 2543 / 3261
MGCP - RFC 2705 / 3149
SIPConnect for SIP Trunking
SIMPLE (Windows Messenger)
TAPI 3.0
DirectX 8.0
SMDI
TCP / IP / UDP
DHCP
FTP / TFTP
SNTP
RTP / RTCP
SOAP
XML
Advanced Communications Features
Call Recording (Optional)
Multi-Level Precedence and Preemption for Emergency / Critical Communications
Softphone for Mobile and Remote Users
User Presence Status Monitoring

[1] http://www.spherecom.com/product_docs/Sphericall_Data_Sheet_53106.pdf

Standard Telephony Features*
Caller ID Display
Call Transfer (Attended or Unattended)
Mute
Hold
Park / Unpark
Do Not Disturb
Transfer to Voice Mail
Redial
Incoming Call Indication with Caller ID
Message Waiting Indication
Missed Call Indication with Caller ID
Multi-Party Audio Conferencing
* Phone/device dependent.

3.5.9 Summary

The list of entities for SIP servers is small compared to H.323. Even though they are listed separately, most manufacturers include several of them into a single application package. The RFC 3265 and the drafts define each server in a functional description, but the method of implementation is left up to the implementer of the servers. Depending on the functionality that is required for the implementation, only some of the server functionality is required. The B2BUA is the core server in the implementation of an IP-PBX, and then the Presence Server can be added with them and implemented. It is a balancing act to handle the throughput that is required with the reduction of hardware. When the system is being designed for high-availability, the structuring of servers needs to be evaluated. Many COTS products have all the functionality implemented into a single solution on a single server. A few of the COTS vendors such as CISCO, has several independent servers that each performs a single function. When they are implemented in a high-availability installation, the number of servers required doubles. The specifications ignored the operating system that the servers are installed on. Because of the throughput that is required, as well as the stability of the application, the operating system needs to be selected carefully to achieve a mix of stability and functionality. There are many expanded references to the RFC3261 specification, one of them on Tech Invite: http://www.tech-invite.com/Ti-sip-CF3261.html and included in the appendixes as Appendex-Tech-invite-SIP-3261-24.pdf. This document walks you through the specification with diagrams explaining each part as you do through the individual pagers.

3.6 H.323 and SIP

There were several standards that have appeared over the years for VoIP, but only two have survived the test of time, H.323 and Session Initiated Protocol (SIP). H.323 was the first one to be adopted by industry so it has a major following. In the past couple years SIP has been endorsed by industry and many vendors are developing SIP based products. Several are moving from H.323 products and replacing them with SIP based products.

3.6.1 H.323

H.323 is the International Telecommunication Union- Telecommunication (ITU-T) recommendation specification that is primarily targeted for teleconferencing multimedia traffic over a packet-based network. The standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multipoint conferences. It is presently at version 5 and is made up of several supporting ITU drafts and annexes. The H.323 system is broken down into multiple parts: terminal, gateway, gatekeeper and multipoint control units (MCU).

A terminal is defined in the H.323 specification to contain a system control unit, a media transmission, an audio codec and a packet-based network interface and may also include video codec and user data applications.

The Gateway is responsible for the setup and teardown of the call, as well as translating between audio, video, and data formats if there is interconnection with a switch circuit network (SCN).

The Gatekeeper is an optional component that supplies pre-call and call-level control services for the endpoint. If a Gatekeeper is present in the system it must supply and perform these tasks: address translation, admissions control, bandwidth control and zone management. The Gatekeeper canoptionally provide these functionalities: call control signaling, call authorization, bandwidth management and call management. An H.323 Proxy Server can work as a Gatekeeper on the outer edge of the network, as well as supplying security. A firewall can be setup to trust the Proxy and pass it all H.323 traffic so the proxy can handle the traffic and direct it as required.

The Multipoint Controller is required for conferences between three or more endpoints. It transmits the capability of each end device and can change them during the conference if required.

3.6.1.1 H.323 Diagram

Figure 3-30 provides an example from VoIP Foro web site for a H.323 call [60].

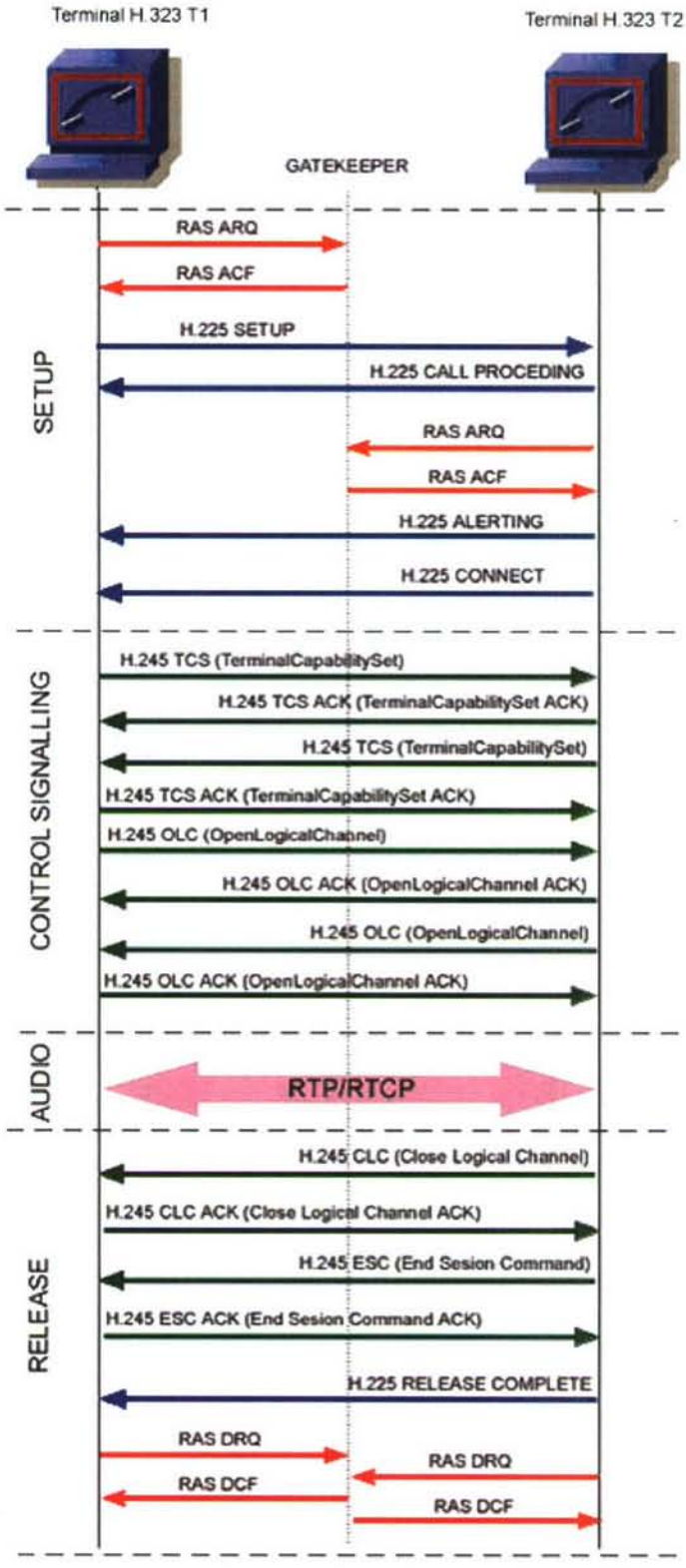


Figure 3-30. H.323 Call Diagram

An H.323 call has four different processes as follows:

1. SETUP
   a. Terminal 1 registers itself with the gatekeeper using the Register, Admission, Status (RAS) protocol () sending an Admission Request (ARQ) message and receiving an Admission Confirm (ACF) message.
   b. Using H.225 protocol (used for setup and release of the call) terminal T1 sends a SETUP message to T2 requesting a connection. This message contains the IP address, port and alias of the calling user or the IP address and port of the called user.
   c. T2 sends a CALL PROCEEDING message warning on the attempt to establish a call
   d. Now, T2 terminal must register itself in the gatekeeper as T1 previously do.
   e. Alerting message indicates the beginning of tone generation phase.
   f. And finally, the CONNECT message shows the beginning of the connection.

2. CONTROL SIGNALLING

In this phase a negotiation using H.245 protocol is opened (conference control), the interchange of the messages (request and answer) between both terminals establishes who will be the master and who the slave, the capacities of the participants and the audio and video codecs to be used. When the negotiation finishes the communication channel is opened (IP addresses, port).

The main H.245 messages used in this step are:

   a. Terminal Capability Set (TCS). Message capabilities supported by the terminals that take part in a call
   b. Open Logical Channel (OLC). Message to open the logical channel which contains information to allow the reception and codification of the data. It contains information of the data type that will be sent.

3. AUDIO

Terminals start the communication using the RTP/RTCP protocol.

4. CALL RELEASE
   a. The calling or the called terminal can initiate the ending process using the Close Logical Channel (CLC) and End Session Command (ESC) messages to finish the call using again H.245.
   b. Then using H.225 the connection is closed with the RELEASE COMPLETE message.
   c. And finally the registration of the terminals in the gatekeeper are cleared using RAS protocol.

3.6.2 Session Initiated Protocol (SIP)

SIP was created by Internet Engineering Task Force (IETF) in 1999 and then updated in 2002 with RFC 3261. It is still being developed and extended to fulfill the signaling needs of the future. SIP was designed differently than the architects of H.323. It was designed to be extended in the future and was given the functionality to negotiate the features that the server and client can support. It was also developed so two peers could communicate without any server in between

them. This peer-to-peer allows the end devices call User Agents Client (UAC) to make their own connection with no reliance on any other application. This can be done by connecting two SIP phones to a network and entering in the IP address of the other phone. The other phone will ring and a conversation can be done. When an IP-PBX is involved the RTP stream can still go between the two UAC and not through the IP-PBX or the IP-PBX can be in between the stream of RTP. SIP provides five different functionalities:

a. User Location: The ability to discover end users inherently makes it work for mobility of users of SIP. Discovery of location allows for the creation of sessions between UA.
b. User Capabilities: The ability to discover the media capability of the devices in the session.
c. User Availability: Determine the willingness of the end user to join the session.
d. Session Setup: Establishment of session parameters for UA to join into a communication session.
e. Session Handling: Handles the modification, transfer and termination of sessions between UA.

3.6.2.1 SIP Methods

The commands that are used in SIP are called methods. SIP implements very few methods, which can then qualify with parameters. This method makes the program and understanding the packets easier then other VoIP protocols. As developers define new parameters, they are setup in a hierarchal structure that is registered with the Internet Assigned Numbers Authority (IANA).. During the INVITE process the client and server agrees on a list of valid commands that will be used during the transaction.

SIP methods are defined in Table 3-8.

Table 3-8. SIP Methods

SIP	Method Description
INVITE	Invites a user to a call
ACK	Used to facilitate reliable message exchange for INVITEs
BYE	Terminates a connection between users or declines a call
CANCEL	Terminates a request, or search, for a user
OPTIONS	Solicits information about a server's capabilities
REGISTER	Registers a user's current location
INFO	Used for mid-session signaling

3.6.2.2 SIP Responses

The errors that are generated during the processing of a call are also structured in a hierarchal structure (see Table 3-9). Because SIP is modeled after the HTTP model, the error codes closely resemble the one used by HTTP. New errors are defined by developers and are also registered with the IANA. The node only needs to understand the highest level of the error to determine how it will react to the error. This makes new code compatible with older applications.

The following Table 3-9 provides SIP responses:

Table 3-9. SIP Responses

Error Code	Description	Examples
1xx	Informational	100 Trying, 180 Ringing
2xx	Successful	200 OK, 202 Accepted
3xx	Redirection	302 Moved Temporarily
4xx	Request Failure	404 Not Found, 482 Loop Detected
5xx	Server Failure	501 Not Implemented
6xx	Global Failure	603 Decline

3.6.2.3 SIP Call Diagram

SIP interacts with many other protocols to extend the functionality of the base SIP protocol. SIP interacts with two types of protocols. The first is standard network protocols that enable network functionality, such as Domain Name System (DNS), Session Description Protocol (SDP), Real-time Transport Protocol (RTP), Resource ReSerVation Protocol (RSVP) and Transport Layer Security (TLS). It also uses other protocols from the IETF that extends the functionality of SIP so it can handle new features. This would include protocols such as Caller , Callee Preferences and Instant Messaging. Many of the extensions coming from SIP are for Instant Messaging and Presence Leveraging Extensions (SIMPLE). SIMPLE is an IETF group that is working on proposing extensions to SIP.

Figure 3-31 is an example of a call done through a SIP Proxy between to UAC with the SIP protocol.[61]

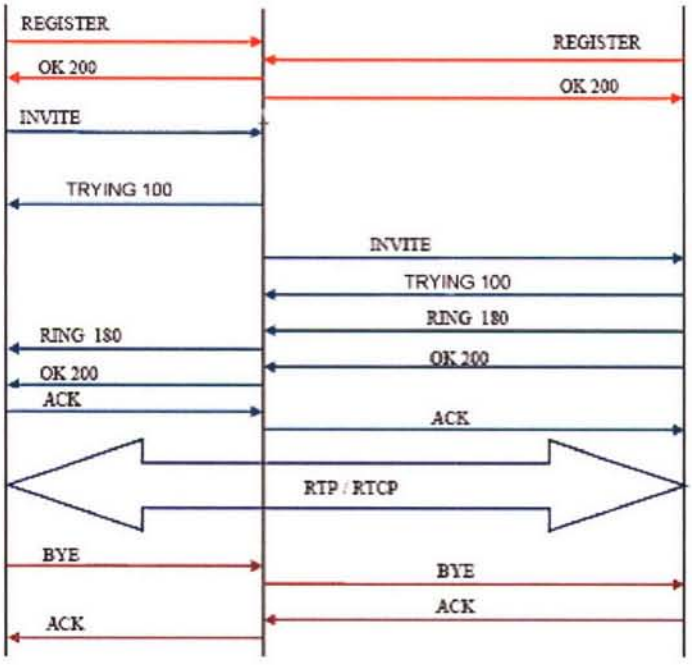


Figure 3-31. Diagram of Call Made Through SIP Proxy to Two UAC

- The first step is the user register. The users must register themselves to be found by other users. In this case, the terminals send a REGISTER request, where the fields "from" and "to" correspond to the registered user (see Figure 3-32 and Figure 3-33). The Proxy server, who acts as Register, consults if the user can be authenticated and sends an OK message if there is no problem.

```
Via: SIP/2.0/UDP
192.168.0.100:5060;rport;branch=z9hG4bK646464100000000b43c52d6c00000d1200000f
03
Content-Length: 0
Contact: <sip:20000@192.168.0.100:5060>
Call-ID: ED9A8038-A29D-40AB-95B1-0F5F5E905574@192.168.0.100
CSeq: 36 REGISTER
From: <sip:20000@192.168.0.101>;tag=910033437093
Max-Forwards: 70
To: <sip:20000@192.168.0.101>
User-Agent: SJphone/1.60.289a (SJ Labs)
Authorization: Digest
username="20000",realm="192.168.0.101",nonce="43c52e9d29317c0bf1f885b9aaff1522d
93c7692"
,uri="192.168.0.101",response="f69463b8d3efdb87c388efa9be1a1e63"
```

Figure 3-32. Proxy User Register Transaction

- The following transaction corresponds to a session establishment. This session consists of an INVITE request of the user to the proxy. Immediately, the proxy sends a TRYING 100 to stop the broadcastings and reroute the request to the B user (see Figure 3-32). The B user sends a Ringing 180 when the telephone begins to ring and it is also rerouted by the proxy to the A user. Finally, the OK 200 message corresponds to the accept process (the user B response the call) (see Figure 3-34).

```
Internet Protocol, Src Addr: 192.168.0.101 (192.168.0.101), Dst Addr:
192.168.0.100 (192.168.0.100)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Session Initiation Protocol
Status-Line: SIP/2.0 200 OK
Status-Code: 200
Resent Packet: False
Via: SIP/2.0/UDP
192.168.0.100:5060;rport;branch=z9hG4bK646464100000000b43c52d6c00000d1200000f
03
Content-Length: 0
Contact: <sip:20100@192.168.0.100:5060>
Call-ID: ED9A8038-A29D-40AB-95B1-0F5F5E905574@100.100.100.16
CSeq: 36 REGISTER
From: <sip:20000@192.168.0.101>;tag=910033437093
Max-Forwards: 70
To: <sip:20000@192.168.0.101:5060>
Authorization: Digest
username="20100",realm="192.168.0.101",nonce="43c52e9d29317c0bf1f885b9aaff1522d
93c7692",uri="sip:192.168.0.101",
response="f69463b8d3efdb87c388efa9be1a1e63"
```

Figure 3-33. OK 200 Accept Transaction

- At this moment the call is established, and the RTP transport protocol starts with the parameters (ports, addresses, codecs, etc.) of the SDP protocol.

- The last transaction corresponds to a session end. This is carried out with a BYE request to the Proxy, and later reroute to the B user. This user replies with an OK 200 message to confirm that the final message has been received correctly.

3.6.3 Comparison of H.323 and SIP

The two protocols were designed in different ways. The philosophy for SIP is related to the Internet and is considered "New World", where H.323 is complex and considered "Old World". H.323 was designed to embrace the older circuit base telephony model, where SIP was designed around the more lightweight Internet protocol called Hypertext Internet Protocol (HTTP). Because of the differences in designs, H.323 uses many more protocols in its operation resulting in a specification that is more than 730 pages long. The SIP specification is only 128 pages long and covers the base, as well as the call control extensions. From the figures above you can see the complexity of H.323 compared to SIP. SIP is designed to be a simple tool kit that reuses elements from the Internet protocols (URL, MIME, DNS) where H.323 specifies everything new including the codecs and how to carry the packets of RTP. H.323 has hundreds of elements compared to SIP which has only 37 headers according to RFC 3261. SIP is developed around a clear text header system that allows individuals to look at the packets and determine what is happening in the process. Because of this simpler design, a complete client GUI-based application can be designed and coded in just two man-months. A H.323 header is binary representations and is based on ASN.1 and the pack encoding rules (PER). H.323 reliance on multiple protocols needs to interact to complete a single function. This results on multiple packets being exchanged to setup a single call, as compared to SIP, which uses a single packet to setup the call.

The two protocols also differ in the ability of them to be expanded on. SIP being created after the lessons learned from HTTP and SMTP, has built in extensibility and compatibility functions. The client sends a list of features that it wants to use to the server. The server then evaluates the list and if it does support the list it returns the list that it does support. The client then determines the problematic features and determines a simpler fallback operation. Any developer can add to the list of features by registering the name of the feature with the IANA. This way compatibility is maintained across different versions. In this same vein the errors are handled in a hierarchical structure of numerical error numbers. There are six basic categories and each category is divided into 100 sections, this way only the class of the error needs to be understood by the device. H.323 has a system of extensibility, but it is more vendor oriented. The parameters are defined by the vendor and never registered so no other vendor knows how to proceed with the value contained in the field. SIP uses Session Description Protocol (SDP) to convey the codec that the end device supports. The codecs are registered with the IANA and new ones can be added as they are developed. H.323 only supports codecs that are developed by UTI and have code-points; they are centrally registered and standardized.

SIP is a peer-to-peer protocol so only the call control is required to be processed by the server. This reduces the amount of processing that a SIP server does for each individual call and during the call the server has no handles that are consumed. This reduces processor, memory, so the number of calls per second is increased. H.323 requires the calls to be passed through the gatekeeper, so as the number of calls increases the memory and process requirements also

increase; this results on a limitation of the ability for a gatekeeper to handle the same number of calls per second. SIP uses a hierarchical URL addressing scheme that allow addresses to be embedded into web pages and emails, where H.323 defines its own addressing scheme that is not scalable and is not able to be clean embedded into other documents.

3.6.4 Summary

In this comparison of SIP and H.323 we have shown that SIP is a more flexible, extendable, scaleable and less complicated than H.323. "SIP Vs. H.323 – Comparative" by VoIP Foro can add more details the conclusions that were arrived at. Note that the VoIP Foro page doesn't take into account the many extensions that have been added to SIP over the pass couple years. As time moves on, SIP continues to get extensions as the drafts are ratified into RFC, making the decision to adopt SIP easier and easier.

3.7 Open Source

3.7.1 Introduction

This section on Open Source Software (OSS) is meant as a review of the OSS community, and is not meant as a legal analysis. This is a review of the community at large and of who makes up this expanding alternative to proprietary software applications. Many mainstream products fall under this community such as: MySQL, Red Hat, and Fedora. The benefits of Open Source is that it can reduce internal costs of the software and result in faster, development cycles, bug fixes, and collaboration between many developers. Many companies, such as Google and Amazon, have developed their infrastructure around Open Source projects.

3.7.2 Open Source

Open Source in the most general term is software that is distributed with a relaxed license.

3.7.3 The Open Source Definition

Submitted by Ken Coar [34]

Introduction

Open source doesn't just mean access to the source code. The distribution terms of open-source software must comply with the following criteria:

1. Free Redistribution

The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

2. Source Code

The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of obtaining the source code for no more than a reasonable reproduction cost preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.

3. Derived Works

The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.

4. Integrity of the Author's Source Code

The license may restrict source-code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.

5. No Discrimination against Persons or Groups

The license must not discriminate against any person or group of persons.

6. No Discrimination against Fields of Endeavor

The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

7. Distribution of License

The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

8. License Must Not Be Specific to a Product

The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

9. License Must Not Restrict Other Software

The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.

10. License Must Be Technology-Neutral

No provision of the license may be predicated on any individual technology or style of interface.

Two terms often used when discussing open source. One is the rights given to the developer/author known as "*copyright*" protection, whereby the author's work is protected under patents and trade secret laws from being copied or used in a manner not intended by the author. The second is "*copyleft*", in which the developer/author provides a license to other users whereby the source code is made available for use under certain terms and conditions, in particular the GNU Public License (GPL). the GPL attempts to insure that if derivatives are created, they will be made available under the same terms as the GPL. A review of the various licenses accepted by the Open Source Initiative will find that they vary from very restrictive, such as the Netscape Public License, to the GNU General Public License. The GPL provides that any modified code or code linked to the open source licensed under the GPL also be open source and be made freely available to the license granting free use without restriction. An example of which is the MIT Academic License. When designing if and how a third party source will be used as a part of a product, how the third party's code is licensed and whether their terms and conditions are compatible with the business strategy must be considered.

3.7.4 History

The OSS movement started in 1983 with the name "Free Software" and then in 1998, the name was replaced with "Open Source". In 1997 Eric S. Raymond assembled a group of essays that was called "The Cathedral and the Bazaar". [35] In this work he compared an organized method of development (cathedral) with a development process that contains multiple agendas and approaches (bazaar). He felt that the bazaar method would achieve a better final solution that fulfilled more individuals needs then the structured development process that was underway in industry at the time. Eric S. Raymond and Bruce Perens formed the Open Source Initiative in 1998. A presentation of Raymond's paper to Netscape convinced the CEO Jim Barksdale to release Navigator source code as Mozilla.

3.7.5 Comparing the Open Source Licenses

There are currently more than 50 licenses that have been accepted by the Open Source Initiative that meet the requirements of the open source community. Of those there are certain licenses that are more widely used and accepted. For reference, see Appendix G "Open Source SIP Whitepaper Phase One" for each of the accepted licenses with active links to the full text. Rather than trying to analyze each license, the components to be conscious of when determining whether or not certain open source is viable for a particular development effort are presented. Note that some open source licenses do not interoperate well with other closed source or open source licenses. It is important to be aware of the compatibility of the licenses when combining or linking source code into a larger program.
The current 50-plus licenses maintained by the Open Source Initiative (OSI) fall into four distinct types. [36]

3.7.5.1 Academic Licenses

Representing the most 'free' of open source licenses, Academic licenses place no requirements whatsoever on the license user. There is not even a requirement for the user to share modifications or redistribute them. Licenses in this category include the BSD (original license from BSD UNIX), MIT Academic license, and Apache licenses.
Academic licenses are designed to provide absolute freedom. The only marked restriction is that these licenses prohibit the leveraging of the original licensor's name as an endorsement in marketing efforts. Other than that, these licenses are truly intended for those who seek complete control over the software, its use, modifications, and subsequent re-releases independently or with another software package.
The BSD, granddaddy of open source licensing, originated within the University of California to grant the free use, modification, and distribution of software built within the institution. It has since become a public license available to open source developers.
The MIT was created by the Massachusetts Institute of Technology as a rewrite of the BSD license. The Apache license differs from the BSD and MIT only in its requirement that a notice be included in either documentation or source code of modified works to identify that the new distribution contains software created by the Apache Software Foundation.

3.7.5.2 Reciprocal Licenses

Like other licenses, Reciprocal licenses grant complete rights to the software's use to the developer and end user. The single difference lies in the requirement that any derivatives of the software be released under the same license, and that the source code must be released. The resulting new software must also be free.
The intent of reciprocity is to ensure that a growing universe of free software emerges, and that original works, as well as modified and new efforts, remain free to users. Some of the most popular software available today remains free and accessible due to its use of the GPL including Linux, MySql, the Bash shell, Mailman, gzip and grep.
The centerpiece of this category is the GPL, by original authors Richard Stallman and Eben Moglen, with input from the open source community at large. The Mozilla Public License also resides in this category.

3.7.5.3 Standard Licenses

Standards licenses seek to create a base standard of software and documentation. Modified and redistributed sources usually have to be distributed as patches, so as to not modify the core.

For example, imagine a situation in which a Web application is created to allow importing and exporting between the various popular blog applications. A Web developer grabs the source of this new software and builds in an additional function to migrate and convert specific design elements along with data. Under a standards license, the core application would be distributed with a plug-in to enable the latter new capability.
The goal of a standards license is to preserve an existing code base so that the originating author can come back to it and evolve it without difficulty. In some cases, plug-ins will not be affected. In others, the original author will update documentation to allow third-parties to update their plug-ins (often also called patches).

3.7.5.4 Content Licenses

Finally, Content licenses cover elements aside from code, such as art, copy and audio/video. Those familiar with Creative Commons (CC) will recognize this license, although a few are listed at OSI, including the Academic Free License.
One caveat with Creative Commons (CC) licenses is that if a Share-Alike attribute is included in a CC license, it makes the license reciprocal, similar to the GPL.

In most instances, in order to comply with the majority of third party licenses, amongst other terms and conditions provided in the individual license agreements, the author must acknowledged and all warranties to the source code be disclaimed unless specific warranties are provided to the user from the author in the license agreement. It is generally a good practice to include the copy right notice and any disclaimers in the installer of the product to ensure that the user is informed.

3.7.6 Sources to Locate OSS

There are many sources for OSS out on the Internet. The expansion of the Internet has made it a simple vehicle to share OSS between developers around the world. The following sections provides a few search engines that simplifies the finding and accessing of OSS:

3.7.6.1 Freshmeat.net Search Engine

Website: http://www.freshmeat.net
Searching capability: Yes
Number of results searching on "SIP": 64
Number of results searching on "VoIP": 80
"freshmeat maintains the Web's largest index of Unix and cross-platform software, themes and related "eye-candy", and Palm OS software. Thousands of applications, which are preferably released under an open source license, are meticulously cataloged in the freshmeat database, and links to new applications are added daily. Each entry provides a description of the software, links to download it and to obtain more information, and a history of the project's releases, so readers can keep up-to-date on the latest developments. [63]"

3.7.6.2 SIPfoundry

Website: http://www.sipfoundry.org

Wiki: http://sipx-wiki.calivia.com/index.php/Main_Page
Searching capability: No

Originally founded by Pingtel in 2004 as an initiative to create the first major open source community concentrating on VoIP technologies, SIPFoundry hosts a battery of SIP packages of their own creation. Their open source software dawned the title of sipX, shorthand for SIP PBX, and is available in a multitude of forms like sipXconfig, sipXtapi, and sipXtacklib.

3.7.6.3 SourceForge

Website: http://sourceforge.net
Searching capability: No
Number of results searching on "SIP": 151
Number of results searching on "VoIP": 176

SourceForge is one of the largest distributors of open source software on the Internet. A quick search of "SIP" turns up about 150 results. Sorting through the list may be a bit of a challenge, but provided you know exactly what you're looking for SourceForge makes it easy to download software, ask questions, even post bug reports. Additionally, SourceForge uses a revision control system to help contributors sync changes with the rest of the community.

3.7.6.4 VoIP-Info.org

Website: http://voip-info.org
Searching capability: No

VoIP-info.org one of the most extensive databases of information regarding VoIP technologies, containing thousands of pages of information. The site is a fairly traditional wiki-based format, allowing all members of the VoIP community to contribute. The site contains links to recent VoIP news, information on VoIP in general, and a good number of links to information on connecting VoIP to PTSN and cellular networks, VoIP PBX, and servers. It also contains exhaustive resources on specific open source products, such as Asterix, SER, sipX, and many others. A complete listing of all the open source software they have on record is available at http://www.voip-info.org/wiki-Open+Source+VOIP+Software.

Website: http://vovida.org
Searching capability: No

Vovida.org contains information and source code for several open source VoIP software packages, with a special focus of VOCAL, Vovida's own open communication application library. While VOCAL is the focus of the site, it also maintains a list of other SIP packages, including SIPRG, SIPSet, and SIPTiger, as well as other VoIP packages such as WinRTP, STUN Server, and more. Each piece of software has its own dedicated page featuring short descriptions, documentation, links to support, and links to the source code.

3.7.6.5 Wikipedia

Website: http://en.wikipedia.org/wiki/List_of_SIP_software
Searching capability: No

Wikipedia maintains a listing of nearly all open source and commercial SIP products. Many products also have their own Wikipedia pages filled with information, and links to their homepages. The list contains SIP servers, clients, firewalls, and communication products.

3.7.7 OSS Projects

This section provides a filtered list of open source SIP projects that were collected by searching the Internet for SIP open source projects that were currently active and had at least one release.

3.7.7.1 Open Source SIP PBXs

3.7.7.1.1 Asterisk

Website:http://www.asterisk.org
Win32Website:http://www.asteriskwin32.com
Language:C, variety of languages available for scripting
Platform: Unix/Linux, Win32, Mac OS X
Last Release: 6/29/2007
License: GNU Public License

Summary: "Asterisk® is a complete IP PBX in software. It runs on a wide variety of operating systems including Linux, Mac OS X, OpenBSD, FreeBSD and Sun Solaris and provides all of the features you would expect from a PBX including many advanced features that are often associated with high end (and high cost) proprietary PBXs. Asterisk® supports Voice over IP in many protocols, and can interoperate with almost all standards-based telephony equipment using relatively inexpensive hardware. [64]"

Features:

Full comprehensive support of all kinds of call services including call forward, call parking, call snooping, enhanced 911, music on hold, and call transfers

- Full support of all Time Division Multiplexing (TDM) protocols and SIP codecs
- Support computer telephony integration with embedded scripting interface supporting multiple languages
- Highly available, supporting remote offices
- Comprehensive feature list available at http://www.asterisk.org/support/features

3.7.7.1.2 CallWeaver

Website: http://www.callweaver.org/blog
Language: C
Platform: Various Unix, Linux, Mac OS X
Activity: Last release 6/07
License: GNU Public License

Summary: "CallWeaver is a community-driven vendor-independent cross-platform open source PBX software project (formerly known as OpenPBX.org). It was originally derived from Asterisk. Now it supports analog and digital PSTN telephony, multi-protocol voice over IP telephony, fax, software-fax, T.38 fax over IP and many telephony applications such as Interactive Voice Response (IVR), conferencing and call center queue management." [65]

Callweaver is a fork from Asterisk. Philosophical reasons for choosing CallWeaver over Asterisk can be found at http://www.voip-info.org/wiki/view/OpenPBX.org%20FAQ

Features:

- Features are very similar to asterisk, as it is a fork from Asterisk
- Callweaver has changed/upgraded some of the internal components and algorithms used in Asterisk, but the main functionality has stayed the same

3.7.7.1.3 FreeSwitch

Website: http://www.freeswitch.org/
Language: C
Platform: UNIX, Linux, Win32, Mac OSX
Activity: Last release 6/07
License: Mozilla Public License

Summary: "FreeSWITCH is an open source telephony platform designed to facilitate the creation of voice and chat driven products scaling from a soft-phone up to a soft-switch. It can be used as a simple switching engine, a media gateway or a media server to host IVR applications using simple scripts or Extensible Markup Language (XML) to control the callflow." [66]

Features:

- Supports various communication technologies including as SIP, H.323, IAX2 and GoogleTalk protocols
- Supports both wide and narrow band codecs making it an ideal solution to bridge legacy devices to the future. The voice channels and the conference bridge module all can operate at 8, 16 or 32 kilohertz and can bridge channels of different rate

3.7.7.1.4 sipX

Website: http://www.sipfoundry.org/sipXpbx/
Language: C++ and Java
Platform: Linux, Mac OSX, and various other UNIX
Activity: Last release 2/2007
License: Lesser GNU Public License

Summary: sipX started its life as a commercial SIP-based IP ECS (Enterprise Communications Server) solution. It became open source first in 2004 and therefore is still rather new. At the time major architectural decisions were taken for sipX it was already clear that SIP would become the protocol of choice for VoIP both on the Enterprise and Carrier side. Therefore sipX can be looked at as a next generation VoIP solution that for the first time truly leverages SIP and follows the standard. sipX is under heavy development and by now has closed the gap to both Asterisk and to much larger and more expensive systems. [67] The largest known production installation of sipX currently supports 5,000 users on a single High Availability (HA) system with a plan to grow. With the addition of high-availability sipX will have eliminated any single point of failures in the call control system and will therefore qualify as a production system for a mission critical application: voice."

Features:

- Full comprehensive support of all kinds of call services including call forward, call parking, call snooping, enhanced 911, music on hold, and call transfers
- Full support of all Time Division Multiplexing (TDM) protocols and SIP codecs
- Highly available, supports clustering and supporting remote offices
- Integrated administration and configuration interface
- Comprehensive feature list available at http://sipx-wiki.calivia.com/index.php/SipX_Features

3.7.7.1.5 Yate

Website: http://yate.null.ro/pmwiki/
Language: C++ with various scripting engines
Platform: Linux, Win32, others.
Activity: Last release 4/07
License: GNU Public License, with some Mozilla Public License

Summary: "Yate - Yet Another Telephony Engine is a next-generation telephony engine; while currently focused on Voice over Internet Protocol (VoIP) and PSTN, its power lies in its ability to be easily extended. Voice, video, data and instant messaging can all be unified under Yate's flexible routing engine, maximizing communications efficiency and minimizing infrastructure costs for businesses.

Yate can be used as a: VoIP server, VoIP client, VoIP to PSTN gateway, PC2Phone and Phone2PC gateway, H.323 gatekeeper, H.323 multiple endpoint server, H.323<->SIP Proxy, SIP session border controller, SIP router, SIP registration server, Jingle server, ISDN passive and active recorder, IAX server and/or client, IP Telephony server and/or client, Call center server, IVR engine, Prepaid and/or postpaid cards system." [68]

Features:

- Support for SIP, AIX2, H.323 and Jingle protocols
- Support for traditional digital telephony circuits, including hardware support for personal computer (PC) based telephony cards
- Includes various components used to build a PBX system

3.7.7.2 Open Source SIP Soft Phones

3.7.7.2.1 Ekiga

Website: http://www.ekiga.org
Language: C++
Platform: Unix/Linux, Win32
Activity: Last release 4/12/2007
License: GNU Public License
UI: Portable Windows Library (pwlib)
SIP Stack: Open Phone Abstraction Library (opal)

Summary: "Ekiga (formerly known as GnomeMeeting) is an open source VoIP and video conferencing application for GNOME. Ekiga uses both the H.323 and SIP protocols. It supports many audio and video codecs, and is interoperable with other SIP compliant software and also with Microsoft NetMeeting". [69]

Features:

- Supports both SIP and H.323 including all full range of codecs.
- Support both audio and video
- Ekiga support call transfer, call hold, and instant messaging.
- Comprehensive feature list available at http://www.ekiga.org/index.php?rub=2

3.7.7.2.2 KPhone

Website: http://sourceforge.net/projects/kphone
Language: C++
Platform: Unix/Linux
Activity: Last release 9/23/2006
License: GNU Public License
UI: X11
SIP Stack: Internal

Summary: "KPhone is a SIP UA for Linux, supporting a multitude of features. Originally developed by Billy Biggs, it was developed at Wirlab until 2005. It is now developed by a team of volunteers in this project" [70]

Features:

- Multiple parallel session (with audio, one may be active, the others are held),
- NAT-traversal and STUN support
- Secure Real-time Transport Protocol (SRTP) encryption for voice

3.7.7.2.3 Linphone

Website: http://www.linphone.org/index.php/eng
Language: C
Platform: Unix/Linux, limited functionality under Win32 and FreeBSD.
Activity: Last release 4/16/2007
License: GNU Public License
UI: X11
SIP Stack: GNU oSIP.

Summary: An open source SIP videophone for Linux and Windows

Features:

- Support for multiple codecs
- GUI and command line interface
- There is a separation between the core and UI

3.7.7.2.4 Minisip

Website: http://www.minisip.org
Language: C++
Platform: Linux, embedded Linux, Win32, Pocketpc Windows Mobile
Activity: Last release 3/1/2006
License: GNU Public License

UI: GTK+
SIP Stack: Internal

Summary: "Minisip is a SIP User Agent ("Internet telephone"). It can be used to make phone calls, instant message and videocalls to your buddies connected to the same SIP network." [71]

Features:

- Multiple lines (users) on the same phone, Multiple incoming/outgoing calls simultaneously
- Focus on security: TLS, end-to-end security, SRTP, MIKEY (DH, PSK, PKE)
- Instant Messaging, Video conferencing, Spatial audio, Push-to-Talk (P2T), Full Mesh audio conferencing
- Separation between the core and UI, Encryption

3.7.7.2.5 PhoneGaim

Website: http://www.phonegaim.com
Language: C++
Platform: Linux and Win32
Activity: Last release 3, 2005.
License: GNU Public License
UI: GTK+
SIP Stack: oSip

Summary: An all-in-one messenger (gaim) and SIP soft phone, built by the makers of Linspire.

Features:

- Built off the popular Gaim instant messenger client

3.7.7.2.6 PJSUA

Website: http://www.pjsip.org/pjsua.htm
Language: C
Platform: Win32
Activity: Last release 6/2007
License: GNU Public License
UI: Command Line
SIP Stack: PJSIP

Features:

- Concurrent calls and conferences
- SIP instant messaging

- Support for NAT traversal with rport and STUN
- Adaptive jitter buffer, adaptive silence detection, and packet lost concealment audio features.

3.7.7.2.7 SFLPhone

Website: http://sflphone.org
Language: C++
Platform: Linux
Activity: Last release 12/2006
License: GNU Public License
UI: Skinnable (ability to completely change look and feel of UI)
SIP Stack: oSip

Features:

- STUN support
- Supports multiple lines

3.7.7.2.8 Twinkle

Website: http://www.twinklephone.com
Language: C++
Platform: Linux
Activity: Last release 5/07
License: Lesser GNU Public License
UI: QT (Open Source Application/GUI Framework at http://www.trolltech.com/products/qt)
SIP Stack: Internal

Features:

- Supports multiple lines
- User scripting for call events
- Automatic failover to secondary server
- Simple address book functionality

3.7.7.2.9 WengoPhone NG

Website: http://www.openwengo.com
Language: C++
Platform: Linux, Win32, Mac OSX
Activity: Last release on 5/07
License: GNU Public License

UI: QT (Open Source Application/GUI Framework at http://www.trolltech.com/products/qt)
SIP Stack:oSip

Summary: WengoPhone NG is a rewrite of WengoPhone classic with the goals of being modular, extensible, and VoIP provider agnostic. Wengophone supports both classic VoIP SIP calls as well as numerous instant-messaging protocols.

Features:

- Fully SIP-compliant softphone with audio, video, and presence support
- Instant messaging features including support for Jabber/GoogleTalk, AIM/ICQ, MSN and Yahoo
- File transfer capabilities
- Encryption using SRTP with AES 128 bit standard encryption

3.7.7.2.10 wxCommunicator

Website: http://sourceforge.net/projects/wxcommunicator
Language: C++
Platform: Linux, Win32, and Mac OSX.
Activity: Last release 5/07
License: GNU Public License
UI: wxWidgets (cross-platform open source user interface platform at www.wxwidgets.org)
SIP Stack: sipXtapi

Features:

- Five simultaneous lines, conferencing, Multiple SIP profiles, with 1 active profile at time
- NAT traversal, STUN, TURN, ICE support
- Full conversation call or conference recording into wav file
- Automatic mute management that un-mutes microphone automatically on incoming call

3.7.7.2.11 Zap!

Website: http://www.croczilla.com/zap
Language: C++ and JavaScript
Platform: Linux, Win32, Mac OSX
Activity: Last release 7/06
License: Mozilla Public License
UI: XUL, Mozilla
SIP Stack: Internal

Summary: "Our goal is to produce an open-source, stand-alone, xulrunner-based SIP client using Mozilla as a platform" [72]

Features:

- Ability to run inside of Mozilla browser
- Supports NAT transversal

3.7.7.3 Open Source SIP Stacks

3.7.7.3.1 eXosip

Website: http://savannah.nongnu.org/projects/exosip
Language: C
Platform: Unix/Linux, Mac OS X
Activity: Last release 4/12/2007
License: GNU Public License (also available with commercial license)

Summary: "eXosip is a library that hides the complexity of using the SIP protocol for multimedia session establishment. This protocol is mainly to be used by VoIP telephony applications (endpoints or conference server) but might be also useful for any application that wishes to establish sessions like multiplayer games." [73]

Features:

- Designed to hide complexity of SIP transactions
- Fairly small footprint

3.7.7.3.2 JAIN-SIP JAVA SIP Stack

Website: http://jain-sip.dev.java.net/
Language: Java
Platform: Unix, Windows, and other support java environments
Activity: Last release 2006
License: Public domain

Summary: "Contains RI, TCK, examples, tools for JAIN-SIP-1.2 (JSR-32 maintenance release) and an SDP library that conforms to the public release of JSR 141 (JAIN-SDP) interfaces. JAIN-SIP RI is a full implementation of RFC 3261. JAIN-SDP interfaces are still under public review and are subject to change. Tools include a signaling trace viewer that can take input from an ethereal/stack trace. RI, TCK and tools are in the public domain." [74]

Features:

- Java code base allows applications to be platform-independent
- Wraps low-level SIP stack and protocols in a java interface layer
- Standardizes the interface to the stack, the events and event schematics, and the transaction schematics

3.7.7.3.3 OpenSipStack

Website: http://www.opensourcesip.org
Language: C
Platform: Unix, Win32
Activity: Last release 1/22/07
License: Mozilla Public License / GNU Public License / Lesser GNU Public License

Summary: "The OpenSIPStack Library is an implementation of the Session Initiation Protocol (SIP) as described in RFC 3261. The primary goal of the library is to provide application developers with a fully compliant interface to the SIP protocol with scalability and stability in mind. The OpenSIPStack Library has both low level interface and high level interface ideal for use in SIP Proxies, Presence Servers, Soft phones and Instant Messaging clients." [75]

Features:

- Fully Compliant Finite State Machines
- RTP Proxy, STUN, and ENUM support

3.7.7.3.4 oSIP

Website: http://www.gnu.org/software/osip/
Language: C
Platform: Unix/Linux, Mac OS X, Win32
Activity: Last release 11/2/2006
License: Lesser GNU Public License

Summary: "The GNU oSIP library is written in C and has no dependencies except the standard C library. oSIP is thread safe and will generally be used in a multi-threaded application. Nevertheless, this is optional. oSIP is little in size and code and thus could be use to implement IP soft-phone as well as embedded SIP software. oSIP is not limited to endpoint agents, and can also be used to implement "SIP proxy". oSIP does not intend to provide a high layer API for controlling "SIP Session" at this step. Instead, it currently provides an API for the SIP message parser, SDP message parser, and library to handle "SIP transactions" as defined by the SIP document." [76]

Features:

- Small footprint.
- Designed for a basic library in order to develop SIP client & gateway.
- Designed to be a low-level SIP message parser and transaction manager

3.7.7.3.5 Open Phone Abstraction Platform

Website: http://www.voxgratia.org/
Language: C++
Platform: Unix, Win32, others.
Activity: Last release 1/07
License: Mozilla Public License

Summary: "OPAL is the "next generation" of OpenH323 that has a new architecture. Not only does it support H.323 and SIP, but new VoIP protocols or devices can be added very easily. It is being actively developed and is used by several projects such as Ekiga (http://www.ekiga.org)" [77]

Features:

- Supports both SIP and H.323

3.7.7.3.6 PJSIP

Website: http://www.pjsip.org
Language: C
Platform: Unix, Linux, Win32
Activity: Last release 5/2007
License: GNU Public License

Summary: "The PJSIP.ORG website provides the Open Source, comprehensive, high performance, small footprint multimedia communication libraries written in C language for building embedded/non-embedded VoIP applications." [78]

Features:

- Extremely portable
- Very small footprint with high performance
- Extensive SIP features and SIP documentation

3.7.7.3.7 ReSIProcate

Website: http://www.resiprocate.org
Language: C++
Platform: Linux, Win32, Mac OSX, and others
Activity: Last release 3/07
License: Vovida Software License

Summary: "The ReSIProcate project consists of a stack and a collection of applications. The ReSIProcate stack is currently used in several commercial products and is considered very stable. ReSIProcate is ideally suited to individuals or companies that are implementing one of the

following SIP applications: Phones (for example, embedded), Softphones (any platform), Gateways, Proxies, B2BUAs, Instant Messaging/Presence Servers or Clients." [79]

Features:

- Full implementation of RFC 3261
- Support for NAT and ENUM.
- Comprehensive feature list available at http://www.resiprocate.org/ReSIProcate_Current_Features

3.7.7.3.8 Sofia-SIP

Website: http://sofia-sip.sourceforge.net
Language: C
Platform: Unix/Linux
Activity: Last release 4/2007
License: Lesser GNU Public License

Summary: "Sofia-SIP is an open-source SIP User-Agent library, compliant with the IETF RFC3261 specification (see the feature table). It can be used as a building block for SIP client software for uses such as VoIP, IM, and many other real-time and person-to-person communication services. The primary target platform for Sofia-SIP is GNU/Linux. Sofia-SIP is based on a SIP stack developed at the Nokia Research Center. " [80]

Features:

- Support for RFC 3261, as well as support for encrypted signaling using SSL/TLS
- Support for offer-answer negotiation via RFC 3264

NAT and STUN support response routing (RFC3581/rport) are supported as well

3.7.7.3.9 Yass

Website: http://yate.null.ro/pmwiki/index.php?n=Main.YASS
Language: C++
Platform: Linux, Win32, others
Activity: Last release 4/07
License: GNU Public License

Summary: The SIP stack that is released as part of the YATE project (see PBX section for details).

Features:

- Small and flexible

3.7.7.4 Various Other SIP Open Source Projects

3.7.7.4.1 OpenSBC

Website: http://www.opensourcesip.org
Language: C
Platform: Unix, Linux, and Win32
Activity: Latest release 1/22/07
License: Mozilla Public License

Summary: "OpenSBC is a reference implementation of a hybrid SIP proxy and B2BUA (back to back user agent) created from the OpenSIPStack core. It is well suited for a number of VoIP implementations. Among other things, it can be used as a Registrar for SIP endpoints, as an entry/egress point for SIP trunking applications, or as a far-end NAT traversal solution." [81]

Features:

- Integrated web UI for basic configuration tasks,
- Far-end NAT traversal with RTP proxy
- Complete transparency for end-nodes with support for pass-thru of non-standard SDPs
- Encryption of SIP and RTP packets with simple hash
- Support for SIP Privacy using RFC 3325.

3.7.7.4.2 Mobicents

Website: http://mobicents.dev.java.net/
Language: Java
Platform: Unix, Windows, and other support java environments
Activity: Last release July 1, 2006
License: GNU Public License

Summary: "Mobicents is a highly scalable event-driven application server with a robust component model and fault tolerant execution environment. Mobicents is the first and only Open Source Platform certified for JSLEE 1.0 compliance. It complements J2EE to enable convergence of voice, video and data in next generation intelligent applications. Web and SIP can be combined together to achieve more sophisticated and natural user experience." [82]

Features:

- Fully JSLEE 1.0 compliant
- Designed for high volume with low latency

- Enables the composition of Service Building Blocks
- Well documented

3.7.7.4.3 OpenSER

Website: http://www.openser.org
Language: C
Platform: Linux, FreeBSD, and others
Activity: Last release 4/07
License: GNU Public License

Summary: "OpenSER is a mature and flexible open source SIP server (RFC3261). It can be used on systems with limited resources as well as on carrier grade servers, scaling to up to thousands call setups per second. It is written in pure C for Unix/Linux-like systems with architecture specific optimizations to offer high performances. It is customizable, being able to feature as fast load balancer; SIP server flavors: registrar, location server, proxy server, redirect server; gateway to SMS/XMPP; or advanced VoIP application server. " [83] OpenSER is a fork of the SER project.

Features:

- Robust and small
- Full support of stateful and stateless proxying
- Comprehensive feature list available at http://www.openser.org/mos/view/Features/

3.7.7.4.4 SIP Express Router (SER)

Website: http://www.iptel.org/ser/
Language: C
Platform: Linux, FreeBSD, others
Activity: Last release 1/06
License: GNU Public License

Summary: is a high-performance, configurable, free SIP server licensed under the open-source GNU license. It can act as SIP (RFC 3261) registrar, proxy or redirect server. SER can be configured to serve specialized purposes such as load balancing or SIP front-end to application servers, SEMS for example." [84]

Features:

- Complete support of RFC 3261 functionality
- Supports a variety of database backends
- Network Address Translation (NAT) and Telephone Number Mapping (ENUM) support

3.7.8 Conclusions of the OSS Review

3.7.8.1 Benefits of Open Source

Open Source projects can provide a great boost in developing and delivering a commercial project to market. The typical instance of this is using a common open source library to provide core functionality, such as XML parsing, logging, and scripting. Another way of leveraging open source would be to use an open source project as the starting point for commercial project. Depending upon the open source license, the commercial project could work in co-operation with the open source projects, donating back certain bug fixes and features as a way of showing appreciation to the open source project.

3.7.8.2 Product Comparisons

3.7.8.2.1 Open Source PBXs

Both the SipX and Asterisk code base was well organized, well documented, and rich in PBX features. Asterisk seemed to have a greater user following, support for other VoIP protocols, as well as a more refined and polished user interface. SipX has a more efficient and distributed architecture, but was SIP only. SipX also is licensed under the less restrictive Lesser GNU Public license rather than Asterisk, which is licensed under the full GNU Public license. Since SipX was developed to be a SIP enterprise communication server rather than just a PBX replacement, it seems more suitable as a starting point for a Navy communication system.

3.7.8.2.2 Open Source SIP Stacks

Both oSIP and PJSIP both has broad Operating System (OS) support, along with tight, clean code. PJSIP stood out against oSip in the area of functionality. PSJIP provides a full SIP stack supporting many SIP and media Request for Comments (RFCs), while oSip provides low-level SIP/SDP parsing and state machine libraries. As well, PJSIP has excellent documentation, including benchmarks detailing it's performance. Given all these advantages, PJSIP seems more suitable as SIP stack for a Navy communication system.

3.7.8.2.3 Open Source Soft Phones

Both wxCommunicator and minisip had clean code, supported end-to-end security, and supported Windows and Linux. From their, they differed greatly in implementation. Minisip has a very minimal interface, and would not run at all on Windows, and crashed when trying to place a call on Linux. wxCommunicator had a much nicer, more refined interface, and was easy to setup and place a call on Windows. As well, it used the SipX SIP stack, providing it the capability of 5 SIP lines with conferencing. The only capability it didn't provide was a mobile version. Given this, wxCommunicator seems more suitable as a starting point for a Navy communication system phone.

3.7.9 Overall Project Summary

Based on the review of the projects in this paper, the following generalizations can be concluded:

- Care has been taken by the project owners to carefully organize the source for the projects into a logical layout.
- All the source and header files contain adequate to excellent comments to assist in documenting the code.
- All the projects had a mechanism for returning errors and for tracing using logging. Many of the projects contained test harnesses to verify implementation.
- Standards based specifications ease in the selecting, coding, and testing of features in open source SIP projects.
- Prolific deployments of Asterisk and SipX, including a 5000 seat deployment of SipX by Amazon.com

Given that all the code was relative high quality, it would seem reasonable that one could take the recommended open source project as a starting point for commercial product.

This page intentionally left blank.

3.8 *Announcing System*

The Central Amplifier Announcing System (CAAS) is a single device used on naval vessels to house the distribution amplifiers used to distribute voice and alarm announcements to the loudspeaker groups. Table 3-10 provides a Derived baseline for the Amplifier Announcing system. The baseline lists the functions and capabilities of the Amplifier Rack by functional subheadings that relate to the VoIP implementation.

Table 3-10. CAAS Amplifier Derived Baseline

Announcement Compatibility	**Current Implementation**	**VoIP Implementation**
Provides Announcing System (AS) Controller and Distribution Amplifier Activation Signaling Compatibility	Amplifiers are connected to remote speakers by a cable system. A number of speakers connected to a single cable run.	The IP packet based system connected via Ethernet infrastructure to an amplifier imbedded in each speaker.
General Operation	**Current Implementation**	**VoIP Implementation**
Activated by the AS Controller During Voice Announcements and Alarms	Announcement System Controller with amplifiers connected through the relay based system to activate selected speakers	IP based announcement configuration will be stored in a PC or small IP based appliance.
Uses Multi-Channel Distribution Amplifiers for One AS Circuit Only	Multi-channel amplifiers tied to relays will operate selected string of speakers based on operational parameters	Each speaker will have an imbedded amplifier that will be connected by POE (Power over Ethernet) cable or vessel power for higher output level speakers.
Provides the Greater of 15 Percent Spare Output Channels Minimum or One Spare Output Channel for Each AS Circuit	Current implementation can comply limited by the power of the amplifier.	Unlimited number of speakers tied to low cost switch ports, which are easily expandable depending on system requirements.
Uses COTS Components with Commercial Standards and Protocols	All component are COTS product with unique relay circuits for interfacing from amplifiers to speakers based on configurations of speakers being activated	Speakers are COTS and control servers based on functionality are in development to become COTS in the near future by several companies.

General Operation	Current Implementation	VoIP Implementation
Sends Voice Announcements and Alarms to Loudspeaker Groups Using Distribution Amplifiers	System has multiple hardened racks for availability and redundancy housing multiple amplifiers	The IP Network is a distributed redundant system from central hardened switches.
Provides Two Output Channels for Loudspeaker Dispersion Minimum	Multiple racks with multiple amplifiers that contain multiple channels.	IP Network is a distributed system from central switches with amplifiers in each individual speaker housing.
Diagnostic Operation	**Current Implementation**	**VoIP Implementation**
Provides AS Controller Remote Fault Detection By Signaling Secure or Failed Amplifier Power or Failed Amplifier Output	Relay based system uses contacts to signal issues with the system.	Network management tool can check end devices and provide fault detection and feed back.
Unit Structure	**Current Implementation**	**VoIP Implementation**
Provides Shipboard Compatible Standard 19-Inch Rack Mount Components	Comply	Comply
Resides with Associated AS Controller	Located in announcement rack	Can be located in any standard rack with both a size and weight savings for deployment

3.8.1 CAAS Controller

The CAAS Controller is a single device used on naval vessels for selecting received audio from microphone stations and for interfacing and distributing the audio to loudspeaker group distribution amplifiers. The CAAS controller unit consists of redundant processing units and alarm tone generators. The following Table 3-11 provides a derived baseline for the CAAS Controller. The baseline lists the functions and capabilities by functional subheadings that relate to the VoIP implementation.

Table 3-11. CAAS Controller Derived Baseline

Announcement Communication	**Current Implementation**	**VoIP Implementation**
Preempts Lower Priority Microphone Station Voice Announcements when a Higher Priority Microphone Station Generates a Voice Announcement.	Done with controller and relay logic	Part of paging server implementation with multiple speakers tied to multiple groups each having set priority.
Overrides Voice Announcements with an Alarm Regardless of the Priority of the Microphone Station Generating the Voice Announcement.	Done with controller and relay logic	This feature of priority and the playback of pre-recorded files will need to be added to the COTS product. Maybe able to be done with the group priority.
Does Not Interrupt Voice Announcements from an Active Microphone Station with an Equal or Lower Priority Microphone Station Voice Announcement	Done with controller and relay logic	Part of priority scheme of paging group definitions
Diagnostic Compatibility	**Current Implementation**	**VoIP Implementation**
Provides Remote Alarm Monitoring Compatible with IC/SM Type Alarm Switchboards	Currently relay based	A network management application can be utilized to monitor and switch a hard contact for alarms
General Connection	**Current Implementation**	**VoIP Implementation**
Connects to a Remote Human Machine Interface (HMI)	The display is independent of the underlying telephony implementation.	The display is independent of the underlying telephony implementation.
Unit Display	**Current Implementation**	**VoIP Implementation**
Provides Audible and Visible Failure Alarm Indication at the Controller and HMI	The display is independent of the underlying telephony implementation.	The display is independent of the underlying telephony implementation.

General Operation	Current Implementation	VoIP Implementation
Uses Commercial and Industry Standard Programmable Controllers	Multiple vendors used	Different vendors house their controller within dedicated COTS appliance or server unit.
Uses Unmodified Licensed and Registered System and HMI Software	Controller has firmware and also uses custom configurations.	Servers and speakers have firmware and also require web-based configurations.
Does Not Use Communication System Unique Software	COTS controller with custom configuration	COTS server or SIP based server with custom configuration.
Does Not Impact Voice Announcements or Alarms Upon Transient Loss of Ship's Vital 115 VAC Power or when Switching between Ship's Vital 115 VAC Power and the UPS	UPS required for Announcing rack of equipment	UPS required for the different components of distributed system, telephony system, POE switches and high power speakers
Announcement Operation	**Current Implementation**	**VoIP Implementation**
Activates Distribution Amplifiers Upon Microphone Station, Interface PTT, or Alarm Input	Controller and relay	Extensions off of the IP based telephony switch.
Assigns Microphone Station Priority	Controller and relay	Priority scheme for alarm group, by extension dialed to activate.
Assigns Alarm Priority	Controller and relay	Priority scheme for alarm group, by extension dialed to activate
Audio Operation	**Current Implementation**	**VoIP Implementation**
Distributes Microphone Station and Interface Audio to AS Amplifiers	Through relay and controller	Through telephony switch and page server.
Selects and Distributes AS Microphone Station or Interface Input Voice Announcements to Specific Loudspeaker Group Amplifiers or Interfaces Applicable to the Specific AS Circuit	Through relay and controller	Telephony switch, microphone station, alarm actuator become telephony end devices.

Audio Operation	**Current Implementation**	**VoIP Implementation**
Uses a Commercial Processing Element Controlling Loudspeaker Group Distribution and Configuring and Prioritizing Microphone Station and Alarm Broadcasts	Through relay and controller	Telephony switch, microphone station, alarm actuator become telephony end devices.
Provides Circuitry to Produce and Distribute Alarm Tones to Supported Amplifiers According to Frequency and Activation Characteristics	Play pre-recorded alarm files from dedicated hardware	Play pre-recorded alarm files. Design maybe from dedicated hardware or from the IP-PBX or Voice Mail system.
Broadcasts Applicable AS Circuit Alarms to All Applicable AS Circuit Loudspeaker Groups and Interfaces	Implemented by Controller program	Implemented by priority scheme in speaker/alarm group
Automatically Mutes or Cuts out the Loudspeaker Located in 1MC Microphone Station Areas when the Associated Microphone Station Generates a Voice Announcement	Implemented by controller and relay logic within the amplifier system	Implemented by priority scheme in speaker/alarm group
Controls Two Isolated Audio Circuits Minimum	Amplifiers has multiple channels	Each speaker contains an individual amplifier, and the pager server unit controls them over the IP network.
Diagnostic Operation	**Current Implementation**	**VoIP Implementation**
Provides That the HMI Monitor Processing Element, Alarm Tone Generator, UPS, and Amplifier Failures are monitored	Done with relays	Watch dog feature and use of ping or network monitoring system.
Provides Component Failure Status to the HMI for Modular Level Fault Isolation	Done with relays	Only failed device is affected since system is distributed and redundant.

Reliable Operation	**Current Implementation**	**VoIP Implementation**
Provides Redundant Processing Units and Alarm Tone Generators for Survivability	System is Redundant	Telephone redundancy in IP-PBX as well as having multiple page servers using DNS.
Provides Redundant Processing Elements Automatically Switch to the Off-Line Processing Element when the On-Line Processing Element Fails	Done with relays	DNS or cluster server handles switch over, automatically between hot systems.
Storage Operation	**Current Implementation**	**VoIP Implementation**
Externally Stores System Configuration, Loudspeaker Group Configuration, Microphone Station Priority, and Alarm Priority for System Restoration after Controller Failure	Dependant on technology implemented	Speakers on boot get configured from the configuration server.
Primary Power	**Current Implementation**	**VoIP Implementation**
Receives Power from Ship's Vital 115 VAC Power Panels	Rack does	Telephony equipment and most speakers powered by POE, depending on the output level of the speaker.
Provides Circuit Breaker Protection for Each AS Circuit	Part of rack	PoE should be handled at the switch and the switch will need to have circuit breakers in the enclosure.
Secondary Power	**Current Implementation**	**VoIP Implementation**
Provides an Internal UPS That Provides 15 Minutes Uninterrupted Power Minimum for Graceful Controller Shutdown Upon Complete Loss of Input Power from Ship's Vital 115 VAC Power	Part of rack	Distributed system rack, graceful UPS, Network switch UPS,

Unit Structure	Current Implementation	VoIP Implementation
Uses Shipboard Compatible Standard 19-Inch Rack Mount COTS Components	System 19-inch rack based	System 19-inch rack based for the IP-PBX and the page server.

3.8.2 CAAS Loudspeaker

The Loudspeaker is a single device used on naval vessels for output of voice announcements and alarms. The type of loudspeaker varies depending on the area where it is used (see Table 3-12). Table 3-13 provides a derived baseline for the Loudspeaker. The baseline lists the functions and capabilities of the CAAS Loudspeaker by functional subheadings that relate to the VoIP implementation.

Table 3-12. Loudspeaker Type

Loudspeaker Type	Shipboard Area	Specification
Low Power Fixed	Low Noise Level Compartments or Spaces	CID A-A0590002/1 MIL-L-24223 (Type IC/SAA or Equivalent)
Low Power Adjustable	Unexposed Work Spaces Subject to Large Volumes of Background Noise	CID A-A0590002/1 MIL-L-24223 (Type IC/SAG or Equivalent)
High Power Fixed	High Noise Level Compartments or Spaces	CID A-A0590002/2 MIL-L-24223 (Type IC/SBA or Equivalent)
High Power Adjustable	Exposed Work Spaces Subject to Large Volumes of Background Noise	CID A-A0590002/2 MIL-L-24223 (Type IC/SBG or Equivalent)
Super High Power	Flight Deck and Superstructure Spaces	Type IC/SGI or Equivalent
Explosion Proof	Spaces Subject to Explosive Conditions	UL 1203 (LS-588/U or Equivalent)

Table 3-13. Loudspeaker Derived Baseline

Audio Interface	**Current Implementation**	**VoIP Implementation**
Provides a Signal Line Buffer Audio Amplifier to Prevent the Loudspeaker and Output Wiring from Acting as a Microphone in Special Intelligence (SI) Areas	Designed in as part of current design for required speakers.	IP packet system does not transfer audio out of speaker. This is not an issue with IP based devices.
General Operation	**Current Implementation**	**VoIP Implementation**
During 1MC Alarms Activates Clearly Visible MIL-F-16377/26 Red Strobe Lights in Machinery Areas where the Ambient Noise Level Exceeds 90 dB	Designed in as part of current design, from the announcing rack to the location of the light.	Currently this feature is not implemented and would need to be in a future release. The proposed design with a manufacturer was to place the relay on the amplifier card in the speaker housing.
Audio Operation	**Current Implementation**	**VoIP Implementation**
Provides Automatic Loudspeaker Level Control in High Noise Areas (Except Propulsion Plant Areas)	Current system has microphones in area to adjust power output through the use of COTs hardware	Currently this feature is not implemented and would need to be in a future version of speaker. A manufacturer proposed design would add the circuitry to the amplifier card located in the speaker housing. This would reduce cabling and wiring.
Unit Structure	**Current Implementation**	**VoIP Implementation**
Watertight and Spray Tight on the Weather Deck and in Weather Exposed Areas	Currently implemented	Current COTs designs are not compliant.

3.8.3 Microphone Station

The Microphone Station is a single device used on some naval vessels for voice announcements and alarms. Detachable microphones with Push-to-Talk (PTT) switches and Alarm Activation Panels (AAP) are used when necessary. The Microphone Station has Single Action Activation switches to select loudspeaker groups and AAP alarms. It displays the loudspeaker group selection status, microphone signal level, and AS circuit activity.
The following Table 3-14 provides a derived baseline for the Microphone Station. The baseline lists the functions and capabilities of the Microphone Station by functional subheadings that relate to the VoIP implementation.

Table 3-14. Microphone Station Derived Baseline

Announcement Communication	**Current Implementation**	**VoIP Implementation**
Used for Voice Announcements	Current implementation complies	Implemented as an extension with special features. Special features may have to be implemented though a different protocol like SOAP.
Unit Display	**Current Implementation**	**VoIP Implementation**
Displays Microphone Signal Level During Voice Announcements	Part of current custom software implementation	IP implementation will need to be evaluated.
Displays Loudspeaker Group Selection Status for Voice Announcements	Part of current custom software implementation	IP implementation will need to be evaluated.
Displays AS Circuit Activity Visible on Applicable Microphone Stations for Voice Announcements or Alarms	Part of current custom software implementation	IP implementation will need to be evaluated.
Audio Interface	**Current Implementation**	**VoIP Implementation**
Uses a Detachable Microphone with an Internal PTT Switch for Voice Announcements	In current design	Part of system design; is independent of the IP design
User Interface	**Current Implementation**	**VoIP Implementation**
Provides Single Action Activation Switches Visible During All Lighting Conditions for AAP Alarm Generation	Incorporated in custom design	Part of system design; is independent of the IP design
Provides Single Action Activation Switches Selecting Loudspeaker Groups for Voice Announcements	Incorporated in custom design	Incorporated in design; use of speed dials may be solution.

Audio Operation	Current Implementation	VoIP Implementation
Generates Voice Announcements at Selected Loudspeaker Groups	Incorporated in custom design	Incorporated in design; use of speed dials maybe solution.
Generates Alarms at Designated Microphone Stations Using an AAP	Incorporated in custom design	Incorporated in design; use of speed dials may be solution.

3.8.4 CAAS Sub-Group Loudspeaker Cutout and Test Panel Rack

The Sub-Group Loudspeaker Cutout and Test Panel Rack is a single device used on naval vessels for manually isolating loudspeaker strings in the event of loudspeaker string damage or for inspection, maintenance or testing of loudspeaker strings. It has cutout switches for connecting and disconnecting loudspeaker strings to/from the distribution amplifiers and test points for testing loudspeaker strings. The following Table 3-15 provides a derived baseline for the Loudspeaker Cutout and Test Panel Rack. The baseline lists the functions and capabilities of the CAAS Sub-Group Loudspeaker Cutout and Test Panel by functional subheadings that relate to the VoIP implementation.

Table 3-15. Sub-Group Loudspeaker Cutout and Test Panel Rack Derived Baseline

Audio Connection	Current Implementation	VoIP Implementation
Connects Multiple Loudspeakers in Parallel to a Common Sub-Group Audio Pair	Compliant per current design	IP based speakers connect back to the Ethernet switch and monitored by network Management.
Test Connection	**Current Implementation**	**VoIP Implementation**
Provides Test Points Compatible with Standard Test Equipment Probes	Compliant per current design	IP based speakers connect back to the Ethernet switch and monitored by network Management.
General Operation	**Current Implementation**	**VoIP Implementation**
Manually Isolates Sub-Group Loudspeaker Strings when Loudspeaker Damage Occurs or for Loudspeaker Inspection and Maintenance	In current design	IP Network Management tools would be used to implement this, but each speaker is independent of each other.

General Operation	Current Implementation	VoIP Implementation
Manually Connects or Disconnects Sub-Group Loudspeaker Strings to/from Distribution Amplifiers for Loudspeaker Load Testing and Electrical Checks	In current design	IP Network Management tools would be used to implement this. This can be done at the switch since each is a single unit.
Provides 15 Loudspeakers per Sub-Group String Maximum	In current design	Can support with no limit on number of speakers, the use of multi-cast allows this.
Provides the Greater of 15 Percent Spare Cutout Switches Minimum or One Spare Cutout Switch for Each AS Circuit	In current design	Can support with no limit on number of speakers. The number of PoE ports on the switches is the limiting factor.
Does Not Exceed 85 Percent of Amplifier Capacity for Amplifier Loading	In current design	Each speaker will have own amplifier so no constraint
Unit Structure	**Current Implementation**	**VoIP Implementation**
Shipboard Compatible Standard 19-Inch Rack Mountable in the Same Cabinet as the Supported AS Circuit Distribution Amplifiers	Per current design	All system components would be mounted within 19-inch rack. Some items with small form factors would be on a shelf. Amplifiers are located in each speaker.

This page intentionally left blank.

3.9 Mobile Communications

3.9.1 Introduction

The following section examines Commercial off the Shelf (COTS) Wireless Technologies available today for supporting mobile communication onboard a naval vessel. The technologies examined include: Wireless Fidelity (WiFi/802.11), Worldwide Interoperability for Microwave Access (WiMAX/802.11), and Cellular. All of these technologies support or are expected to support both voice and data in the near future.

Before discussing these mobile communication solutions, some background information on wireless communication in general is presented.

First, known issues or impairments that wireless technologies must be able to overcome are discussed. These issues, which exist in all wireless environments, can be even more pronounced onboard a navy ship. A mobile solution that may be acceptable in one location onboard may not be appropriate or even work in another location. The use of wireless communications in different areas of a ship as well as the types of communication a naval vessel will be expected to support are examined.

Next, the basic techniques that allow today's commercial wireless systems to support multiple users are discussed. The coding and modulation techniques developed to support these systems are defined, along with each technique's ability to tolerate the impairments facing wireless communication.

Following this background information, each of the three COTS Wireless Technologies is described. Remaining issues and concerns surrounding security, interference, and Quality of Service (QoS) of COTS wireless equipment are also discussed. Finally, the benefits and disadvantages of each of the three wireless technologies are discussed.

3.9.2 RF-Challenged Environments

Several impairments make high-speed wireless communications challenging in any environment. To varying degrees, all of the impairments in Table 3-16 are present onboard a ship. As detailed later, some impairments are very pronounced on ship. Fortunately, COTS products need to deal with the same set of impairments in other environments (e.g., urban, office, residential).

Table 3-16. Summary of Wireless Communication Impairments

Challenge	Description
Rayleigh Fading	Variations in signal strength as a receiver moves through space, including "deep nulls" due to summing of multipath interference
Delay Spread	Inter-symbol interference due to propagation delay of multipath interference
Doppler Spread	Relative motion of sender and receiver resulting in perceived shift in frequency
Attenuation	Decrease in signal strength over distances and when passing through objects (e.g., drywall)
External Interference	Various EMI sources (e.g., generators, radar)
Co-channel Interference	Interference from nearby devices using the same protocol
Slow Fading	Variations in signal strength as the receiver moves through space due to shadows caused by objects in the signal's path

Multipath interference is a key concern for wireless systems, especially within a ship. Obstructions, such as concrete and glass buildings, terrain, and metal walls, reflect EM waves. Precisely how much of the energy is reflected is a complex function depending on the properties of the material and the frequency. For microwave frequencies (roughly 300MHz to 30GHz), metals (such as steel) reflect nearly all of the energy. Multiple copies of the original signal (following different paths) recombine at the receiver. Because the lengths of the paths vary, each signal is received some short delay after the first one.

In one experiment, measurements taken inside a large steel structure contained significant noise from waves that reflected off of up to six surfaces. The value of six surfaces was calculated by dividing the measured delay spread by the longest dimension of the aircraft hanger where the test was performed. In addition to the number of reflections measured, analysis of the results also showed the presence of scattering. *Scattering* is a process where the energy bounces at a diffuse set of angles, instead of the angle of the expected reflection (e.g., like an image in a steamy mirror). Interference from scattered reflections causes problems for the receiver.

The following simple mathematical principles help to understand how multipath affects wireless signals. Wireless signals are transmitted as one or more sinusoidal waves. Mathematically, the sum of two sine waves at the same frequency is another sine wave with new amplitude and phase. This statement holds even when the amplitudes of the sine waves are different (as would be the case for a primary wave and a weakened and delayed reflection). The amplitude of the resulting sine wave may be larger (constructive) or smaller (destructive) than either of the original sine waves, depending on the relative phases of the waves. If the two waves are equal in amplitude and 180° out of phase, they cancel each other out entirely, such that no information can be transmitted.

3.9.2.1 Rayleigh Fading

As mentioned above, multipath interference can be constructive or destructive depending on the relative phase of the signals arriving at the receiver. In typical environments, one finds several reflected paths at different amplitudes (amplitude and signal strength are equivalent). The phases of each path are usually independent, such that they tend to cancel each other out (according to the Central Limit Theorem). Nonetheless, there will be regions in space where the interference is constructive (i.e., where a majority of paths are in phase with the strongest signal) and other regions where the interference is destructive. The effect is known as *Rayleigh fading* because the *Raleigh distribution* (also known as a *Weibull* distribution) approximates the distribution of the signal strengths over space.[2]

The distance between these regions depends on the wavelength of the signal. Consider a simple system with a transmitter, receiver, and a wall in a line. If the receiver moves a quarter of a wavelength (0.25λ)[3] toward or away from the wall, the distance the reflection travels changes by 0.5λ (0.25λ out plus 0.25λ back). This could be the difference between the reflection doubling the received signal and completely canceling it. At 2.4GHz, 0.25λ is just 3.125 cm. Thus, very small changes in path length may make a considerable difference in how the signals combine (constructively or destructively). In three dimensional space and with multiple paths, Rayleigh fading results in variations of signal strength across space. Regions where the signal is very weak may be as small as 0.25λ along some dimension.

Figure 3-34 shows a classic example of Raleigh fading along a straight line. The plot was generated using a simulation of six random reflections of a 1.5 GHz signal (20cm wavelength) with random phases (delays), amplitudes, and bearings (i.e., angles of arrival). The plot shows the signal strength in decibels (dB)[4] as a function of position along a straight line that is 1m (or 5λ) long. Without multipath, a single signal would have a constant power over all positions, as shown by the green line. The characteristic mark of Raleigh fading is the area of "deep nulls," where the power dips very low (below -30dB in this example) for a short distance. Also note that there are regions where multipath results in a signal that is stronger than the single-wave case.

---

[2] Rician fading is similar to Rayleigh fading, but assumes that the primary signal is stronger than the reflected signals. Rician fading more accurately describes the case where the primary signal is present. For the purposes of this study, the distinction is unimportant.

[3] Lambda (λ) traditionally designates wavelength.

[4] A quantity X (typically power or signal strength) expressed in decibels is defined as $10\log_{10}(X/X_0)$, where X_0 is some reference unit to which X is being compared. In some cases, the reference unit is specified after the dB label. For example, dBW indicates the reference unit is 1 watt and dBm indicates the reference unit is 1 milliwatt. When comparing relative powers, isotropic decibels are often used. For example, a +6dBi antenna boosts the signal strength four-fold. In other cases, the reference unit is unimportant and dB appears without another further specifier.

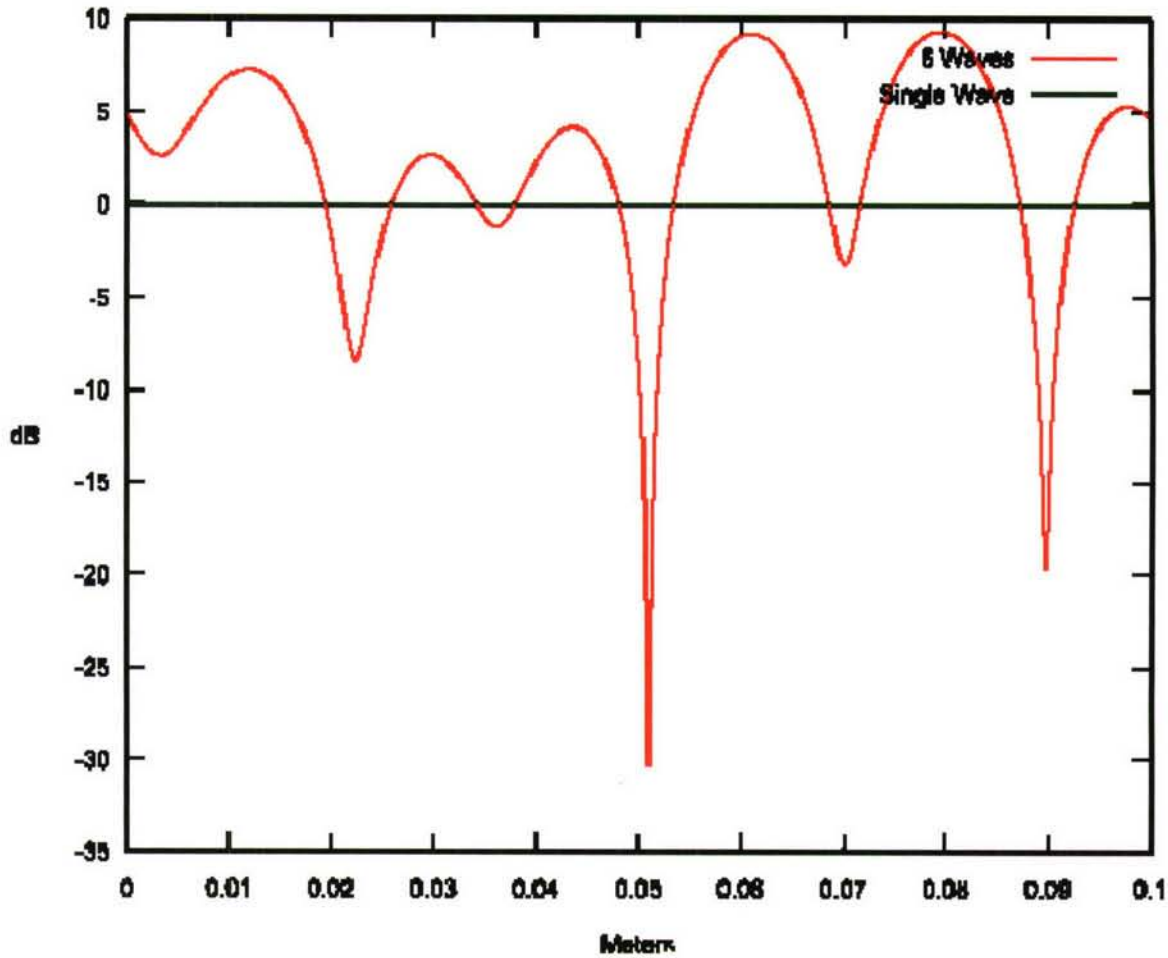


Figure 3- 34. Example Rayleigh Fading Pattern

In areas with strong multipath interference, this type of fading can result in small areas with very poor reception, even when the receiver is close to the transmitter. Most wireless systems are able to compensate for deep nulls. One approach is to use multiple antennas that spans distances greater than 0.25λ. Another is to spread the power spectrum of the signal over a range of frequencies. At a given location, a deep null may exist over part of the frequency range, but not the entire range.

The frequency band (e.g., 700 MHz vs. 2.4 GHz) makes little difference in how well a system overcomes Rayleigh fading. Although the wavelengths are different (along with the spacing between nulls) the impacts to the system are similar.

3.9.2.2 Delay Spread

Wireless systems transmit information as a sequence of symbols over time. Each symbol represents one or more data bits (i.e., the modulator converts some set number of data bits to form a symbol). The symbol period (i.e., the reciprocal of the symbol rate) must be long enough for the receiver to extract the information from the signal (or *demodulate* the signal). The symbol rate is directly proportional to the data rate because each symbol represents a fixed number of data bits.

Rayleigh fading, as described above, takes affect within a single symbol period due to delayed versions of the same signal. Inter-symbol interference, on the other hand, may occur when delayed versions of *different* signals overlap.

Delay spread is the time between when the receiver observes the first signal and when it observes the last "significant"[5] reflected signal. If the delay spread is large compared to the symbol rate, the spread causes inter-symbol interference that can be highly destructive. Empirical results have shown that a delay spread interfering with just 10% of the symbol period can make the signal unusable. Thus, delay spread is a limiting factor in the symbol rate, and hence the data rate.

Many protocols include a gap, called a *guard interval*, between symbols where the transmitter is silent. This reduces the impact of the delay spread when the delay is small because interference during the gap can be ignored safely. More specifically, the receiver does not attempt to process the received signal during the guard interval, and because no signal is sent during this gap, delayed versions of the guard interval do not interfere with the next symbol. Channel equalization, described later in this document, offers a potential countermeasure against delay spread.

Figure 3-35 and Figure 3-36 illustrate the effect of delay spread. Both figures show a sequence of symbols (in blue), a delayed version of the signal (in red), and the combination of the signals at the receiver. The signal is high when sending information and low during the guard interval. The length of the arrows on the left indicate the amount of delay for the signal. The original uses a guard interval where no signal is transmitted. Because there is no signal energy in the guard interval (neither the original signal nor the delayed one), the delayed signal's guard interval does not interfere with the next symbol. As shown in Figure 3-36, the delayed signal does not interfere with the original one.

In Figure 3-36, the second signal has a longer delay than the one in Figure 3-35. The delay is large enough that the delayed signal overlaps the next symbol from the original signal causing inter-symbol interference.

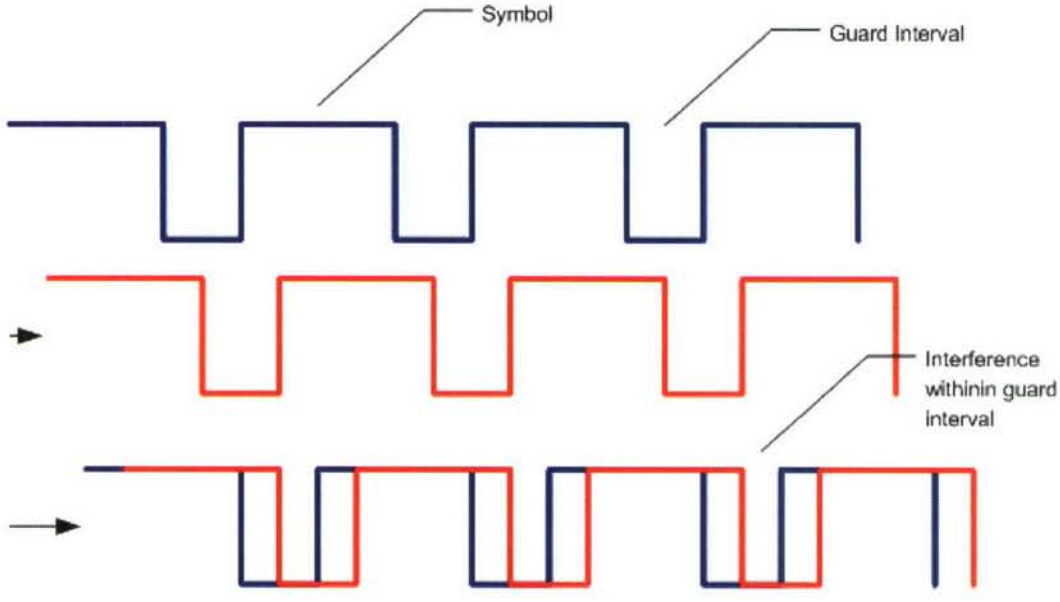


Figure 3-35. No Inter-Symbol Interference with Small Delay Spread

[5] *Significant* is loosely defined so that one can ignore very weak, late reflections that are indistinguishable from background noise.

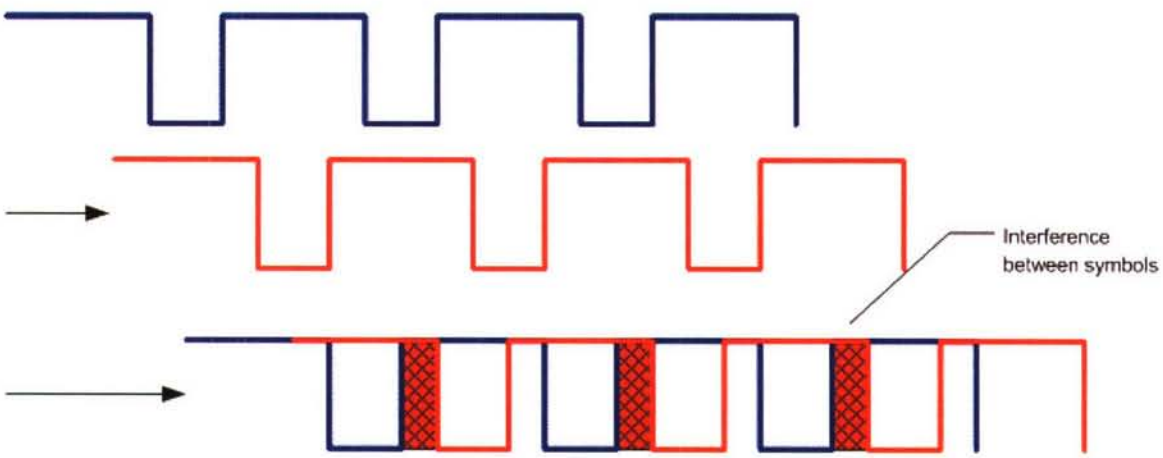


Figure 3-36. Inter-Symbol Interference with Large Delay Spread

3.9.2.3 Doppler Shift

Most people are familiar with the sound of a siren on a passing vehicle. As the vehicle moves away, the siren's pitch decreases. The change in pitch between the transmitted and received frequencies is known as the *Doppler Shift*. The same phenomenon occurs in wireless communications. For EM waves, the change in frequency can be expressed as $\Delta f = -f_0 v/c = -v/\lambda_0$, where Δf is the change in frequency, f_0 is the transmitted frequency, v is the relative velocity of the receiver with respect to the sender, c is the speed of light (approximately 300,000km/s), and λ_0 is the transmitted wavelength. For 2.4GHz, the frequency shift due to a vehicle moving at 100km/hr (or 27.8 m/s) is 222Hz.

Doppler shift reduces the signal level at the receiver because the power spectrum's peak moves away from the frequency that the receiver is tuned for. More importantly, if the spacing between different channels is small relative to the Doppler shift, signals in nearby frequency bands may interfere with one another.

3.9.2.4 Attenuation

Attenuation is a general term for a signal losing strength between transmitter and receiver. Distance between transmitter and receiver is one source of attenuation, called *path loss*. Interaction with objects is another source.

Signal strength can be expressed as energy per unit area. Unobstructed waves expand radially in space, while conserving the total energy, E. Thus the ratio of signal strengths at two distances r_1 and r_2 is $(E/4\pi r_2^2)/(E/4\pi r_1^2) = r_1^2/\, r_2^2$. In other words, the path loss is proportional to the distance squared. That is, if the signal loses half its strength at 100m, it will lose 75% at 200m.

Note that path loss as described above only applies in free space. In a closed environment, such as a metal room, the energy is contained within the volume of the room. Thus, one should not expect to see appreciable path loss in the interior of a ship.

Attenuation also occurs as waves pass through materials, such as walls. In the case of steel, nearly all the signal is reflected (or absorbed). Artifacts in the steel wall (joints, door frames, etc.) may act as weak antennas and transfer some of the wave into adjacent rooms.

Some materials, such as metals and water, attenuate signals at all microwave frequencies. Other materials, such as foliage, block high-frequency waves, but allow low-frequency waves (e.g., 700 MHz) to pass. Such frequency-dependent issues do not appear to be a concern for this study.

3.9.2.5 External Interference

Several external sources can produce Electro-Magnetic Interference (EMI) that affects wireless signals. For example, microwave ovens operate near 2.4GHz, which has caused problems for residential Wireless Local Area Networks (WLANs). Power systems (e.g., generators and transmission cables) emit EMI over broad frequency ranges. Other systems that are common on a ship (e.g., radar and long-range communication systems) may contribute to EMI.

In general, these external sources of interference appear as white noise, which is uncorrelated with the signals. Although the interference does degrade the signal quality, systems are designed to accommodate a certain level of background noise.

3.9.2.6 Co-channel Interference

Different networks using the same protocol often interfere with each other. This is known as *co-channel interference*. How one provides multiple instances of wireless networks in close proximity to each other is a fundamental issue for cellular system architects. Unlike random interference (e.g., from a microwave oven), interference from nearby channels using the same protocol (frequency, modulation schemes, etc.) cannot be averaged out to isolate the desired signal.

Cellular networks require sophisticated engineering to plan the location and transmit power of each antenna to manage co-channel interference. On a ship, however, the insulating properties of the metal walls help reduce co-channel interference.

3.9.2.7 Slow Fading

Wireless signals are also affected by fading patterns that vary slowly over distance. For example, as a mobile user passes a mountain or large building, the signal or a strong reflection may disappear (or reappear). This impairment is less important within this study because

Rayleigh fading will dominate it and most protocols handle slow fading well.

3.9.3 Shipboard Wireless Usage

A shipboard environment poses several challenges for wireless communications. In particular, the ship's metal infrastructure interacts with wireless signals and certain sub-systems may contribute to background Radio Frequency (RF) emissions that may interfere with the signals.

Similar impairments are found in traditional environments (e.g., commercial office space, urban areas), albeit to a lesser extent. To overcome impairments in such environments, engineers have proposed various coding and modulation techniques. The techniques offer tradeoffs between performance (data rate) and the ability to operate in harsh environments.

The characteristics of the wireless environment aboard a ship change based on location and usage. Table 3-17 shows how the issues vary with location.

Table 3-17. Areas of Ship with Wireless Challenges

Location	Issues	Comments
Interior (Large Room)	Large spaces result in echoes with long delays	e.g., hanger
Interior (Small Room)	Signals attenuate between rooms	e.g., crew cabin
Deck	Large area; interference from other communication devices and radar	

Location	Issues	Comments
Ship-to-ship/shore	Generally "wireless-friendly," but may be long distance; ship may be moving	
Interior (Noise Source)	Power systems leak RF emissions	Most techniques tolerate "white noise"

Wireless communication systems onboard vessels must deal with several challenges. The significance of these challenges varies with the usage and location of the communications. This section identifies challenges that apply to mission areas around the ship.

3.9.4 Internal to Navy Vessel

Most general-purpose voice and data communications occur within the interior of the vessel. We can model the interior of the vessel as a set of metal rooms of varying sizes (ranging from hangers on a carrier to tight cabins).

Metal walls reflect or absorb most of the energy at wireless communication frequencies, such that only a small portion of the energy propagates between adjacent rooms. One approach to address the attenuation is to use a large number of access points, relative to the number required for a typical office environment. Another potential approach is to use distributed antennas.

Multipath reflection is a significant issue in large rooms because reflections off metal walls contribute to very large delay spreads. In outdoor or typical office/residential environments, signal strength drops due to path loss (with the square of the distance) or attenuation (as the signal interacts with building materials, such as walls). Within a vessel, the metal building materials trap the signal inside the room causing

(a) Long delay spreads and

(b) Scattering, which reduces the effectiveness of equalization mechanisms such as rake filters.

In small rooms, the total delay spread may be small enough that its effect can be tolerated. As stated in Section 3.9.2 six significant reflections in a metal room may be typical. Consider the *worst-case* delay from a 5m×5m×3m room. Even if the signal bounces off walls six times along the diagonal of the room, the total path would be just over 46 m (or 0.15 μs), which all protocols considered in this study should tolerate. Now, consider a very conservative estimation of the delay in a different room with that is 150 m long, which is much smaller than a hanger on a carrier. Using just three reflections (instead of the six) over a 150 m length (instead of the diagonal used before), in contrast, account for 450 m (or 1.5 μs), which is a significant challenge for most protocols.

External interference can be an issue within the ship. A few subsystems, such as power and propulsion, use generators or motors that emanate EMI. Close proximity to these sources will most likely interfere with all wireless communications. Most wireless protocols are designed to tolerate some background interference and gracefully degrade service as the level of interference increases.

3.9.5 On Deck

The ship's deck has very different wireless characteristics compared to the interior of the vessel. In general, the deck is more friendly to wireless communications because the multipath effects are limited (e.g., because most paths are reflected harmlessly away from the ship).

Radar systems may cause interference to wireless communication systems. In theory, the radar systems all operate within their specially licensed spectrums to minimize their impact on other systems. In practice, systems may leak energy at other frequencies (e.g., at nearby frequencies or at harmonics of the operating frequency). If a radar system interferes with the wireless system, it is possible for the radar's slow, periodic scanning behavior to make the wireless protocol unstable. In particular, many wireless systems use dynamic modulation or equalization techniques that are designed to compensate for interference that varies slowly and may become unstable if the interference varies with the periodicity of the radar systems.

3.9.6 In Port

Links to land-based communication systems offer the potential for high-quality communication with external networks (e.g., the Internet and NIPRNET/SIPRNET). Such links may be beneficial for transferring large files, such as the ship's manifestos/logs and software updates for information technology systems.

It may be reasonable to assume that multiple forms of land-based communications systems (e.g., WiFi, Cellular, WiMAX) will be within range of most ports in the near future, or could be added inexpensively. We assume that the vessel's network would be configured such that the link from ship to shore used a gateway (e.g., outside the firewall). Thus, the link to port would be independent of any wireless system used inside the ship (e.g., one could use WiFi internally and WiMAX externally).

A limiting factor in the effectiveness of ship-to-shore communication may be range, because the land-based receiver could be far from the ship. Directional antennas (preferably ones that can be steered in software, such as a phased array) are attractive for this type of point-to-point link.

Another concern when in port is spectrum availability. Local governments allocate spectrum differently. Despite a desire to create widely used standard frequencies for each wireless technology, no such "standards" are globally accepted. Section 3.10.4.1 discusses this issue in more detail.

3.9.7 Ship to Ship

Close proximity ship-to-ship operations have similar characteristics as ship-to-shore. In both cases, the ship needs to communicate with external entities (e.g., another vessel in the fleet or an expeditionary vessel or a land-based tower). As with the port example, distance may be an issue. On the other hand, open water is one of the best environments for wireless communication because it is practically free of multipath interference.

Doppler fading may be an issue for a few reasons. First, expeditionary craft move much faster (relative to the shipboard antenna) than other communication endpoints (e.g., a person walking with a handset). Second, when the ocean causes both vessels to rock, the antennas (particularly ones on high masts) may move very quickly. For example, with a mere 10 degree list caused by

waves with a 10 second period, an antenna 50 meters above the center of rotation moves at a maximum speed of approximately 5.48m/s, which induces a Doppler shift varying from −40Hz to +40Hz every 10 seconds. Not all technologies can tolerate such behavior. More specifically, standards do not address how quickly or to what extent implementations of wireless systems need to react to changes in frequency (except that some mobile applications require wireless systems to operate at appropriate shifts caused by vehicles at highway speeds).

3.9.8 Wireless Principles

Useful wireless systems need to support multiple users. Various multiplexing techniques are available to allow multiple users to share the same network. Note that most of the multiplexing techniques are independent from each other and can be combined.

This section describes the basics of wireless communication techniques. It explains how each technique applies to the impairments described in Section 3.9.2. The relation between the techniques and specific COTS wireless products is reserved for Section 3.10.

3.9.8.1 Frequency Division Multiplexing (FDM)

FDM divides the spectrum into multiple frequency bands such that each (uni-directional or bi-directional) channel has its own frequency band. Such systems need to include a gap between the channels to prevent signals in one band from bleeding into others. In particular, Direct Sequence Spread Spectrum (DSSS) (see Section 3.9.9) needs to be concerned about such bleeding because the spreading process usually results in power in neighboring bands.

3.9.8.2 Time Division Multiplexing (TDM)

TDM shares each channel in time slices. In wired telephony, TDM is used to multiplex multiple subscribes. For example, a T1 circuit has 24 synchronous time slots, one for each of 24 different subscribers. Wired data protocols, such as Ethernet, use asynchronous time slots. For example, Ethernet uses Carrier Sensed Multiple Access (CSMA). In this scheme, a host listens for silence on the medium (wire) before transmitting. Assuming no other host tries to send at the same time,[6] the host is allowed to transmit until it has sent its entire frame (e.g., up to 1518 bytes). Data networks tend to use asynchronous TDM schemes because it works efficiently with bursty traffic.

3.9.8.3 Code Division Media Access (CDMA)

CDMA allows multiple users to share the same medium (i.e., frequency) concurrently using codes with different keys. The keys are selected in such a way that (a) the receiver can identify a signal using the key and (b) the remaining signals appear as uncorrelated white noise. Section 3.9.9 describes such systems.

3.9.8.4 Orthogonal Frequency Division Media Access

Orthogonal Frequency Division Multiplexing (OFDM) (described in Section 3.9.10) can reserve sets of subcarriers for individual users. OFDMA shares OFDM subcarriers between multiple users. This allows multiple users to share the same spectrum.

---

[6] Due to propagation delays, it is possible for a second host to believe that the channel is available and to start sending packets. This results in a collision. A common solution (CDMA/CD) force both hosts to wait some prescribed period of time with a random backoff before attempting to resend the data.

3.9.9 Spread Spectrum

Spread spectrum operates by sending the same signal over a span of frequencies within a spectrum band, instead of using a single frequency (e.g., the center frequency). With Direct Sequence Spread Spectrum (DSSS), this is accomplished by multiplying (XORing) the signal with a repeatable pseudo-random code sequence at a rate (called the *chip rate*) that is faster than the symbol rate. For example, each Global Positioning System (GPS) satellite uses a different 1023-bit code that runs 1023 times faster than the symbol rate. The code is XORed with the data or symbol (GPS uses a single data bit per symbol) before transmission.

DSSS is inherently resistant to delay spread. The pseudo-random sequence has a low autocorrelation over most delays. Only signals that are within the same chip or separated by the entire code sequence (e.g., 1023 chips apart with GPS) interfere with one another.

Another version of spread spectrum is frequency hopping. With Frequency Hopping Spread Spectrum (FHSS), the signal periodically cycles through a sequence of frequencies. In general, the hopping frequency is much slower than the symbol rate. For example, the system could hop to one of ten frequencies every 50ms. As with DSSS, due to Rayleigh fading, we expect that some frequencies will be weak (such that the receiver cannot reconstruct the correct symbol) and others will be strong.

3.9.10 Orthogonal Frequency Division Multiplexing (OFDM)

OFDM provides a method of sending signals using an approach that is very different from those described above. OFDM divides a channel into a large number, *N*, of closely spaced frequencies (subcarriers). Each subcarrier transmits a different data symbol (except that some carriers are reserved for special purposes, such as pilot tones and guards). The method for mapping the data bits to subcarrier symbols makes efficient use of Fast Fourier Transform (FFT) operations that are common on Digital Signal Processors (DSPs). Because *N* symbols are sent in parallel, OFDM systems can use a longer symbol period while providing a higher data rate than a single-carrier equivalent. To obtain the same data as single-carrier system, an OFDM system could hold each symbol nearly *N* times the period of an equivalent single-carrier system. In practice, OFDM systems use a symbol period that is only a few times longer than that of the single carrier system to improve the data rate.

OFDM can be particularly tolerant of delay spread because it uses a long symbol period. It usually includes a guard interval between symbols where delay spread can safely occur.

OFDM is almost always used in conjunction with Forward Error Correction (FEC) codes (See Section 3.9.12). Use of FEC allows OFDM to operate when some fraction of subcarriers have weak signals. Because OFDM spreads the FEC across multiple frequencies, this approach tolerates bit errors due to Rayleigh fading.

3.9.11 Multiple Input Multiple Output

Use of multiple antennas, called Multiple-Input/Multiple-Output (MIMO) (See [85] [86] [87] [88]), has the potential of significantly improving the performance of wireless systems. In many cases, effects (such as multi-path and interference) that impair the performance of single antenna systems, or Single-Input/Single-Output (SISO) systems, can actually *improve* the performance of MIMO systems by providing diversity between antenna pairs. Under appropriate conditions

(including some scattering of signals due to multi-path), MIMO can improve data rates linearly with the number of antennas (specifically the minimum of the number of transmit and receive antennas).

The main goal of MIMO is usually to improve spectral efficiency (measured in bits/second/Hz; where Hz is the spectral bandwidth). Claude Shannon determined that a fundamental limit of the channel capacity (rate that data can be sent over a medium) is given by the equation $C = B\log_2(1-S/N)$, where C is the theoretical maximum channel capacity (bps), B is the spectral bandwidth (Hz), S is the energy in the signal, and N is the energy of the noise (including interference). Spectral efficiency is a measure of how close the system comes to attaining this limit. It is a limiting factor in the maximum throughput of a system.

Advantages of MIMO include:

Increased bit rate
Decreased bit error rate
Reduced power
Increased range
Resilience to fading/interference

Not all of the advantages can be attained at the same time. In fact, there is usually a direct trade-off between bit rate, bit error rate, and power such that one can improve any one metric at the expense of the others (up to limitations such as maximum transmit power and available modulation methods). Regardless of the choice of parameters, MIMO systems consistently improve spectral efficiencies over comparable SISO systems.

3.9.12 Modulation and Coding

Various approaches exist for mapping data bits to digital signals. The process of performing this mapping is called *modulation*. Common modulation techniques include BPSK, QPSK, QAM-16, and QAM-64 (see Table 3-18). These schemes map sets of data bits into waveforms that can be represented as points on a constellation diagram. A constellation diagram (see Figure 3-37) plots a waveform onto two dimensions, which can be represented as the real (in-phase) and imaginary (quadrature)[7] components of the waveform at a given frequency (e.g., as calculated by an FFT). The main differences between the schemes are the number of bits represented by each symbol and their resistance to noise. High-rate techniques require a strong signal strength and error correction.

Table 3-18. Sample Modulation Techniques

Modulation Technique	Bits per symbol
Binary Phased Shift Keying (BPSK)	1
Quadrature Phased Shift Keying (QPSK)	2
Quadrature Amplitude Modulation-16 (QAM-16)	4
Quadrature Amplitude Modulation-64 (QAM-64)	6

[7] In signal processing, one can represent periodic waves in a number of equivalent ways, based on the orthogonality of sine and cosine waves. One method is to plot cos() on the real axis and sin() on the imaginary. Using polar coordinates, one can express phase as an angle. If the amplitude of the cos() is plotted on the x-axis (i.e., with phase 0, or "in-phase"), sin() would be expressed as being a quarter-circle (or "quadrature") out of phase relative to the cos().

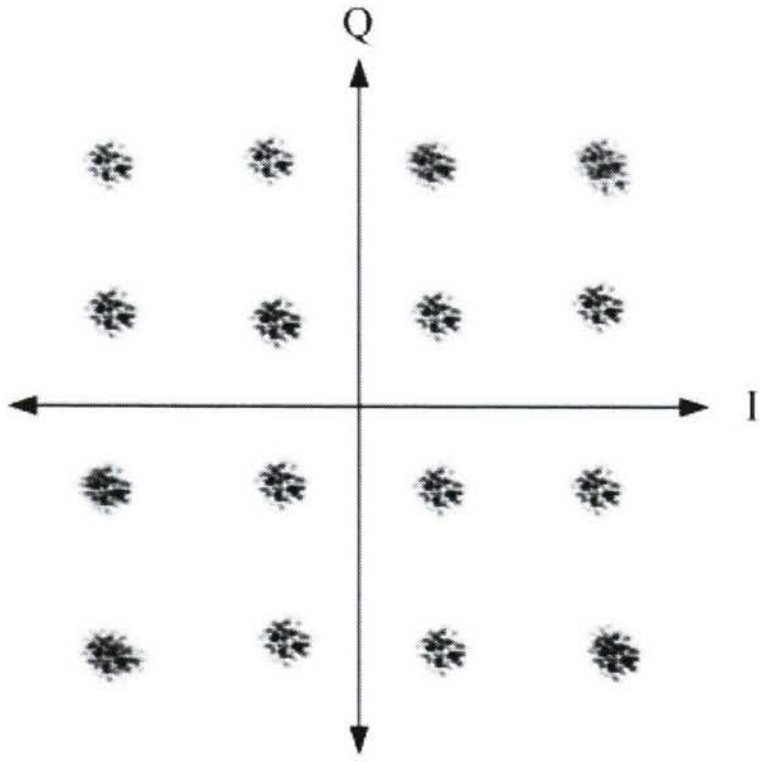


Figure 3-37. Example QAM-16 Constellation Diagram

Figure 3-39 illustrates an example of BPSK modulation. The topmost curve shows the data bits (i.e., high is logical 1 and low is logical 0). The next two curves show the carrier and the carrier shifted 180° out of phase. The signal is formed by selecting the in-phase carrier when the data bit is 1 and the out-of-phase carrier when the data bit is zero.

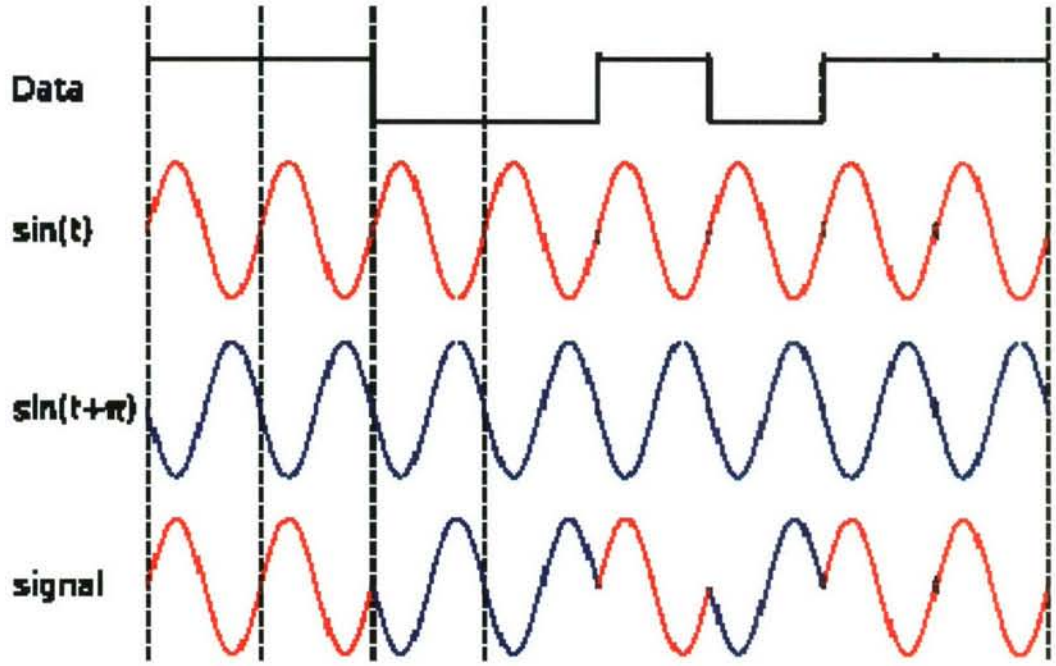


Figure 3- 38. BPSK Example

Figure 3-38 shows an example constellation for QAM-16. A scatter plot of measured in-phase and quadrature amplitudes may result in a plot like the one shown in the figure. One can visually identify the 16 distinct symbols, each of which QAM-16 assigns a different 4-bit value.

Forward Error Correction (FEC) codes encode data with redundant bits such that the receiver can recreate the original data even when bit errors corrupt the transmitted data. Reed-Solomon codes (which are used, for example, in RAID-6 and on audio CDs) are examples of a FEC algorithm. There is generally a tradeoff between the data overhead and the ability to tolerate bit errors. Typical FEC rates in wireless systems range from 1/2 to 5/6 data bits per symbol bit. Some data systems use per-frame error detection codes (e.g., Cyclic Redundancy Check (CRC)) to detect (but not correct) errors. High data-rate protocols tend to rely on the correcting ability of FEC codes.

All common wireless protocols today use adaptive modulation, which dynamically selects the appropriate modulation technique based on the received signal strength. When the signal strength is good, the system uses a high data-rate modulation technique and forward error correcting code. When the system starts to detect errors, it selects a more robust modulation technique and/or FEC rate, resulting in a lower data rate.

3.9.13 Gaussian Minimum Shift Keying

Another modulation scheme is Gaussian Minimum Shift Keying (GMSK). It can be generated by switching between two sinusoidal signals (e.g., the carrier frequency and half the carrier frequency). This section is included because GSM uses GSMK. The details of this scheme are beyond the scope if this report.

One characteristic of GMSK is a very narrow power spectrum. This allows efficient use of spectrum because channels may be packed together tightly. GMSK systems can operate at low power (relative to other modulation techniques). Inexpensive hardware implementations for

GMSK have existed for several years. GSM takes advantage of properties of GMSK that work well with simple channel equalization approaches (below).

3.9.13.1Channel Equalization

Signal processing can be used to help cancel out multipath effects. In principle, equalization techniques work by measuring the strength of received multipath signals in the recent past to predict and cancel out their present effects. An efficient equalizer can actually enhance the received signal by combining each received reflection.

Simple, linear equalizers are inexpensive, but tend to amplify noise. Non-linear equalizers, such as decision-feedback equalizers, perform well except after a bit error, when the processor incorrectly predicts the transmitted signal and, as a result, uses an incorrect prediction of the subsequent reflections, often resulting in a burst of bit errors.

Maximum-likelihood sequence detection is an optimal equalization algorithm, but scales poorly with the delay period and the modulation scheme's bits/symbol ratio. Various approximations (e.g., Dual-Decision Feedback Equalizer (DDRE) and Reduced-State Sequence Estimator (RSSE) may be used in practice.

3.9.14 Summary of Wireless Techniques

Table 3-19 summarizes the differences between the main wireless techniques discussed above with respect to their ability to tolerate the critical impairments described in Section 3.9.2. The first column lists the impairments. The remaining columns qualitatively and subjectively describe the relative effectiveness of each technique. The second column describes a system that uses narrowband FDM and TDM (i.e., without combining other techniques).

Table 3-19. Summary Mapping between Technologies and Impairments

Impairment	FDM/TDM	DSSS	OFDM	MIMO
Rayleigh Fading	Poor	Good	Good	Excellent
Doppler Shift	Poor	Fair	Fair	Fair
Delay Spread	Poor	Good	Excellent	Excellent
Interference	Fair	Good	Good	Good
Co-channel Interference	Poor	Fair	Poor	Fair

This page intentionally left blank.

3.10 OTS Wireless Technologies

This section describes the details of relevant wireless technologies. Only technologies that are available now or are likely to be commercially available by 2012 are considered. The technology will be expected to support voice and data applications.

The wireless technologies include:

WiFi, wireless local area network,
WiMAX, wireless broadband, and
Cellular, including Global System for Mobile communications (GSM)/Universal Mobile Telecommunication System (UMTS), and CDMA.

A few technologies were considered but determined to be impractical. Bluetooth is used for personal area networks. It provides low range (e.g., about 10 m) and low bandwidth (less than 3 Mbps). Bluetooth also has limitations in the maximum number of devices in a single network and questionable security. In the future, Bluetooth may address these open issues. It should be noted that the next generation of Bluetooth expects to use Ultra-Wide Band (UWB). UWB has the potential to work very well in RF-challenged environments primarily because it operates over a very large frequency range (which helps systems to tolerate interference, fading, and Doppler effects). Because the specifications are not complete, it is not possible to analyze how well UWB-based Bluetooth will work in the naval environment.

Existing technologies, such as Land Mobile Radio (LMR), already provide wireless voice service within the Navy. User experience has suggested that the voice quality is substandard. LMR does not provide data service. Similarly satellite communication is not considered because of its low bandwidth and inability to penetrate below deck or underwater.

3.10.1 802.11/WiFi

The leading technology for WLANs is WiFi (or Wireless Fidelity). WiFi uses the IEEE 802.11 standard, including a number of addendums (See 5-20). The term Wi-Fi is a trademark owned by the Wi-Fi Alliance, which is a trade group of equipment manufacturers promoting 802.11 WLAN products. WiFi (which usually appears unhyphenated) and 802.11 can be used interchangeably in most contexts. Because WiFi is widely used today, the cost of equipment is very low (e.g., about $50 to $75 for an access point).

Since its initial publication in 1997, the standard has evolved continually. Each amendment to the original standard is published with a different letter appended to the 802.11 label. For example, 802.11b extended the maximum data rate to 11Mbps. This approach can lead to a confusing set of sub-standards. Table 3-20 lists the most significant addendums.

Table 3-20. IEEE 802.11 Standard Addendums

Addendum	Title	Comment
802.11a	High Speed in 5 GHz Band	Up to 56 Mbps
802.11b	Higher Speed in 2.4 GHz Band	Up to 11 Mbps
802.11e	Quality of Service Enhancements	Prioritization (WMM)
802.11g	Further Higher Data Rate Extension in 2.4 GHz Band	Up to 56 Mbps (compatible with 802.11b)
802.11i	MAC Security Enhancements	Security (WPA/WPA2)
802.11n	High Throughput	MIMO (mid 2008)

WiFi is used primarily for data applications. It was designed to support residential and business users as a wireless replacement to Ethernet networks. Although it provides reasonable bandwidths, most users experience data rates considerably slower than the maximum supported rate (e.g., 2 to 5 Mbps may be common for a 56 Mbps 802.11g system in typical environments). Also note that users sharing the same access point must compete for the same bandwidth (as compared to a switched Ethernet network where many connections can operate in parallel).

In an obstruction-free environment (e.g., at sea), WiFi can span distances over 100 m (802.11n should reach 160 m). The limiting factor appears to be signal strength (recall that the signal attenuates with the square of the distance). Typical environments contain obstructions (e.g., walls) that greatly reduce the effective range of WiFi systems to at least half the maximum range.

3.10.2 802.16/WiMAX

WiMAX (or Worldwide Interoperability for Microwave Access) was developed to create a standards-based protocol for wireless broadband. The WiMAX Forum promotes the standard and provides certification processes to ensure interoperability (similar to what the WiFi Alliance does for WiFi). The IEEE created and maintains the standards as the 802.16 series, again similar to 802.11 for WiFi (see Table 3-21). The most recent standard with commercial implementations, 802.16e is replacing the previous one (802.16d) as the de facto standard. The most significant difference between the two is that 802.16e supports mobility.

Table 3-21. WiMAX Standards

Standard	Title	Key Advancement
802.16a	Extension to sub-11 GHz	2 to11 GHz bands and OFDM (for NLOS)
802.16d-2004	Air Interface for Fixed Broadband Wireless Access Systems	Incremental improvements
802.16e-2005	Air Interface for Fixed and Mobile Broadband Wireless Access Systems	Support mobility
802.16m	Advanced Air Interface	100 Mbps for mobile; 1 Gbps for fixed (late 2008)

WiMAX will likely play a crucial role in the next generation of cellular wireless technologies (4G). Unlike previous mobile technologies, which are circuit based, 4G will be IP-based packet switched. Voice applications will use Voice over IP (VoIP), e.g., SIP [89], over a 4G network. To meet this goal, WiMAX is designed to support the bandwidth and QoS requirements necessary for toll-quality voice.

3.10.3 Cellular Technologies

Commercial cellular services use one of two competing families of protocols. 3GPP maintains standards for one family, which includes GSM and UMTS; 3GPP2 maintains the other family, which includes CDMA and will soon include Ultra Mobile Broadband (UMB). Both families will compete with WiMAX in the near future.

The two families perform similarly (e.g., in terms of number of subscribers and data rates). The main differences between the two families are

a) the modulation and coding techniques,
b) the spectrum they operate in (so that they can coexist in the same physical area),
c) where they are supported. CDMA is used in North America; GSM is supported worldwide with approximately ten times the subscriber base as CDMA.

Originally, the most striking technical difference between the two was that GSM used TDMA whereas CDMA (as the name implies) uses CDMA. When 3GPP introduced UMTS to improve data rate (e.g., for the wireless web), it moved to a CDMA-based protocol. Due to bandwidth limitations of CDMA-based technologies, both families plan to move to OFDM in the next generation, e.g., Long Term Evolution (LTE) and UMB.

Table 3-22 lists the cellular data protocols defined by 3GPP (GSM) and 3GPP2 (CDMA). The table shows the approximate year the protocol was (or is expected to be) standardized, the approximate maximum data rate, the protocol family and the bandwidth per channel. The data rates are approximate. Most protocols have some degree of parameterization, such as the number of uplink and downlink channels or the total number of channels. In some cases where the data rates are asymmetric, the downlink and uplink rates are both shown (separated by a slash). Some data rates can be misleading, such as those for High-Speed Downlink Packet Access (HSDPA), which defines support for a 14 Mbps mode of operation even though no vendor expects to be able to build such a system for several years. Figure 3-39 illustrates most of the information in Table 3-22 graphically. Each box in the figure is positioned approximately with the year of introduction on

the horizontal axis and with the bandwidth on the vertical axis (on a log scale). Color connects protocols belonging to the same family.

Table 3-22. Cellular Data Protocols

Year	Protocol	Data Rate (down/up)	Family	Bandwidth
3GPP				
1997	General Packet Radio Service (GPRS)	115 kbps	GSM	200 kHz
1999	Enhanced Data Rates for GSM Evolution (EDGE)	384 kbps	GSM	200 kHz
2002	High-Speed Downlink Packet Access (HSDPA)	1.8 to14 Mbps	UMTS	5 MHz
2007	EDGE Ev	750 kbps	GSM	200 kHz
2007	High Speed Packet Access Plus (HSPA+)	<14 Mbps/5.76 Mbps	UMTS	5 MHz
2008	High Speed OFDM Packet Access (HSOPA)	40 Mbps	UMTS	5 MHz
2009	LTE/HSDPA Evolved	>100 Mbps/50 Mbps	LTE	≤20 MHz
3GPP2				
1995	cdmaOne	14.4 kbps	IS-95	1.25 MHz
2000	1 times Radio Transmission Technology (1xRTT)	307 kbps/153 kbps	Cdma 2000	1.25 MHz
2002	Evolution-Data Optimized (EV-DO) (rev 0)	2.4 Mbps/144 kbps	Cdma 2000	5 MHz
2006	EV-DO rev A	3.1 Mbps/1.8 Mbps	Cdma 2000	5 MHz
2007	EV-DO rev B	14.7 Mbps/5.4 Mbps	Cdma 2000	5 MHz
2008	UMB	>100 Mbps	UMB	TBD

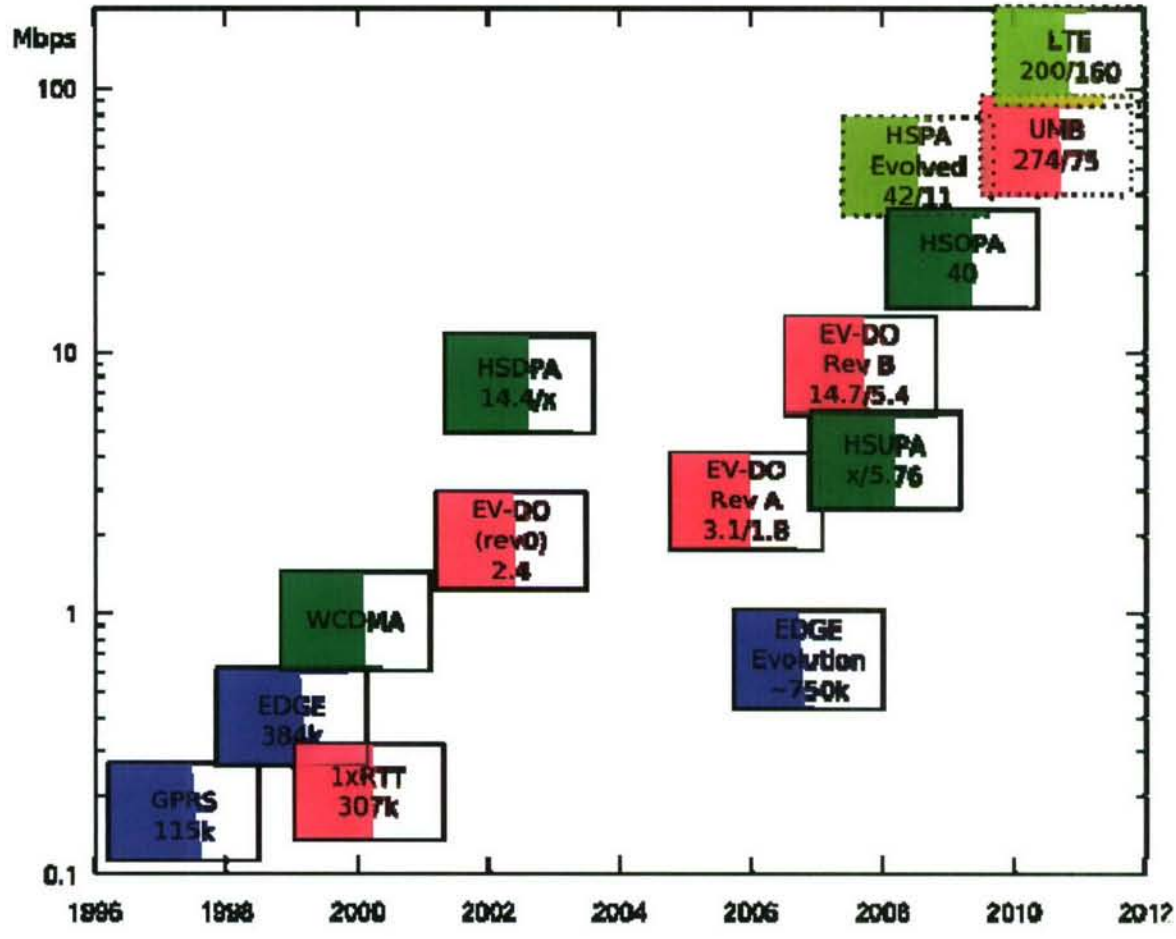


Figure 3-39. Evolution of Cellular Data Protocols

3.10.4 Issues and Concerns for Wireless Systems

3.10.4.1 Spectrum Issues

Spectrum is a band of frequencies that wireless systems operate in. Allocating distinct spectrum for each wireless system helps to prevent interference between different technologies. Some bands are "unlicensed," which means that under certain restrictions (such as power limitations) users may operate equipment that uses frequencies in the spectrum without obtaining a license to do so.

Unlicensed spectrum is practical for short range systems, such as WLANs (e.g., WiFi). Competing technologies can share the same frequencies in different geographical areas (e.g., at the discretion of the property owner). For example, WiFi and Bluetooth both operate in the 2.4 GHz spectrum. Although the two technologies would interfere with each other if used in the same room, the fact that both operate at low power serves to reduce their interference, say, between buildings. Protocol and equipment vendors need to assume that devices operating in unlicensed spectrum will usually suffer from low to moderate levels of interference from other technologies.

Although some broad spectrum bands have near-global acceptance as unlicensed bands (in particular, 2.4 GHz and 5.8 GHz), most nations have imposed restrictions on the use of frequency bands typically on either side of the normally accepted ranges. With 802.11b, for example, although most countries support 2.4 GHz operations, no single channel can be used in US, Europe, and Japan. Table 3-23 indicates which channels are available for use (as marked with an "X") by country or region.

Table 3-23. 802.11 Channel Allocation by Country

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Freq.	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462	2467	2472	2484
US	X	X	X	X	X	X	X	X	X	X	X			
Europe	X	X	X	X	X	X	X	X	X	X	X	X	X	
France										X	X	X	X	
Spain										X	X			
Japan														X

Interference from different systems sharing the same frequencies would impair one or both systems. To avoid such conflicts, governments carefully regulate how spectrum is used. Regulations typically define the application, power restrictions, amount of leakage into nearby bands, etc. Sometime regulations include whether the communication is uni- or bi-directional, type of multiplexing or media access (e.g., FDM, TDM), etc.

Independent decisions to allocate bands for specific applications and resistance to change historically allocated bands, has resulted in fragmented spectrums that differ between countries, despite economic advantages to having global interoperable standards. As a result, wireless technology developers struggle to find spectrum that can be reused between countries.

After the government approves spectrum for the application (e.g., WiMAX), equipment vendors can configure their equipment (e.g., adjust frequencies and power) to operate accordingly. After that point, the end customer has little concern about spectrum. This is not the case, however, for naval systems because each port may have different regulations. The naval system needs to be aware of potential issues in (or near) foreign ports. One option is to disable wireless

communication equipment before entering port. Another potential option is to use software-defined radios that can select appropriate frequency and transmit power in accordance with each visited country's regulations.

3.10.4.2 Data and VoIP

As a general rule, systems designed for data communications provide poor quality voice and systems designed for voice communications provide poor quality data. WiMAX, was designed for both data and voice (specifically VoIP) and should provide very good quality for both.

Many attempts at VoIP over WiFi have been tried. Under good conditions (i.e., consistently good signal strength and low contention from other users), VoIP over WiFI works very well. When signal strength is low short outages results in poor voice quality. Similarly, when other WiFi users saturate the channel (e.g., by performing big file transfers for example), the system does not always have enough bandwidth for voice, causing voice quality to suffer. Newer WiFi products with higher bandwidth and better signal properties (e.g., MIMO in 802.11n) may fare better than the previous generation of WiFi products for supporting VoIP.

Cellular systems currently provide low data bandwidth, though rates are improving (see Section 3.10.3). Even with higher maximum bandwidth, cellular systems have higher frame error rates than most other systems. The small frame size and high frame error rate can result in a high IP packet drop rate, which reduces throughput (particularly for TCP-based applications due to TCP's congestion control algorithms).

WiMAX has been engineered to support both high-bandwidth data applications and VoIP. We expect that it will provide very good performance for both.

3.10.5 Resilience

3.10.5.1 Security

Historically, wireless data and voice systems suffered from inadequate security. WiFi's security woes with Wired Equivalent Privacy (WEP) are well documented (e.g., [90][91][92]). Similarly, fraud (e.g., cloning) posed problems for the cellular industry in the 80's and early 90's. Both data and voice systems have addressed these historical issues to significantly improve their security. In each case, the improved security models and protocols provide confidentiality for user data and support authentication between mobile units and access points.

WEP suffered from poor key reuse, small key sizes, and a vulnerable encryption algorithm. To fix these issues, IEEE created 802.11i (which is the basis for the WiFi Forum's WPA2). 802.11i uses strong cryptographic techniques: Advanced Encryption System (AES) in Counter-CBC/MAC (CCM) mode, temporal keys (i.e., it does not reuse the same key for multiple sessions and purposes, as WEP does), and mutual authentication. For authentication, 802.11i makes use of Extensible Authentication Protocol (EAP), which is a versatile framework that can tie into pre-existing authentication systems (e.g., Public Key Infrastructure (PKI), Common Access Card (CAC), Secure ID, RADIUS, etc.). Most cryptography experts believe that 802.11i is a sound protocol when configured to require mutual authentication.

WiMAX supports a set of cryptographic procedures similar to those of 802.11i. It uses standard algorithms, such as AES, for link encryption and EAP for authentication. Because WiMAX is a

new technology, it is not clear that all implementations available today make full use of the security features WiMAX supports.

The current generation of cellular systems uses encryption to protect content (voice and data) and to authorize the mobile stations. Most suffer from weak key sizes and are potentially vulnerable to cryptographic attacks because they use non-standard algorithms.

GSM introduced a smart card, called the Subscriber Identity Module (SIM) card, to enhance security. The card securely stores the mobile user's private keys and performs cryptographic operations (e.g., to generate the 32-bit response needed to authenticate the mobile station (MS) to the base station (BS). During the authentication process, the BS and MS negotiate a 64-bit[8] session key to encrypt the payload of each frame (e.g., the voice and data payload). The encryption algorithm, A8, is based on COMP128 (as is A3, the primary algorithm for authentication). Several cryptographic attacks demonstrating weaknesses in these protocols have been publicized (e.g., [93][94][95]).

CDMA uses encryption for link privacy and authentication. Instead of the SIM card, CDMA provisions each MS with a 64-bit authentication key, or A-Key, which is similar to a password. After a handshake, the MS and BS negotiation separate authentication and encryption keys (64-bit each). The authentication key is used to calculate an 18-bit hash value that authenticates the MS to the BS. By assumption, if both parties agree on the derived encryption key, they must know the MS's A-Key and hence the MS implicitly authenticates the BS. Signaling messages use the 64-bit encryption key. Data applications (e.g., EV-DO) use a 32-bit encryption algorithm. Voice traffic is not encrypted, per se, but is encoded according the 48-bit "long code sequence." The long code sequence is one of the CDMA codes shared between the MS and BS[96].

3.10.5.2 Interference

Some equipment used aboard ships (e.g., engines/generators/reactor) creates electro-magnetic interference over broad frequency ranges. Radar systems, other communication devices, and appliances (e.g., microwave ovens) may also contribute interference. In general, all the technologies described in this study should tolerate reasonable levels of interference. The effect of the interference varies with distance. The strength of the interference and the good signal both decay with the square of the distance. Thus, in close proximity to an interference source, wireless devices may fail to operate.

It is common practice to perform a site survey prior to installing access points. Part of the site survey includes measuring background interference at the target frequency band over the target site. Any issues due to external interference should be detected and corrective measures (such as moving access points or adding additional ones) can be taken.

Some techniques, such as DSSS, help systems to tolerate interference by spreading the signal energy over a wide bandwidth. This improvement is called *processing gain.* For example, a DSSS that is six times wider than a comparable narrowband signal would effectively reduce the interference by a factor of six (or about −7.8dB).

MIMO is naturally resistant to interference. In fact, MIMO sometimes relies on some level of interference to provide diversity between distinct channels.

[8] The key is effectively 54 bits because the first 10 bits are set to zero.

3.10.5.3 Jamming

All COTS products are susceptible to jamming because all the system parameters (e.g., frequencies, spreading keys) are known. Because of the very tight tolerances with high data-rate signals (e.g., ones using OFDM with QAM-16) weak jamming efforts may cause the system to adapt to a low-bandwidth configuration (e.g., BPSK).

Signal acquisition (i.e., the process of determining what devices, if any, are accessible on a channel) is almost always vulnerable to jamming. Wireless protocols that rely on pilot tones (e.g., CDMA cellular systems and most OFDM systems) are similarly vulnerable to advanced jamming techniques. By jamming the pilot tone (e.g., sending a strong pilot tone that is out of sync with the true one) the system becomes unusable.

Another approach to jamming is to inject packets that purposely collide with other packets (e.g., from a device that joins the network according to the protocol). Most systems detect contention and obligingly back off until the channel appears to be available.

Although DSSS-based protocols often tout resistance to jamming as a benefit, the statement is only true when the Pseudo-Random Number (PRN) sequences are unknown to the jammer. That is not the case for the COTS protocols in this study. Potential jammers can easily obtain the sequences from the standards. Note that the long sequence used in CDMA cellular systems is shared between the BS and MS, but not known to others and hence provides some resistance to jamming.

MIMO has some very good properties for anti-jamming. The extra degrees of freedom due to the multiple antenna combinations afford MIMO with an opportunity to work around interference due to jamming. In particular, when being jammed, MIMO's channel estimation algorithm treats the jamming signal the same as any other type of interference. Though beyond the scope of this report, MIMO also lends itself well to sophisticated (non-COTS) anti-jamming strategies to counter advanced jamming techniques (e.g., spoofing pilot signals and pulsed jamming).

Note that the vessel itself provides excellent protection against jamming. The steel exterior would reflect nearly all of the energy from an external jammer. For the low decks, water provides even better insulation against microwave signals.

3.10.6 QoS and Interface to the Core Network

Each technology provides some degree of QoS. In most cases, multimedia applications drove the need to include QoS provisioning into the network. In each case, a standard IP interface can be used to connect to the core network. WiFi typically plugs directly into Ethernet switches. WiMAX can plug directly into IP routers or Ethernet switches. Cellular systems are more likely to aggregate traffic on one network and use a gateway to connect to the core network. In any case, because of security concerns, it is good practice to isolate the wireless network (e.g., via VLANs) to perform authentication and access control (e.g., using EAP and/or firewalls) before allowing access to the core network.

WiFi provides a strict priority-based QoS mechanism with Wi-Fi MultiMedia (WMM). WMM is the WiFi Alliances protocol, based on IEEE 802.11e. Most new 802.11 equipment supports the WMM standard. Although Microsoft provides an API for using WMM with their latest mobile OSes (e.g., Windows Mobile) and desktop OSes (e.g., Vista), few (if any) applications make use of

it. Though it is possible to translate the WMM priorities into DiffServ code points (DSCP), it is not clear if any wireless routers does so by default.

WMM defines four classes, voice, video, best effort, and background. The standard refines the backoff procedure to recover from a collision, such that higher priority services will wait less time before attempting to retransmit than low priority services.

WiMAX defines five types of services to support different classes of service (See Table 3-24). Support for VoIP drove much of the QoS architecture. Service levels can be assigned on a per-flows basis. The WiMAX standard leaves many QoS details up to the equipment vendors (such as how to schedule packets). The service classes can be mapped to DiffServ classes where the WiMAX network connects to the wired network.

Table 3-24. WiMAX Service Classes

Service Class	Use
Unsolicited Grant Service	Fixed periodic traffic (similar to T1)
Real-time Polling Service	Variable sized periodic traffic (e.g., MPEG video)
Non-real-time Polling Service	Low latency applications
Best-effort Service	Common data applications
Extended Real-time Polling Service	Combines Unsolicited Grant Service and Real-time Polling Service

QoS is inherent in cellular networks because it is a channel-based network. Typically, one can provision a minimum number of voice and data channels, and either service can make use of unused resources belonging to the other. Voice is almost always given priority over data services. Beyond the wireless network, the cellular system connects to separate networks for voice and data. A base station router (e.g., a self-contained cellular system with only an IP interface on the wired side) may provide standard QoS translations (e.g., DiffServ) to prioritize VoIP over data traffic.

3.10.7 Cost

WiFi is a very cost effective system today. Most laptops ship with integrated WiFi support. State of the art access points for $100-$200 are readily available (Federal Information Processing Standard (FIPS) 140 [28] certified devices may be more expensive). Network interface cards range from $20-$100. Connecting to the wired network is easy because WiFi access points use standard Ethernet interfaces.

Cellular systems can be very expensive (in the hundreds of thousands of dollars). Smaller systems, such as base-station routers, provide a subset of the features commercial providers require and range in price from a few hundred to a few thousand dollars each.

WiMAX attempts to position itself between WiFi and cellular in terms of cost. Commodity WiMAX end devices are starting to appear on the market. Sprint's announced plan [97] to provide nationwide coverage across the United States should reduce the cost of WiMAX equipment. Today, full-featured WiMAX routers for high-speed point-to-point links cost upwards of $10,000. Smaller routers for indoor use start at a few hundred dollars each.

3.10.8 Availability of COTS products

WiFi devices are readily available today. Although the 802.11n standard has yet to be published, devices conforming to pre-publication draft versions of the standard are currently on the market. Most new products have the WiFi Alliance's WPA2 certification, which requires conformance to a subset of the 802.11i standard. A few WiFi devices also have FIPS 140-2 certifications.

WiMAX devices are just reaching the market now. WiMAX infrastructure (e.g., base stations) and PC cards appeared on the market within the last year. Sprint [97] has announced plans for nationwide WiMAX coverage by the end of 2008 using 802.16e-2005 in the 2.5 GHz spectrum. Such a network would greatly accelerate the availability and selection of WiMAX devices.

The cellular systems are constantly upgrading to the latest standards to improve service and data rates. Due to the complexity of cellular systems, development times may be long. Typical lag time from release of standards to widespread deployment is about two years. New technologies (e.g., ones requiring new hardware or spectrum) may require more time. Compact base stations lag one to two years behind commercial deployments. Ruggedized, miniature base stations may lag another one to two years. Thus, the COTS cellular systems suitable for a vessel in the next five years may resemble what is commercially available today.

3.10.9 Benefits and Disadvantages

This section summarizes the strengths and weaknesses of each technology group.

3.10.9.1 WiFi

WiFi is the standard technology for wireless local-area data networks. Commercial success and competition (primarily in residential and office environments) has lead to very cost effective equipment. The success has also driven considerable development efforts to improve the bandwidth and signal quality of WiFi devices. Because WiFi is inexpensive and limited in range, it is common (and feasible) to have many access points to cover a small area (e.g., one access point per room or for every other room).

Initial attempts to provide voice service over WiFi have been only moderately successful. Under good conditions (e.g., a strong signal with few users), VoIP over WiFi operates just like VoIP on a wired network. As additional users contend for the data bandwidth (e.g., transferring files), the quality of the voice call quickly degrades. Similarly, if the signal is weak, there may be short service outages that also degrade voice service. Several advances in WiFi may help address these problems: traffic prioritization with WMM, increased bandwidth, and improved coverage with MIMO (802.11n).

We expect that multipath interference in large, open interior areas (e.g., hangers) will be problematic for WiFi due to delay spread. Unpublished experiences with first generation WiFi equipment in the airship hanger at Lakehurst, NJ support this expectation. Actual measurements with more recent WiFi devices could quickly determine the extent to which multipath degrades WiFi performance.

3.10.9.2 WiMAX

WiMAX provides significant bandwidth improvements over the other technologies. Because it was designed to support data and voice applications, it has provided QoS capabilities from its inception. WiMAX supports protocols (e.g., MIMO and OFDM) that are resistant to most of the impairments found in RF-challenged environments.

WiMax is a new technology. As such, the cost is still relatively high and not all of its features have been proven in the field. The initial WiMAX applications are used primarily for point-to-point connections (similar to what is needed for ship-to-shore).

Section 3.10.4.1 discusses license issues that affect WiMAX deployments.

3.10.9.3 Cellular

Cellular systems provide near-ubiquitous voice coverage at (or close to) toll quality. Commercial pico-cell designs (including base station routers) and distributed antenna systems can be used to create a cellular network extension (or private network) in an RF-challenged environment (usually indoors or underground).

Although cellular technologies support data applications, the data rates are lower than the other technologies. The data rates, however, are constantly improving. Unlike the other data networks, where voice and data compete for the same resources (e.g., a single channel), cellular systems can

reserve channel resources. Because channels are independent, the quality of voice and data applications does not degrade (until the system approaches its capacity).

Cellular systems have questionable security. As described in Section 3.10.5.1, cryptographic systems in GSM and CDMA use weak key sizes and potentially vulnerable algorithms.

The spectrum issues described in Section 3.10.4.1 may affect cellular technologies. In general, voice bands are fairly well standardized because of the industry's push for mobile sets that can operate globally (e.g., otherwise frequent travelers would need several cell phones depending on where they visit). It is not clear that data services (e.g., UMTS) will be able to share the same level of commonality.

This page intentionally left blank.

3.11 Embedded Devices

3.11.1 Overview

The following section discusses several embedded, Commercial Off The Shelf (COTS), design solutions available today for VoIP Terminal devices. This discussion is intended to provide the reader with an understanding of the types of embedded solutions available and in use today for VoIP communication. It is not intended to be a complete listing of embedded design solutions, nor is it intended to advocate any one solution over another.

In this paper, the terms Embedded Device and VoIP Terminal are used interchangeably. The embedded design solutions discussed here have been separated into three categories:

- Stand-Alone VoIP Devices.
- Integrated Circuit (IC) VoIP Devices
- Custom VoIP Devices

By looking at the differences in call data routing over a circuit switched vs. packet switched network, we identify the major functional tasks that a VoIP Terminal must perform to support voice communication. These functional tasks are then mapped to computer hardware components needed to support each task.

Finally, example devices from each of the embedded design solution categories are examined. Each example device is briefly described, and examined in terms of its supported hardware components.

3.11.2 Embedded Design Solutions

For discussion purposes we define three categories of embedded design solutions for VoIP Terminal devices as follows.

3.11.2.1 Stand-Alone VoIP Devices

The first category, Stand-Alone VoIP Devices, includes IP Telephones, Analog Telephone Adapters (ATA), and other stand-alone VoIP endpoint devices. These solutions are designed to work "out of the box" with minimal configuration and connect directly to a high speed IP network.

3.11.2.2 Integrated Circuit (IC) VoIP Devices

The second category, Integrated Circuit (IC) VoIP Devices, includes IC solutions currently being produced and manufactured by semiconductor companies for use by third party integrators. These types of embedded solutions normally need to be fitted for power, and may require integration of computer peripherals such as a display and input device.

These solutions are normally provided with supported voice codecs, and will include demo source code for building an IP Soft Phone application. In some cases the manufacturer may additionally provide a software development library for building VoIP Terminal devices for their particular hardware solution.

3.11.2.3 Custom VoIP Devices

The third category, Custom VoIP Devices, would include devices built around custom chosen COTS hardware. These devices would include Single Board Computer (SBC) designs in which the integrator would be responsible for choosing specific hardware components used in the final VoIP Terminal design. The integrator may also be responsible for any software integration including a SIP or H.323 VoIP software stack, voice codecs, and the selection or custom development of an IP Soft Phone application.

Some of the example Custom VoIP Device solutions discussed later in this section are PC/104 based. The PC/104 architecture is a compact version of the ISA (PC and PC/AT) bus. PC/104 modules are 8-bit or 16-bit, which correspond to the PC and PC/AT bus implementations respectively. PC/104 SBCs and PC/104 I/O Modules have a small form factor of approximately 3.6 x 3.8 inch (3.550" X 3.775"), and have a stackable design allowing PC/104 boards to be connected one on top of the other without the overhead of a backplane and card cage.

3.11.3 Circuit vs. Packet Switched Telephony Networks

To understand how VoIP Terminals work, we consider the difference between communications over the traditional circuit switched voice network vs. communication over a packet switched network. Although both circuit and packet based networks are able to carry voice data, they do so differently. These differences help to identify the requirements placed on VoIP Terminal devices.

3.11.3.1 Telephone Terminals in a Circuit Switched Network

The Public Switched Telephone Network (PSTN) is a circuit switched network. Figure 3-41 shows a typical path over which voice data could travel when two Telephone Terminals are connected in a call over a circuit switched network.

When a call is placed from Telephone A to a Telephone B over the PSTN, a path is chosen through the various telephone company switches and a physical circuit connection is established between the two endpoints. This circuit is maintained for the entire duration of the call. All voice data is carried full duplex over this circuit until the call is ended.

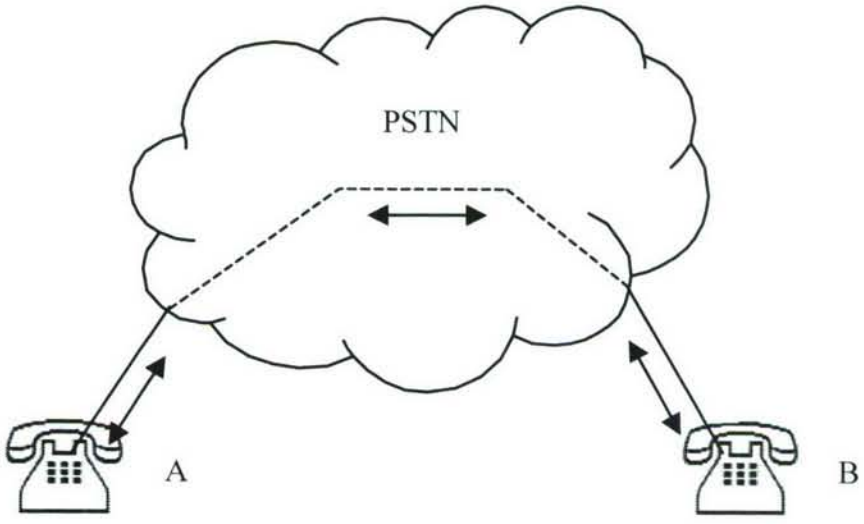


Figure 3-40. Call Data Routing in a Circuit Switched Network

3.11.3.2 VoIP Terminals in a Packet Switched Network

The Public IP Network is a packet switched network. Figure 3-40 shows the path that any individual packet of voice data may travel when two VoIP Terminals are connected in a VoIP call over a packet switched network.

When a call is placed from one VoIP Terminal to another VoIP Terminal over the Public IP Network, no distinct path exists, and there is no physical circuit connecting the endpoints. Voice data is sent as sampled packets of audio data over the network. Each packet in the network has a unique identifier and knows its own source and destination addresses. This allows the packets in a packet switched network to be routed independently. Multiple packets in a VoIP call may traverse the IP network over different routes.

The differences in call data routing over a circuit vs. packet switched network help to identify the basic requirements all VoIP Terminals must support for voice communication over an IP network. The next section discusses these requirements.

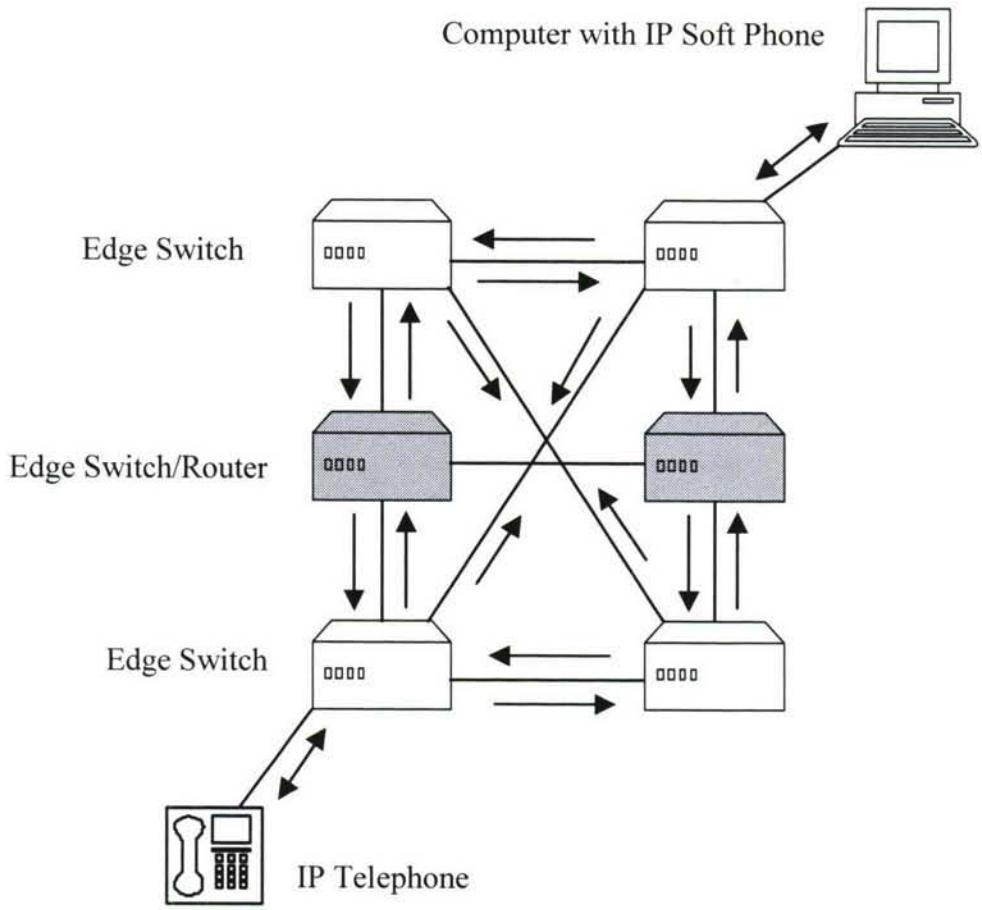


Figure 3-41. Call Data Routing in a Packet Switched Network

3.11.4 VoIP Terminal Requirements

As described in the previous section, audio data is routed differently over circuit and packet switched networks.

A Telephone Terminal operating in a circuit switched network environment works similar to a microphone and speaker. A user normally speaks into the telephone handset mouthpiece, and listens to a remote user through a telephone handset earpiece.

VoIP Terminals on the other hand must perform additional processing on all voice data it sends and receives. VoIP Terminals must be capable of sampling, compressing, and packetizing input voice data for transmission over the IP network. Additionally, VoIP Terminals must be able to receive packets of compressed voice data from the IP network, reassemble or reorder the voice data stream, uncompress the voice data and convert it to an analog signal for playback to the end user.

Figure 3-41 shows the process flow a VoIP Terminal must follow to send voice data over a packet switched network.

- The VoIP Terminal must be capable of sampling and digitizing an analog audio signal input.

- The VoIP Terminal must be able to compress the sampled audio, using a negotiated or agreed upon audio codec.
- The endpoint device must then be able to bundle the compressed audio in an IP packet, and send that packet over a high speed IP network to some remote destination address.

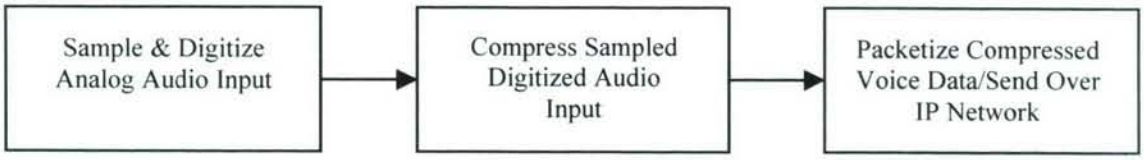


Figure 3-42. Send Voice Data Process Flow Diagram

Figure 3-42 shows the process flow a VoIP Terminal must follow to receive a voice data over a packet switched network.

- The VoIP Terminal must be capable of receiving IP packets containing compressed voice data from the network.
- The VoIP Terminal must re-assemble compressed voice data from IP packets into an ordered audio stream, and uncompress audio using the appropriate audio codec.
- The VoIP Terminal must convert the audio data to an analog signal and output the analog audio.

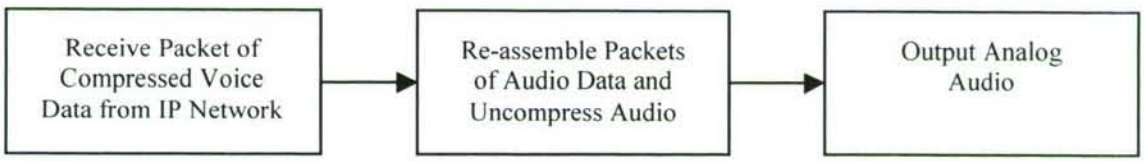


Figure 3-43. Receive Voice Data Process Flow Diagram

Since most VoIP Terminals are used for full duplex communication, a VoIP Terminal must be able to send and receive voice data over the IP network. The next section identifies the computer hardware components required to perform these operations.

3.11.5 VoIP Terminal Hardware

The requirements outlined above for sending and receiving voice data over an IP network require that VoIP Terminals be equipped with appropriate computer hardware. This hardware may include:

- **Display:** Some type of character or video graphics display for validation of user input as well as terminal setup and configuration. The display could also provide additional VoIP call information, or be used for other data processing tasks.
- **Input Device:** Some type of pointer device such as a mouse or touch screen, or a keypad/keyboard is needed for terminal configuration and VoIP Terminal operation.
- **Audio Device:** Some type of audio device, i.e. a sound card, for sampling user audio input and streaming audio output.

- **Processor:** Some type of host processor for device control and processing of audio codec algorithms for voice encoding/decoding.
- **Network Interface Device:** Some type of network interface device for transmitting and receiving packetized voice data over an IP network.

Although most VoIP Terminal devices will be equipped with the hardware components identified here, this is not true for all embedded VoIP devices. Some of the embedded solutions discussed in this section rely on a remote interface to provide certain functionality. Other devices may only need to support a subset of the hardware components identified.

Some embedded devices require no user interaction beyond device configuration. These devices may provide a software interface and rely on some type of serial or network interface for device configuration. A device equipped with a web server software interface could be configured from a remote computer through a web browser such as Windows Explorer or Netscape.

Embedded devices that only need to operate on voice data in half-duplex environment might require less computer processing power and network throughput. Additionally this type of device may only need to receive audio data and would have no requirement to sample an incoming analog audio signal for transmission.

3.11.5.1 Display Considerations

Although all embedded devices need to support some type of user interface for device configuration, not all are equipped with their own display device. These devices would use some type of serial or network connection for device configuration through a remote interface, i.e. another computer/computing device with display interface.

Most embedded devices capable of originating VoIP calls will have some type of display device for validation of remote addressing as well as general device control. The decision on the type of display an embedded device will support is often decided by some combination of cost, power, and size requirements.

Many of the stand alone embedded solutions, and some IC Phone designs, offer only small character based displays supporting only a few lines of fixed length text. Custom designs on the other hand can be fitted with full graphics based displays of various sizes and resolutions.

Things that might be considered when evaluating a particular embedded device's display capabilities might include:

- How many concurrent VoIP connections will the VoIP Terminal support?
- Does the VoIP Protocol support additional call information or advanced calling features?
- Will the VoIP Terminal be shared to support other data connections and/or applications?

3.11.5.2 Input Device Considerations

Although all embedded devices need to support some type of user interface for device configuration, not all are equipped with their own input device. These devices would use some type of serial or network interface for device configuration through a remote interface, i.e. another computer/computing device with input device.

Most embedded devices capable of originating VoIP calls will have some type of input device for data entry of remote address information. The input device could be a keypad, keyboard, mouse, touch screen, or some combination of these interfaces. In the case of ATAs, the attached analog phone device would provide the user input interface.

Many IC Phone designs only support a limited keypad input interface. Custom designs on the other hand can be fitted with all supported input devices including a combination of mouse, full keyboard, and touch screen. As is true with the decision on the type of display supported by an embedded device, the type of supported input device is often decided by some combination of cost, power, and size requirements.

Things that might be considered when evaluating a particular VoIP Terminal's user input capability might be:

- How easy or difficult is it to configure the VoIP Terminal?
- How many concurrent VoIP connections will the VoIP Terminal support?
- Does the VoIP Protocol support additional call information or advanced calling features?

3.11.5.3 Audio Device Considerations

All embedded devices will support some combination of user audio input and/or output. The audio input to an embedded device will normally be human voice, though it could be any analog audio signal. An audio device, i.e. soundcard, is used for audio input/output.

The audio device samples an input analog signal at some known frequency, and the sampled audio is converted to digital data through an Analog to Digital Converter (ADC). The resulting sampled digital data will be compressed and packetized before it can be transmitted over an IP network.

Similarly, the packetized audio data received over an IP network arrives in some compressed digital format. This compressed digital data must be uncompressed before it can be passed on to the VoIP Terminal's audio device. The audio device is responsible for converting the digital audio data to an analog signal for playback to the end user over a phone handset or speaker interface. The digital data is converted to an analog signal by the audio device through a Digital to Analog Converter (DAC).

Things that might be considered when evaluating a VoIP Terminal's audio device capabilities might be:

- How many concurrent VoIP connections will the embedded device support?
- How many active, i.e. not on hold, VoIP connections will the embedded device support?
- How many concurrent users will the embedded device support?
- Does the embedded device support hands free speakerphone operation?
- Will the analog audio input to and/or output from the embedded device the need to be amplified?

3.11.5.4 Processor Considerations

All embedded devices process data. The way that an embedded device processes data is directly related to the device's processor architecture. Tradeoffs in terms of speed, cost, and efficiency have led to different processor architectures.

Most Stand-Alone VoIP Devices use a combination of one or more Digital Signal Processors (DSP) along with some type of Central Processing Unit (CPU) or controller. This is also the case for many of the IC VoIP Device designs, while Custom VoIP Devices may be designed to work with or without DSPs.

DSPs are specialized computer processors that are designed to solve specific computational algorithms in real time. These algorithms typically have high computational requirements and tend to be processor intensive. Embedded device architectures that include DSPs will use these processors to perform codec operations, i.e. the compressing and uncompressing of digital voice data. They do so many times for cost savings since DSPs tend to be more cost effective than custom integrated circuits, and give embedded devices the performance needed for VoIP communication with a less powerful controller.

Since latency, or delay, is a major factor in VoIP Quality of Service (QoS), the task of compressing and uncompressing the digital voice data must be performed as close to real time as possible. DSPs are able to perform these tasks with little to no latency. DSPs often provide additional QoS functions including echo cancellation and gain control, and can be used to provide conferencing services.

Other processing tasks including system configuration as well as device interfacing are left to the main controller. Device interfacing tasks could include: input and output of voice data through audio device, co-ordination of audio data through DSP resources, and interface to IP network through network interface device.

Many Stand-Alone and IC Phone VoIP Devices are architected with slower less expensive CPUs. In these designs the codec processing is offloaded to one or more DSPs depending upon the number of supported active voice connections.

Alternatively, IP Softphones developed for Single Board Computer (SBC) architectures may use the SBC's host CPU for all processing tasks including codec processing. In these solutions the host CPU might be an Intel Pentium or similar speed processor.

Things that might be considered when evaluating a particular VoIP Terminal's processing capabilities might include:

- How many concurrent VoIP connections will the embedded device support?
- How many active, i.e. not on hold, VoIP connections will the embedded device support?
- How many concurrent users will the embedded device support?
- What codecs will the embedded device support?
- Will the embedded device need to support video either now or in the future?

3.11.5.5 Network Interface Device Considerations

VoIP Terminals must be equipped with some type of Network Interface Card (NIC) or adapter that supports the Internet Protocol (IP). Most Ethernet NICs today are 10/100 based, which means they can function on 10 and 100 Mbps networks. There are also 10/100/1000 based NICs that will additionally function on Gigabit networks. Although most NICs interface to the underlying network through copper wiring, some will also interface through fiber optic connections.

Consider the example where two VoIP Terminals are connected in a VoIP call each using a standard G.729 codec. By definition, standard G.729 voice data is processed and therefore transmitted at a rate of 8 Kbps. Assuming a full duplex connection, each VoIP Terminal would therefore need to transmit and receive 8 Kbps of voice data for a total throughput of 16 Kbps.

Clearly even in the 10 Mbps network environments there is plenty of throughput to support VoIP communications for single or multiple voice connections. Although the calculation above does not take into consideration protocol control packets, the overhead for these packets would be negligible.

Things to consider when evaluating a VoIP Terminal's networking capabilities, might be:

- What speed network will the embedded device will be connected to?
- Does NIC operate in full or half duplex?
- Does the embedded device need to be single or dual homed?
- Will the embedded device need to support video, either now or in the future?
- Will this embedded device be processing other network data?

3.11.6 Embedded Solution Categories

Here we examine representative embedded device solutions from each of the embedded design categories. The products identified here are described briefly with an emphasis placed on the required hardware components each includes to support VoIP communication.

3.11.6.1 COTS Stand-Alone VoIP Devices

3.11.6.1.1 Polycom, Inc., SoundPoint IP Family of IP Telephones

Website: http://www.polycom.com

Polycom, Inc. is a voice, video and networking company that develops and manufactures the SoundPoint IP family of IP telephone devices. Polycom's SoundPoint IP 300 series of phones are marketed as entry-level business IP telephone solutions, while the SoundPoint IP 600 series products are advertised as high-end feature rich IP telephone solutions.

- **Polycom SoundPoint IP 301**

  The SoundPoint IP 301 is a two-line desktop IP telephone marketed as a cost-effective business solution supporting core enterprise functionality. As a two-line IP telephone, it can be configured to support up to two line keys, i.e. phone numbers. Each line key can support multiple concurrent calls, but only one call can be active at any given time. All other calls must be placed on hold.

  The Soundpoint IP 301 comes equipped with the following hardware components:
  Display: Four line x 20 character monochrome LCD display.

  Input Device: Twelve button keypad supporting alpha, numeric, and special character input, 10 dedicated feature keys, and 3 context sensitive soft keys.

  Audio Device: Supports handset and hands free headset operation.

  Processor: Uses proprietary digital signal processors (DSP) for voice signal encoding/decoding.

  Network Interface: Two 10/100 Mbps Ethernet ports and embedded Ethernet switch. This allows a second Ethernet device to be connected to the IP network through the IP telephone. When a second Ethernet device is connected, the embedded Ethernet switch will give higher transmit priority to packets originating in the phone.

- **Polycom SoundPoint IP 601**

  The SoundPoint IP 601 is six-line desktop IP telephone, marketed as a high-end business solution supporting both core and advanced enterprise functionality. As a six-line IP telephone, it can be configured to support up to six line keys, i.e. phone numbers. Each line key can support multiple concurrent calls, but only one call can be active at any given time. All other calls must be placed on hold.

Optional SoundPoint IP Modules allow support for up to 12 IP phone lines, and offers advanced call-handling capabilities for voice attendant stations. In addition to its traditional telephone capabilities, the Soundpoint IP 601 also has limited network browser capabilities offering voice and data convergence.

The Soundpoint IP 601 comes equipped with the following hardware components:

Display: 320 x 160 pixel grayscale graphical LCD display.

Input Device: Twelve button keypad supporting alpha, numeric, and special character input, 18 dedicated feature keys, 4 context sensitive soft keys, and 6 display/menu navigation keys.

Audio Device: Supports handset, and headset devices, as well as full-duplex hands free speakerphone operation.

Processor: Uses proprietary digital signal processors (DSP) for voice signal encoding/decoding.

Network Interface: Two 10/100 Mbps Ethernet ports and embedded Ethernet switch. This allows a second Ethernet device to be connected to the IP network through the IP telephone. When a second Ethernet device is connected, the embedded Ethernet switch will give higher transmit priority to packets originating in the phone.

3.11.6.1.2 Cisco Systems, Inc., 180 Series Analog Telephone Adapters

Website: http://www.cisco.com

Cisco Systems, Inc. is a leading provider of computer networking equipment. The Cisco 180 Series of Analog Telephone Adapters (ATA) are handset-to-Ethernet adaptors allowing users to connect traditional analog telephone devices to IP networks for VoIP communication.

- **Cisco ATA 186**

The Cisco ATA 186 supports up to two analog telephones, each with their own telephone number.

The ATA 186 comes equipped with or has support for the following hardware components:

Display: Built in web server for remote configuration through web browser. Alternatively, the ATA can be configured in "Voice Configuration Mode" using an attached analog telephone.

A lighted function button on ATA allows a user to enter voice configuration mode. In this mode the user listens, through the attached telephone handset, to a series of voice prompts from the ATA, and responds with some combination touch-tone values through the telephone keypad. The lighted function button on the ATA, which is used to enter voice configuration mode, also provides visual feedback to the user to indicate the success of ATA voice configuration process.

Input Device: Uses attached touch-tone telephone keypad for remote address input, as well as device configuration when operating in "Voice Configuration Mode".

The lighted function button on ATA unit also acts as an input device allowing users to place the ATA in "Voice Configuration Mode" when the button is depressed.

Audio Device: Audio input through attached telephone handset, ADC processing handled by ATA device

Processor: Uses proprietary digital signal processors (DSP) for voice signal encoding/decoding.

Network Interface: One half-duplex 10 BaseT Ethernet port.

- **Cisco ATA 188**

The Cisco ATA 186 supports up to two analog telephones, each with their own telephone number.

The ATA 186 comes equipped with or has support for the following hardware components:

Display: Built in web server for remote configuration through web browser. Alternatively, the ATA can be configured in "Voice Configuration Mode" using an attached analog telephone.

A lighted function button on ATA allows a user to enter voice configuration mode. In this mode the user listens, through the attached telephone handset, to a series of voice prompts from the ATA, and responds with some combination touch-tone values through the telephone keypad. The lighted function button on the ATA, which is used to enter voice configuration mode, also provides visual feedback to the user to indicate the success of ATA voice configuration process.

Input Device: Uses attached touch-tone telephone keypad for remote address input, as well as device configuration when operating in "Voice Configuration Mode".

The lighted function button on ATA unit also acts as an input device allowing users to place the ATA in "Voice Configuration Mode" when the button is depressed.

Audio Device: Audio input through attached telephone handset, ADC processing handled by ATA device.

Processor: Uses proprietary digital signal processors (DSP) for voice signal encoding/decoding.

Network Interface: Two 10/100 BaseT Ethernet ports, with single shared uplink to 10/100 Mbps full-duplex network supporting the ATA 188 and a second Ethernet-capable device.

3.11.6.1.3 CyberData Corporation, VoIP Ceiling Speaker

Website: http://www.cyberdata.net

CyberData Corporation is an OEM firm that designs and manufactures peripheral devices for VoIP phone systems.

- **VoIP Ceiling Speaker**

  The VoIP Ceiling Speaker is a SIP-enabled, Power-over-Ethernet (PoE 802.3af) public address loudspeaker. The VoIP Ceiling Speaker is compatible with most SIP-based IP PBX servers that comply with SIP RFC 3261. The speaker is also capable of broadcasting audio sent over multicast IP addresses and port numbers.

The VoIP Ceiling Speaker comes equipped with or has support for the following hardware components:

Display: Built in web server for remote configuration through web browser.

Input Device: Built in web server for remote configuration through web browser.

Audio Device: Proprietary audio interface for DAC and audio output to speaker.

Processor: Atmel AT75C ARM-based Microcontroller with integrated OakDSPCore for voice signal decoding.

Network Interface: One 10/100 BaseT Ethernet port.

3.11.6.2 Integrated Circuit (IC) VoIP Devices

3.11.6.2.1 Texas Instruments, TNETV Family of VoIP System-On-Chip
Website: http://www.ti.com

Texas Instruments (TI) is a semiconductor company and leader in analog, and digital signal processing technologies. TI produces the TNETV Family of VoIP System-on-Chip designs that are used today by many IP Phone manufacturers as well as other third party integrators.

The TNETV Family includes the TNETV1050/1055 Integrated Circuit (IC) design, and the TNETV1051/1052/1053 IC design.

- **TNETV1050/1055**

  The TNETV1050/1055 IP Phone designs provide integrators with a complete hardware/software solution for developing IP Terminal devices. The TNETV1050/1055 design includes support for external peripherals, and has been integrated with TI's Telogy Software for IP Phone Applications.

The TNETV1050/1055 comes equipped with or has support for the following hardware components:

Display: Integrated support for a 16-bit color LCD display.

Input Device: Integrated Support for an 8x8 keypad interface.

Audio Device: Two ADCs with support for up to 5 programmable inputs, and two DACs with four programmable outputs.

Processor: Programmable TMS320C55x DSP *(running at 125 MHz on TNETV1050, and 100 MHz on TNETV1055)*, with MIPS32 4KEc Reduced Instruction Set Computer (RISC) Processor *(running at 165 MHz on TNETV1050, and 125 MHz on TNETV1055)*.

Network Interface: Integrated support for a three-port line rate internal Ethernet Switch, with dual Media Access Controllers (MAC) and Physical Layer (PHY) for IP Phone and PC connectivity.

- **TNETV1051/1052/1053**

The TNETV1051/1052/1053 IP Phone designs provide integrators with a complete hardware/software solution for developing IP Terminal devices. Like the TNETV1050/1055 design, the TNETV1051/1052/1053 platforms include support for external peripherals, and have been integrated with TI's Telogy Software for IP Phone Applications.

The TNETV1051/1052/1053 series of VoIP System-On-Chip designs offer increased processing speeds over the TNETV1050/1055 series design. Additionally the TNETV1051/1052/1053 is designed to offer greater Ethernet throughput with support for Gigabit Ethernet connections.

The TNETV1051/1052/1053 comes equipped with or has support for the following hardware components:

Display: Integrated support for a 16-bit color LCD display.

Input Device: Integrated Support for an 8x8 keypad interface.

Audio Device: Two ADCs with support for up to 5 programmable inputs, and two DACs with 4 programmable outputs.

Processor: Programmable TMS320C55x DSP *(running at 150 MHz)*, with dual core MIPS32 24KEc Reduced Instruction Set Computer (RISC) Processor *(running at 300 MHz)*.

Network Interface: Integrated support for two 10/100/Gigabit Ethernet media access controllers (MAC) via three Gigabit Ethernet ports. *(TNETV1051 offers two 10/100 Ethernet PHYs for cost savings when gigabit technology is not required).*

3.11.6.2.2 Infineon Technologies AG, INCA-IP line of VoIP chipsets

Website: http://www.infineon.com

Infineon Technologies manufactures a line of VoIP chipsets designed to integrate IP phone support hardware into a single IC.

- **INCA-IPc**

  Infineon Technologies markets the INCA-IPc as a single-chip cost-optimized solution for VoIP terminals.

  The INCA-IPc comes equipped with or has support for the following hardware components:

  Display: I^2C Bus Interface for control of character based LED/LCD displays. Additionally the INCA-IPc has support for up to 20 LEDs.

  Input Device: Provides keypad scanner interface supporting keyboard/keypad peripheral of up to 36 keys.

  Audio Device: Proprietary Analog Front End (AFE) interface to three differential inputs/outputs providing audio interface for speakerphone, handset and headset.

  Processor: Proprietary processor design incorporating a 32-bit MIPS RISC CPU core running at 100 MHz, with a 16-bit fixed point DSP running at 100 MHz for voice processing.

  Network Interface: One 10/100 BaseT Ethernet MAC and PHY interface, and and optional Reduced Media Independent Interface (RMII) interface. Supports full and half-duplex modes, as well as QoS through voice packet prioritization (SIP RFC 802.1p) and Virtual LAN (VLAN) operation (SIP RFC 802.1Q).

- **INCA-IPs**

Infineon Technologies also markets the INCA-IPs as a single-chip cost-optimized solution for VoIP terminals. The INCA-IPs integrates additional interfaces, and has additional feature support over the INCA-IPs.

The INCA-IPs comes equipped with or has support for the following hardware components:

Display: I^2C Bus Interface for control of character based LED/LCD displays. Additionally the INCA-IPs has support for up to 24 LEDs.

Input Device: Provides keypad scanner interface supporting keyboard/keypad peripheral of up to 91 keys.

Audio Device: Proprietary Analog Front End (AFE) interface to three differential inputs/outputs providing audio interface for speakerphone, handset and headset.

Processor: Proprietary processor design incorporating a 32-bit MIPS RISC CPU core running at 150 MHz, with a 16-bit fixed point DSP running at 100 MHz for voice processing.

Network Interface: Two 10/100 BaseT Ethernet MAC and PHY interfaces and optional RMII interface. Embedded three port Ethernet switch for INCA-IPs and PC connectivity. Supports full and half-duplex modes, as well as QoS through voice packet prioritization (SIP RFC 802.1p) and Virtual LAN (VLAN) operation (SIP RFC 802.1Q).

- **INCA-IP2**

The INCA-IP2 is Infineon Technologies' second generation of IP Phone terminal chips. The INCA-IP2 has additional processing power, support for video, and higher throughput Ethernet capabilities.

The INCA-IP2 comes equipped with or has support for the following hardware components:

Display: Support for character and video based displays.

Input Device: Provides keypad scanner interface supporting keyboard/keypad peripheral of up to 91 keys.

Audio Device: Proprietary Analog Front End (AFE) interface to three differential inputs/outputs providing audio interface for speakerphone, handset and headset. Includes two DAC and ADCs for additional audio processing support.

Processor: Proprietary design consisting of two 400 MHz MIPS 24KEc processors. One processor acts as the INCA-IP2's CPU, while the second is dedicated for voice and video processing.

Network Interface: Two 10/100 BaseT Ethernet MAC and PHY interfaces with embedded three port Gigabit Ethernet switch for INCA-IP2 and PC connectivity. Interface support for two Gigabit Media Access Controllers (GMAC) and Reduced Gigabit Media Independent Interface (RGMII) for optional connection of Gigabit Physical (GPHY) Ethernet connectors. Support for QoS through voice packet prioritization (SIP RFC 802.1p) and Virtual LAN (VLAN) operation (SIP RFC 802.1Q).

3.11.6.3 COTS Custom VoIP Devices

3.11.6.3.1 Signalogic PC/104 DSP/Telecom/Data Acquisition Boards

Signalogic is a computer hardware/software company that develops, manufactures and markets OEM and off-the-shelf embedded systems for voice, and video, and wireless technologies.

Signalogic develops a line of PC/104 DSP/Telecom/Data Acquisition boards that can be used to produce custom VoIP solutions. These boards offer a modular design and can be fitted with up to four Signalogic SigSD4/SD8 SODIMM analog input modules, and SigC54/C55xx-SIMM processor modules for customized VoIP solutions.

- **SigC54/55xx-PC/104**

The SigC54xx and SigC55xx board are fully compliant with the PC/104 specification v2.3 in terms of mechanical considerations and dimensions. Their modular design offers integrators and developers a scalable solution for channel capacity and processing power.

Display: Requires integration with third party PC/104 SBC.

Input Device: Requires integration with third party PC/104 SBC.

Audio Device: Accepts SigSD4 and SigSD8 SODIMM analog input modules capable of supporting up to four and eight lines of analog I/O respectively. Integrated support for single or quad T1/E1 interface.

Processor: Accepts up to SigC54xx and Sig55xx SIMM modules. These modules each contain six Texas Instruments C54xx or C55xx DSPs respectively with 128k x16 (or 256k x16) SRAM devices. *(Requires SBC with host CPU).*

Network Interface: Integrated support for a 10/100 Mbps Ethernet controller.

- **SigC67-PC/104**

Like the The SigC54xx and SigC55xx boards, the SigC67 design is fully compliant with the PC/104 specification v2.3 in terms of mechanical considerations and dimensions. Its modular design offers integrators and developers a scalable solution for channel capacity and processing power.

Display: Requires integration with third party PC/104 SBC.

Input Device: Requires integration with third party PC/104 SBC.

Audio Device: Accepts SigSD4 SODIMM analog input modules capable of supporting up to four lines of analog I/O. Integrated support for single or quad T1/E1 interface.

Processor: Accepts SigC67xx 32-bit floating point SODIMM modules. These modules each contain four Texas Instruments C67xx DSPs with four 4M x32 SDRAM devices. *(Requires SBC with host CPU).*

Network Interface: Integrated support for a 10/100 Mbps Ethernet controller.

3.11.6.3.2 Adaptive Digital Technologies, Inc., ipPhoneChip
Website: http://www.adaptivedigital.com

Adaptive Digital Technologies, Inc., develops and licenses DSP algorithms and solutions for telephony, audio, and video applications including VoIP.

- **IpPhoneChip**

The IpPhoneChip is a scalable IP phone DSP software solution for turning a TI TMS320C5000 family DSP into an easily controlled IP phone engine. The IpPhoneChip API provides developers with a software interface for performing audio I/O, echo cancellation, gain control, tone generation, conferencing, voice coding/decoding, and packetization. The IpPhoneChip must be interfaced with some host processor or CPU for building custom embedded VoIP devices.

The IpPhoneChip comes equipped with or has support for the following hardware components:

Display: Provided by Host Computer.

Input Device: Provided by Host Computer.

Audio Device: Provided by Host Computer. IpPhoneChip interfaces to audio device through the IpPhoneChip API and low level firmware.

Processor: Scalable DSP architecture with the TI TMS320C5000 family of DSPs. Requires third party host control processor or CPU.

Network Interface: Provided by Host Computer.

3.11.6.3.3 R.L.C. Enterprises, Inc., XScale-Extreme

Website: http://www.rlc.com

R.L.C. Enterprises, Inc. designs and manufactures Embedded Single Board Computers, Controllers, and related I/O products for the embedded control market.

- **XScale-Extreme**

  The XScale-Extreme is a SBC design with included Color LCD display directly mounted to the SBC, and comes loaded with the Microsoft Windows CE 6.0 Operating System (OS) and fully supports application development with the Microsoft Visual Studio 2005 Interactive Development Enviroment (IDE).

  Display: Built in LCD controller interface. Comes with a mounted 6.5 inch Color LCD.

  Input Device: Touch screen display. Support for mouse/other pointer device through USB, or RS-232 serial interfaces.

  Audio Device: Processor: Intel XScale PXA270 Processor with 520 MHz CPU.

  Network Interface: Optional XScale-Ethernet Expansion Module provides one 10/100 compatible Ethernet port. Operates in full-duplex with a maximum transmit rate of 750 kbps, and a maximum receive rate of 1,929 kbps.

This page intentionally left blank.

3.12 End Devices

There are multiple End Devices used to meet the communications requirements of a naval vessel including standard devises in various configurations or form factors and specialized end devices customized to meet specific requirements. These include Integrated Communication Terminals (ICT), Dial Telephones, Emergency Phone, Lockout Trunk Interface Unit, and Speakers, or similar devices under different names depending on the specific vessel. The following sections will explain a sampling of them and then show a derived baseline for the end devices. The requirements were drawn from the many different vessel specifications that were reviewed for the project. The requirements that were taken will give common features that relate to the end device and its relationship to VoIP. Requirements that would not change or vary the design or were redundant to other ones were left out to keep this section to a manageable size. Two columns were added to the requirements, "Current Implementation" and "VoIP Implementation"; this shows how it was done related to how is will change or not change relative to a VoIP implementation.

3.12.1 Integrated Communications Terminal (ICT)

The ICTs are packaged in various configurations: The configurations of the end devices are functionally the same but present physical differences to meet specific ship's installation requirements and also to address devices requiring the additional functionality of the General Alarm Switch (GA switch) requirement.

List of typical ICTs are as follows:

- Bulkhead mount unit with and without General Alarm switch
- Console mount unit with and without General Alarm switch
- Portable unit.
- Remote ICT display panel with and without General Alarm switch

3.12.1.1 Bulkhead Mount

This version of the ICT is for mounting on vertical bulkheads or similar structures. These units are located throughout a vessel as per the ship's plan. The electronics are housed within an enclosure providing environmental and EMI integrity. The housing also provides holes for mounting hardware and connectors for ship's wiring. The bulkhead mount ICT operation is common to all ICTs. Refer to the Figure 3-44 for a view of the bulkhead mount ICT. Figure 3-45 shows a General Alarm Switch as part of the ICT with an attachment providing the general alarm activation and cancel feature. This feature is provided at specific stations according to the ship's plan. The attachment consists of a small enclosure with a general alarm and cancel switch. A collar, extending above the switch to prevent accidental activation, protects the general alarm switch.

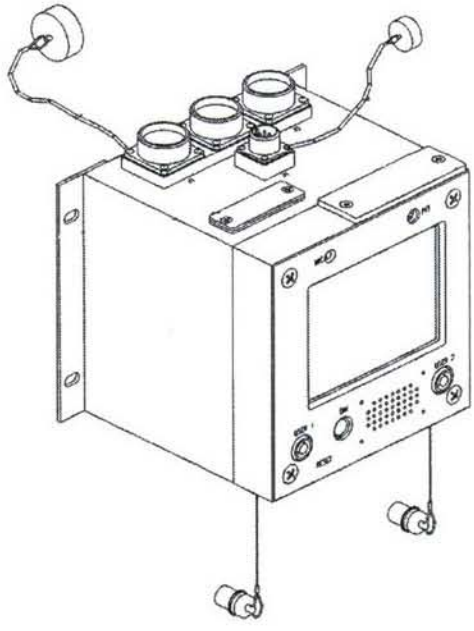


Figure 3-44. ICT, Bulkhead Mount, (no alarm)

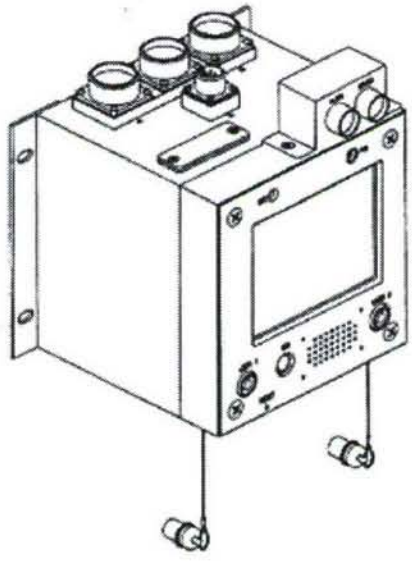


Figure 3-45. ICT Bulkhead Mount with General Alarm Switch

3.12.1.2 Console Mount

An alternate version of the ICT is designed for installation within a console. This form factor is defined by the ship's plan. Any variation from this size would make retrofitting of systems an issue. These units are located throughout the vessel as per the ship's plan. When mounted in a well provided in the console, the front panel is flush with the console surface. Connections are made to the rear plate of the units. The console mount ICT operation is common to all ICTs.

Refer to the following Figure 3-46 for a view of the console mount ICT. This console version can also come with an alarm and would be similar to the mounted ICT.

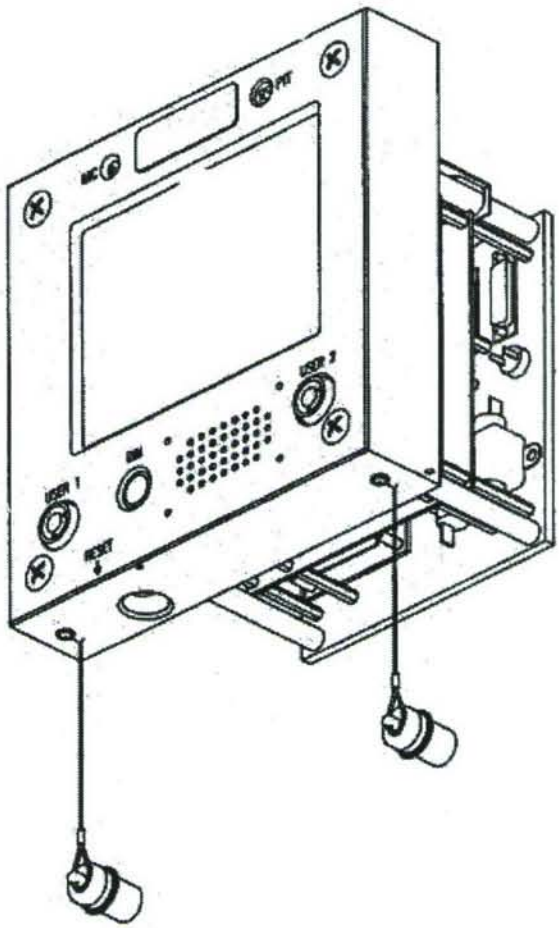


Figure 3- 46. Console Mount

3.12.1.3 Derived Baseline For ICT

The following Table 3-25 provides a derived baseline for the ICT. The baseline lists the functions and capabilities by functional subheadings that relate to the VoIP implementation.
A number of items are not affected by the VoIP implementation and changing from the current implementation to VoIP will have no impact on the system. These features are identified under the VoIP implementation column with the following comment "This feature not affected with VoIP implementation, use current design".

Table 3-25. Derived Baseline for ICT

General Communication	Current Implementation	VoIP Implementation
Monitors Multiple and Simultaneous Telephony and Radio Calls	The ICT uses a proprietary circuit board to handle the audio and mix it as required	SIP does not define the implementation. The sound card will be required that can handle multiple audio inputs and outputs and be able to mix the streams, as required.
Monitors Four Active Calls, Minimum, Between the Host Telephony Unit and the RCS	The ICT uses a proprietary audio device to collect and mix the audio signal from the PBX and RCS.	The source will come in as IP packets and be converted to audio that the sound card will process and mix, as required.
Allows Simultaneous Active Calls to the Host Telephony Unit and the TVS	The ICT brings in the telephony through BRIs.	SIP is a packet-based technology. The design can use VLANs, VPN or dual homed connections to the network to connect to the different switches and RCS.
Overrides Transmission to the Supervisor Jack from the User Jack Muting the User Microphone when the Supervisor PTT Footswitch is Active	Coded into the interface	This feature not effected with VoIP implementation; use current design.
Uses Commercial Standards and Protocols for Telephone and Radio Calls (Using the TVS)	The current design uses BRI for the connection to the switch, RCS and TVS	The protocol will be SIP for the telephony connections. The RCS connection will be converted to SIP by a media gateway, as required.

Intercom Communication	Current Implementation	VoIP Implementation
Provides Two-Way Intercom Calling Function	Designed into the software and supported by the BRI	The PBX and the ICT will need to support draft-ietf-sip-answermode-04 that addresses Intercom Calls.
Intercom Call Emulates Two-Way LS-518/SIC and LS-519/SIC MC Announcing Circuits	Designed into the software	This feature not effected with VoIP implementation, use current design.
Transmits Intercom Calls to Another ICT	Designed into the software and configuration in the switch	The ICT will need to have the Class of Service (CoS), to allow it to generate Intercom Calls.
Transmits Intercom Calls Using the Internal Loudspeaker, Microphone, and PTT Switch	Designed into the software and configuration in the switch	The ICT will need to have the CoS to allow it to generate Intercom Calls.
Radio Communication	**Current Implementation**	**VoIP Implementation**
Initiates Radio Calls Similarly to Telephone and Intercom Calls	Radio Calls initiated through the BRI using two channels	Radio calls will be initiated same as all calls and routed to a media gateway interface.
Allows Two Distinct Radio Calls, Minimum (Using the TVS)	Depending on the vendor's product if this is a limitation	Because of the method described above, this will not be an issue.
Allows Four Radio Calls Determined by Watchstation Requirements (Using the TVS)	Depending on the vendor's product if this is a limitation	Because of the method described above, this will not be an issue.
Initiates and Transmits Radio Calls	Done through the BRI	The media gateway must understand the radio interface, i.e., Raytheon ARA-1.
Transmits a Single Radio Call Exclusively	Designed into the software	Designed into the software
Transmits a Single-Connected Radio Call Using an Accessory Handset or Headset and a PTT Footswitch	Designed into the hardware	RFC 4354, is one of the specifications, as well as several drafts, that need to be consulted for the PTT functionality to be implemented.
Integrates Exterior Radio Communications	Done through the BRI	The media gateway must understand the radio interface,i.e., Raytheon ARA-1.

Telephony Communication	Current Implementation	VoIP Implementation
Allows Four Distinct Telephony Calls Minimum	Designed into the software and supported by the BRI	SIP will allow multiple calls at a single time. The audio device will also need to support it by mixing the audio streams, as required.
Initiates, Receives, and Transmits Telephony Calls	Designed into the software and supported by the BRI	SIP allows the initiation, receiving and transmitting of calls.
Transmits and Receives Telephony Calls Using an Accessory Handset or Headset	Designed into the hardware	This feature not effected with VoIP implementation; use current design.
Transmit a Single Telephony Call Exclusively	Designed into the software and supported by the BRI	SIP will allow single or multiple calls to be processed.
Transmits Multiple Telephony Calls Simultaneously	Designed into the software and supported by the BRI	SIP will allow single or multiple calls to be processed.
Provides Commercial Interface for Telephony Calls	BRI	SIP signaling protocol IP infrastructure
Integrates Interior Vital, Tactical, and Administrative Communications	PBX design	IP-PBX can handle multiple trunks and end devices. With the use of a media gateway it can be integrated with multiple telephony switches and devices.

Radio Compatibility	**Current Implementation**	**VoIP Implementation**
Compatible with the RCS	BRI/Interface	Media Gateway, i.e., Raytheon ARA-1.
Compatible with All Radio User Functions	BRI/Interface	Media Gateway, i.e., Raytheon ARA-1.
Compatible with Radio Connectivity Signaling Requirements	BRI/Interface	Media Gateway, i.e., Raytheon ARA-1.
Compatible with Radio Encryption Equipment Control Signaling Requirements	BRI/Interface	Media Gateway- Interface for signaling will need to be determined.
Compatible with Radio Voice Signaling Requirements	BRI/Interface	Media Gateway, i.e., Raytheon ARA-1.
Telephony Compatibility	**Current Implementation**	**VoIP Implementation**
Compatible with the Host Telephony Unit	BRI/Interface	VoIP solution required on both ends. The use of a media gateway if required to connect to a BRI device.
Compatible with Commercial Telephony Standards for User Operation	Designed into the software	This feature not effected with VoIP implementation; use current design.

TVS Compatibility	Current Implementation	VoIP Implementation
Compatible with Required TVS User Features	Software design	SIP features must support the high level features. See SIP Feasibility section for more details.
Compatible with TVS Signaling Requirements	BRI/Interface	Depends on if the TVS solution will be an IP packet based system. If not, a media gateway will need to be defined for the protocol of the TVS solution..
General Connection	**Current Implementation**	**VoIP Implementation**
Provides Shipboard Approved Commercial Standard Connectors	Hardware design	This feature not effected with VoIP implementation; use current design.
Provides Connectors for External PTT Footswitches	Hardware design	This feature not effected with VoIP implementation; use current design.
Provides PTT Footswitch Connector Controlling the User Jack Microphone State	Hardware design	This feature not effected with VoIP implementation; use current design.
Provides Connectors for a Profile Storage Device	Hardware design	This feature not effected with VoIP implementation; use current design.
Does Not Provide Dual-Homed to Separate Node Room Host Telephony Units	Hardware design	This feature not effected with VoIP implementation; use current design.
Does Not Provide Physical or Virtual Data Connections to a Separate Data Network Outside the Host Telephony Unit or the TVS	Hardware design	The network can be either converged or not. See the section on security.

Audio Connection	**Current Implementation**	**VoIP Implementation**
Provides Two Front Panel User Jacks for Accessory Handsets or Headsets	Hardware design	The hardware will be required to support multiple active calls at once.
Provides Jacks that Accept a Commercial Cord with an Overall Shield and a Separate Shield for the Microphone Leads	Hardware design	This feature not effected with VoIP implementation; use current design.
Provides One Jack Labeled "USER" for the User and One Jack Labeled "SUPERVISOR" or "USER 2" for the Supervisor	Hardware design	This feature not effected with VoIP implementation; use current design.
Provides Connectors for External Loudspeakers	Hardware design	This feature not effected with VoIP implementation; use current design.
Provides External Chassis Connector Allowing Remote Loudspeaker Radio Call Monitoring	Hardware design	This feature not effected with VoIP implementation; use current design.
Data Connection	**Current Implementation**	**VoIP Implementation**
Does Not Provide Segregated Data Connections	Hardware design	The network can be implemented as a converged. Review section on security.
Power Connection	**Current Implementation**	**VoIP Implementation**
Provides Two connectors for 48 VDC Power from Separate Node Room Host Telephony Units, Minimum	Hardware design	This feature not effected with VoIP implementation; use current design. The ability to be powered by PoE is questionable because of the display power required.

Radio Connection	**Current Implementation**	**VoIP Implementation**
Provides Separate Connector for Physical Radio Signaling Segregation	Hardware design	Separate LAN connections can be done or converged network. See security section.
Provides Connectors for Two Radio Calls, Minimum	Designed into the software and supported by the BRI	SIP will allow single or multiple active calls to be processed. This will require a SIP stack that supports it.
Provides Connectors for Four Radio Calls to Applicable C2 Supervisor Watch stations	Designed into the software and supported by the BRI	SIP will allow single or multiple active calls to be processed. This will require a SIP stack that supports it.
Provides Two Connectors for Radio Call Signaling, Minimum	Designed into the software and supported by the BRI	Number of connections is determined with the method of security used and the media gateway.
Telephony Connection	**Current Implementation**	**VoIP Implementation**
Provides Separate Connector for Physical Telephony Signaling Segregation	Hardware design	Separate LAN connections can be done or converged network. See the security section.
Provides Connectors for Four Telephony Calls, Minimum	Designed into the software and supported by the BRI	SIP will allow single or multiple active calls to be processed. This will require a SIP stack that supports it.
Provides Two Connectors for Call Signaling from Separate Node Room Host Telephony Units, Minimum	Designed into the software and supported by the BRI	SIP runs on the IP-network backbone, so the location or separation of redundant IP-PBX does not matter. Dual home from multiple network switches needs to be supported for resilience. See security section.

TVS Connection	**Current Implementation**	**VoIP Implementation**
Connects Directly to the TVS	Designed into the software and supported by the BRI	SIP runs on the IP-network backbone, so the location or separation of redundant IP-PBX does not matter. Dual home from multiple network switches needs to be supported for resilience.
Unit Display	**Current Implementation**	**VoIP Implementation**
Bold and Contrasting Display between Telephony Calls and Radio Calls	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Bold and Contrasting Display between Telephone Calls and Intercom Calls	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Bold and Contrasting Display of Each Active Call Operation Mode	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Bold and Contrasting Display of the Presence of Encrypted Voice Messages Received Off-Ship (Detect) that Remains Illuminated until Encrypted Voice Messages are not Detected	Hardware/Software design	A method of determining if encrypted will need to be determined. This may require a separate protocol that will handle this messaging stream, such as SOAP.
Displays the Active Call Status on All Single Button Activation Calling Screens	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Displays the Active Call Status on the Keypad Screen	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Displays the Active Call Endpoint	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Displays the Caller ID Station Name	Hardware/Software design	Caller ID, is supported with in SIP, the ICT will need to display it. RFC 2543bis defines the method used to define it in the SIP header

Unit Display	**Current Implementation**	**VoIP Implementation**
Displays the Caller ID Dialed Number of Active Calls to Interface Trunks	Hardware/Software design	Caller ID is supported in SIP The ICT will need to display it. RFC 2543bis defines the method used to define Caller ID in the SIP header.
Displays the Caller ID Dialed Number if the Station Name is not Available	Hardware/Software design	Caller ID, is supported with in SIP, the ICT will need to display it. RFC 2543bis defines the method used to define it in the SIP header.
Provides Single Button Activation Calling Screen	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides Keypad Screen with Standard Telephony Keypad Functions	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides User Configuration Screen For Selecting which Active Connection is Left, Right, and Left and Right when Binaural Headset Output is Selected as Left/Right	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Audio Interface	**Current Implementation**	**VoIP Implementation**
Accepts a Single-User Handset or Headset with Single-Action Select-and-Talk	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Accepts Binaural Accessory Headsets	Hardware/Software design	Hardware will need to support it, as well as the SIP stack.
Accepts External Loudspeakers	Hardware/Software design	Hardware will need to support it as well, as the SIP stack.

Power Interface	Current Implementation	VoIP Implementation
Accepts Power from Either Node Room Host Telephony Unit Connection	Hardware design	VoIP runs on the IP-network. The ability to be powered by PoE is questionable because of the display power required. A distribution system will need to be defined for devices that exceed the 15W power of PoE.

Radio Interface	Current Implementation	VoIP Implementation
Provides Segregated Radio Interface (Using the TVS)	Hardware design	SIP runs on the IP-network backbone. Dual home from multiple network switches needs to be supported. See the security section.
Telephony Interface	**Current Implementation**	**VoIP Implementation**
Provides Segregated Telephony Interface	Hardware design	SIP runs on the IP-network backbone. Dual home from multi network switches needs to be supported. See the security section.

User Interface	Current Implementation	VoIP Implementation
Provides Touch Screen Display	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides Internal PTT Switch	Hardware/Software design	RFC 4354 is one of the specifications, as well as several drafts, that need to be consulted for the PTT functionality to be implemented.
Accepts PTT Footswitches	Hardware/Software design	RFC 4354, is one of the specifications, as well as several drafts, that need to be consulted for the PTT functionality to be implemented.
Provides Single Button Activation Calling Virtual Button for Telephone Calls	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides Single Button Activation Calling Virtual Button for Intercom Calls	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides Single Button Activation Calling Virtual Button for Radio Calls	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides 48 Single Button Activation Calling Virtual Buttons Minimum	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides User Control Muting or Activating the Internal Loudspeaker During Telephone Calls	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides User Control Muting or Activating an External Loudspeaker During Radio Calls	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides Virtual Button Switching a Call between Transmit Mode and Monitor-Only (Mute) Mode	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides Virtual Button Placing a Radio Call in Cipher (Encrypted) Mode	Hardware/Software design	A method of determining if encrypted will need to be determined. This may require a separate protocol that will handle this messaging stream, such as SOAP.
Provides Virtual Button Placing a Radio Call in Plain (Unencrypted) Mode	Hardware/Software design	This feature not effected with VoIP implementation; use current design.

User Interface	Current Implementation	VoIP Implementation
Provides User Level Ability to Archive a Profile After Making Changes	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
General Operation		
Able to Transfer the Screen Configuration and Watch Station Profile to Another ICT for Automatic Reconfiguration of a Replacement	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Uses Shipboard Compatible Commercial Standards and Protocols for Telephony and Radio Interface Signaling (Using the TVS)	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Does Not Modify Host Telephony Unit Software to Accommodate Caller ID	Hardware/Software design	Caller ID is supported in SIP. The ICT will need to display it. RFC 2543bis defines the method used to define it in the SIP header.
Does Not Use an In-Circuit Ship's Data Network for Profile Transferring, Loading, or Archiving	Hardware/Software design	VoIP runs on the IP-network, It can be a converged network or a segregated one, depending on the security requirements. See the security section.

Audio Operation	Current Implementation	VoIP Implementation
Allows Both Intercom Call Parties to Transfer an Intercom Call to an Accessory Handset or Headset	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides Internal Microphone and Loudspeaker	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Enables the Internal Microphone for Intercom Calls	Hardware/Software design	The auto answer draft "draft-ietf-sip-answermode-04" allows for this type of operation. ICT and IP-PBX will need to support it.
Allows the User to Reply to an Intercom Call by Speaking into the Internal Microphone	Hardware/Software design	The auto answer draft "draft-ietf-sip-answermode-04" allows for this type of operation. ICT and IP-PBX will need to support it.
Allows Binaural Headset Output as Left/Right or Monitor/Transmit	Hardware/Software design	The hardware, as well as the SIP stack, will need to support the multiple active calls at once.
Ensures Active Calls in Transmit Mode are on One Side and Channels in Monitor-Only (Mute) Mode are on the Other Side when Binaural Headset Output is Selected as Monitor/Transmit	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Allows the User to Listen to Telephone and Intercom Calls with the Internal Loudspeaker	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Enables the Internal Loudspeaker when an Incoming Intercom Call is Received	Hardware/Software design	The auto answer draft "draft-ietf-sip-answermode-04" allows for this type of operation. May require added parameter into the INVITE request to point it to a set output device. ICT and IP-PBX will need to support it.
Mutes the Internal Loudspeaker when the Internal PTT Switch Enabling the Internal Microphone is Active for Intercom Calls	Hardware/Software design	This feature not effected with VoIP implementation; use current design.

Intercom Operation	Current Implementation	VoIP Implementation
Provides Auto-Answer For Incoming Intercom Call	Hardware/Software design	The auto answer draft "draft-ietf-sip-answermode-04" allows for this type of operation. ICT and IP-PBX will need to support it.
Allows the Calling or Called ICT to Initiate Intercom Calls by Placing the Active Connection On-Hook	Hardware/Software design	The auto answer draft "draft-ietf-sip-answermode-04" allows for this type of operation. May require added parameter into the INVITE request to point it to a set output device. ICT and IP-PBX will need to support it.
Enables the Internal PTT Switch for Intercom Calls	Hardware/Software design	RFC 4354 is one of the specifications, as well as several drafts, that need to be consulted for the PTT functionality to be implemented.
Radio Operation	**Current Implementation**	**VoIP Implementation**
Places All Existing Telephony and Radio Calls in Monitor-Only (Mute) Mode when a Radio Call is Initiated	Hardware/Software design	The ICT will need to know that it is a radio call passing through a media gateway.
Enables a PTT Footswitch for Radio Calls	Hardware/Software design	The ICT will need to know that it is a radio call passing through a media gateway. RFC 4354 is one of the specifications, as well as several drafts, that need to be consulted for the PTT functionality to be implemented.
Does Not Use VOX for Active PTT Radio Signaling	Hardware/Software design	The media gateway will need to support this type of actuation of the radio signal
Does Not Support or Initiate Radio Call Redundancy when in Use or in Stand-by with Another ICT	Hardware/Software design	This feature not effected with VoIP implementation; use current design.

Secure Operation	Current Implementation	VoIP Implementation
TEMPEST Certified to Pass Non-Secure Communications to the Host Telephony Unit and Secure Communications to the TVS	Hardware/Software design	This is covered in the Security section of this report. Certification will need to be sought for the new VoIP designs.
Storage Operation	**Current Implementation**	**VoIP Implementation**
Stores the Call Type, Station Name, and Dial Number into a Single Button Activation Calling Virtual Button	Hardware/Software design	This feature not effected with VoIP implementation, use current design.
Stores All Shipset ICT Profiles	Hardware/Software design	The ICT will be on an IP-network, and will get configuration files from a configuration server. A feature to push profiles will need to be added to devices that can change their own profiles.
Preserves the Single Button Activation Calling Configuration During Power Loss and Shutdown	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Telephony Operation	**Current Implementation**	**VoIP Implementation**
Places All Existing Telephony and Radio Calls in Monitor-Only (Mute) Mode when an Active Telephony Call is Initiated	Hardware/Software design	This is supported by SIP and requires the software to manage the resources.
Allows Calling Party Termination of an Active Telephony Call to Force the Called Party On-Hook	Hardware/Software design	This is defined in the RFC 3261 specification.
Allows Called Party Termination of an Active Telephony Call to Force the Calling Party On-Hook	Hardware/Software design	This is defined in the RFC 3261 specification.
Manages Basic Telephony Features	Hardware/Software design	This is defined in the RFC 3261 specification.
Does Not Support or Initiate Telephony Call Redundancy when in Use or in Stand-by with Another ICT	Hardware/Software design	This is defined in the RFC 3261 specification.
Is Not Configured in the Host Telephony Unit to Access Pier Shorelines or the ADNS	Defined in the Class of Service	Defined in the Class of Service

Power Consumption	**Current Implementation**	**VoIP Implementation**
Power Consumption of 40 W (Objective) to 50 W (Threshold)	Hardware design	Hardware design – This load is too high for PoE, powering (15W).
Primary Power	**Current Implementation**	**VoIP Implementation**
Accepts a 48 VDC Primary Power Source	Hardware design	If multiple network connections are used, then the sum of the PoE may be able to be used. This will need to be tested in the lab.
Secondary Power	**Current Implementation**	**VoIP Implementation**
Accepts a 48 VDC Secondary Power Source	Hardware design	If multiple network connections are used, then the sum of the PoE may be able to be used. This will need to be tested in the lab.
Unit Reliability	**Current Implementation**	**VoIP Implementation**
Operates During All Ship Conditions and Operations	Hardware/Software design	This feature not effected with VoIP implementation; use current design.
Provides O-Level Maintenance Philosophy	Hardware/Software design	This feature not effected with VoIP implementation; use current design.

Unit Structure	Current Implementation	VoIP Implementation
Single Device	Hardware design	This feature not effected with VoIP implementation; use current design.
Hand-Held Device	Hardware design	This feature not effected with VoIP implementation; use current design.
Stand-Alone	Hardware design	This feature not effected with VoIP implementation; use current design.
Combat Console Compatible	Hardware design	Hardware design
Locate the Telephony, Radio, PTT Footswitch, and External Loudspeaker Connectors on the Chassis Accommodating Installation and Cable Termination Requirements	Hardware design	Hardware design
Upgrade	**Current Implementation**	**VoIP Implementation**
Replaces Multiple Interior and Exterior Devices	By Design	By Design
Unit Accessories	**Current Implementation**	**VoIP Implementation**
Provides a Handset and/or Binaural Headset with 15-Foot (Stretched) Commercial Twist-Type Cord with an Overall Shield and a Separate Shield for the Microphone Leads	Hardware design	Hardware design
Provides a 25-Foot (Stretched) Cord or a 10-Foot (Stretched) Quick-Disconnect Extension Cord for Watchstations with Extended Area Requirements	Hardware design	Hardware design

3.12.2 Dial Telephone

This end device is comparable to an office phone that has been repackaged for shock and vibration survivability. The phone can be either analog or digital depending on the equipment of the vessel and the features required. The features vary from the analog to digital with the digital having the standard office type features, such as display, and buttons for control features. A watertight version of the dial telephone is provided for use in hazardous areas, such as the weapons magazines. Features and operation are identical to the standard dial telephone. The dial telephone can come with or without a General Alarm Switch (see Figure 3-47).

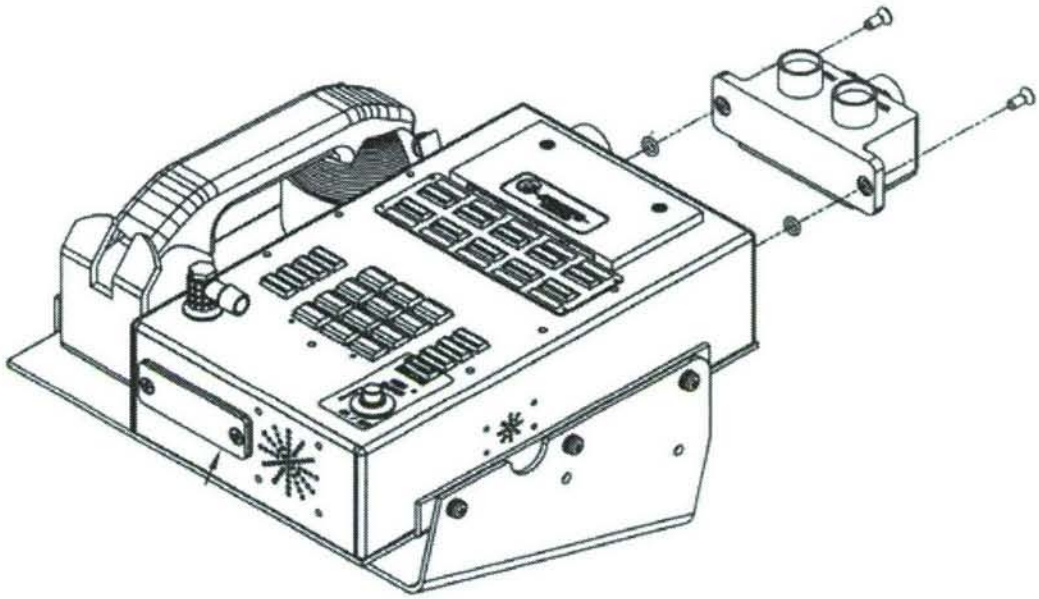


Figure 3-47. Dial Telephone

The Voice Network provides both digital Dial Telephones, which utilize commercial standards and protocols, and standard commercial Tip & Ring analog Dial Telephones for low-level administrative communications and special applications. Analog Dial Telephones have limited features compared to the digital phone version.
The Dial Telephone is a single device used on naval vessels designed for vertical installation on a wall or horizontal installation to a desktop. The Dial Telephone initiates and receives telephone call connections and initiates intercom call connections. Hand-held microphones, external loudspeakers, and Push-to-Enable (PTE) handsets are used, when necessary. The digital Dial Telephones has a caller ID display and Single Button Activation (speed dial) for intercom calls to associated watch stations.

3.12.2.1 Dial Telephone Derived Baseline

Table 3-26 provides a baseline list of the functions and capabilities of the Dial Telephone by functional subheadings that relate to the VoIP implementation.

Table 3-26. Dial Telephone Derived Baseline

Intercom Communication	**Current Implementation**	**VoIP Implementation**
Allows Intercom Calls for Digital Telephones	Hardware/Software design	The auto answer draft "draft-ietf-sip-answermode-04" allows for this type of operation. ICT and IP-PBX will need to support it.
Telephone Communication	**Current Implementation**	**VoIP Implementation**
Provides Standard Commercial Analog Telephone for Low-Level Administrative Communication and Special Applications where Analog Technology is Only Available to Satisfy Specific Vital Communication Functions	Hardware design	The use of VoIP phones that have limited functions can be substituted for the analog phones. The use of sound powered telephones can also be used and interfaced into the VoIP-network using media gateways.
Provides Digital Telephone for Areas not Requiring an Analog Telephone	System design	System design
Telephony Compatibility	**Current Implementation**	**VoIP Implementation**
Compatible with Host Telephony Unit DTMF Operation	Hardware design	This is supported in SIP. The end devices will need to support it. Determination on method used to transport will need to be made, so all devices are configured the same. Refer to RTP – RFC 2833 and Info Method – RFC 2976.
Display	**Current Implementation**	**VoIP Implementation**
Displays Caller ID in Accordance with the Host Telephony Unit Telephone User List for Digital Telephones	Hardware design	Caller ID is supported in SIP. The end device will need to display it. RFC 2543bis defines the method used to define it in the SIP header.

Audio Interface	**Current Implementation**	**VoIP Implementation**
Accepts Hand-Held Microphones, External Loudspeakers, and PTE Handsets for Digital Telephones	Hardware design	Hardware design
Accepts Hand-Held Microphones and External Loudspeakers for Intercom Calls	Hardware design	Hardware design
Uses PTE Handsets in SI and Vital Operation Areas	Hardware/software design	Hardware/software design
Telephony Interface	**Current Implementation**	**VoIP Implementation**
Accepts Multiple Calls through the Host Telephony Unit	Hardware design	On the standard SIP phone one primary call and the others are placed on hold.
User Interface	**Current Implementation**	**VoIP Implementation**
Provides Single Button Activation Calling for Intercom Calls to Associated Watchstations on Intercom Circuits	Hardware/Software design	The auto answer draft "draft-ietf-sip-answermode-04" allows for this type of operation. End device and IP-PBX will need to support it.
General Operation	**Current Implementation**	**VoIP Implementation**
Uses Commercial Standards and Protocols	Analog or BRI	SIP
Does Not Modify Signaling Circuits Unique to Host Telephony Unit Functionality	Analog or BRI	SIP – done with RFC and drafts
Does Not Modify Host Telephony Unit Software to Accommodate Caller ID	Hardware design	Caller ID is supported in SIP. The end device will need to display it. RFC 2543bis defines the method used to define it in the SIP header.

Audio Operation	Current Implementation	VoIP Implementation
Uses PTE Handsets in Sensitive Areas	Hardware design	This feature not effected with VoIP implementation, use current design.
Allows the Calling Party to Control the Called Party's Ability to Receive and Transmit Audio on a Hands-Free Telephone Preventing Call Blocking Due to Excessive Background Noise	This is a new requirement and Henschel was not able to determine if it is presently being done. Multiple methods can be used. (VOX, two lines for example)	This will need to be evaluated to determine if it would be done with hardware or software or a combination of the two. It is not specified in the SIP specifications.
Physically Disables the Internal Microphone in SI Areas	Hardware design	IP packet system does not transfer audio out of speaker. This is not an issue with IP based devices.
Unit Structure	**Current Implementation**	**VoIP Implementation**
Provides Grade B Shock Qualified Chassis Mounted Vertically or Horizontally for Analog Telephones	Hardware design	Hardening of COTS IP phones or the use of IP phone chips will be required to achieve the requirement.
Provides Grade A Shock Qualified Enclosure for Analog Telephones Used for Vital Communication	Hardware design	Hardening of COTS IP phones or the use of IP phone chips will be required to achieve the requirement.
Provides Grade A Shock Qualified Chassis Mounted Vertically or Horizontally for Digital Telephones	Hardware design	Hardening of COTS IP phones or the use of IP phone chips will be required to achieve the requirement.

3.12.3 Sound Powered Telephone Interface

The Sound Powered Telephone (SPT) Interface is a single device used on naval vessels for communication to designated SPT circuits. The SPT is used as a backup to the primary phone system and does not require vessel power to operate. It is included here because it is interfaced to the primary phone system for communications between the two systems. Individual circuits on the SPT are connected to the primary phone system through media gateways, allowing the two systems to communicate in a limited fashion. The primary phone system can not ring a phone on the SPT, so the operator of the phone needs to know to pick up the phone. Vice verse, the SPT can not ring the primary phone system. Table 3-27 provides a derived baseline listing the functions and capabilities of the SPT by functional subheadings that relate to the VoIP implementation.

Table 3-27. SPT Interface Derived Baseline

SPT Interface	**Current Implementation**	**VoIP Implementation**
Provides Interface to Designated SPT Circuits	Hardware/circuit design	Media gateway to interface between SPT and the IP-network.
Provides Interface For Designated SPT Circuits to the Host Telephony Unit or Shipboard Air Traffic Control Communication (SATCC) Exclusively	Hardware/circuit design	Media gateway to interface between SPT and the IP-network.
User Interface	**Current Implementation**	**VoIP Implementation**
Connects Host Telephony Unit Users to SPT Circuits with Conferencing Nets	Hardware/circuit design	Media gateway to interface between SPT and the IP-network.
Allows Host Telephony Unit and SATCC Users to Access SPT Interface Conferences	Hardware/circuit design	Media gateway to interface between SPT and the IP-network.
Provides Designated SPT Circuit Isolation Switches	Hardware/circuit design	Media gateway to interface between SPT and the IP-network. Media gateway can require authentication before allowing traffic from the IP-network to transverse it.

Audio Operation	**Current Implementation**	**VoIP Implementation**
Automatically or Manually Balances SPT Circuit Interface Audio Levels	Hardware/circuit design	Media gateway to interface between SPT and the IP-network. May require some modification for balancing of the circuit.
Does Not Degrade Audio Level when SPT Circuit User Accessories are Connected or Disconnected	Circuit design	This feature not effected with VoIP implementation; use current design. May require some modification for balancing of the circuit.
Does Not Degrade SPT Circuit Audio Quality or Level when Connected to a SPT Circuit	Circuit design	This feature not effected with VoIP implementation; use current design. May require some modification for balancing of the circuit.
Reliable Operation	**Current Implementation**	**VoIP Implementation**
Functions During All Ship Conditions and Operations	Circuit design	The SPT is self-powered, but the interface to the IC requires the media gateway to have power.
Telephony Operation	**Current Implementation**	**VoIP Implementation**
Activates a SPT Conference when the First Host Telephony Unit User Accesses a SPT Conferencing Net	PBX and SPT design	Media gateway to interface between SPT and the IP-network. Call bridge may need to be configured special for this type of use.
Deactivates a SPT Conferencing Net when the Last Host Telephony Unit User Releases the Conference Call	PBX and SPT design	Media gateway to interface between SPT and the IP-network. Call bridge may need to be configured special for this type of use.

Upgrade	Current Implementation	VoIP Implementation
Reduces SPT Circuit User Configuration	Circuit design	This feature not effected with VoIP implementation; use current design.

3.12.4 Conference Bridge

The Conference Bridge is a single device used on naval vessels for multi-party conferencing. The following Table 3-28 provides a derived baseline for the Conference Bridge that lists the functions and capabilities of the Conference Bridge by functional subheadings that relate to the VoIP implementation.

Table 3-28. Conference Bridge Derived Baseline

Diagnostic Compatibility	Current Implementation	VoIP Implementation
Provides Control Circuitry For Remote Alarm Monitoring Compatible with IC/SM Type Alarm Switchboards	Hardware/software design	Network monitoring tool to monitor call bridge and other components of the IP telephony network.
Telephony Compatibility	**Current Implementation**	**VoIP Implementation**
Provides Commercial Standard Conferencing Capability	COTS implementation that interfaces to the PBX	Solution range from an additional piece of hardware, but for smaller requirements it is also done in a software solution.
Provides Switching Mechanism and Bearer Circuitry Using Shipboard Compatible Commercial Standards and Protocols	Depends on the vendor of the conferencing system and the PBX	Solution range from an additional piece of hardware but for smaller requirements it is also done in a software solution.
Provides Control Circuitry Using Commercial Telephony Standards	Depends on the vendor of the conferencing system and the PBX	The different solutions are all developed around IETF specifications and drafts.

Unit Display	**Current Implementation**	**VoIP Implementation**
Provides Audible and Visible Indication of Alarms Impacting Conferencing Operation	Sent to the alarm panel	Only an issue with a hardware solution, even then there are no bearing circuits to deal with. Network monitoring tool would be used to monitor it and other components in the IP telephony network.
Provides Visible Summary Indication of Failed Bearer Interface Circuitry Interface Ports	Sent to the alarm panel	Only an issue with a hardware solution, even then there are no bearing circuits to deal with. Network monitoring tool would be used to monitor it and other components in the IP telephony network.
Telephony Interface	**Current Implementation**	**VoIP Implementation**
Provides Conference Switch Bearer Circuitry Interface Directly to the Host Telephony Unit as a User Interconnectivity Gateway	Depends on the vendor of the conferencing system and the PBX	It is handled on the IP-network so no interconnectivity gateway is required.
Provides Conference Switch Bearer Circuitry Interface to End Points Using Commercial Telephony Standards and Protocols	Depends on the vendor of the conferencing system and the PBX	The different solutions are all developed around IETF specifications and drafts.

General Operation	Current Implementation	VoIP Implementation
Integrates Two-Way Multi-Channel (MC) Intercom Circuits and the Host Telephony Unit	Depends on the vendor of the conferencing system and the PBX	Configuration of class of service is required to give the correct rights to individual end devices to connect to conference groups.
Does Not Interrupt Active Conferences when On-Line Controller Circuitry Fails Automatically Switching to Stand-by Control Circuitry	Depends on the vendor of the conferencing system and the PBX	With a hardware solution, that would need to be a requirement. If a software solution is used, and is not a man-in-the-middle, then this would not be an issue.
Does Not Use System-Unique Non-Commercial Hardware or Firmware in the Host Telephony Unit Bearer Circuitry Interface	COTS purchased bridge	COTS purchased bridge
Diagnostic Operation	**Current Implementation**	**VoIP Implementation**
Provides Built-in Diagnostic Testing of Bearer Circuitry Components and On-Line/Off-Line Control Circuitry	Designed by the manufacture of the hardware solution.	There are no bearing circuits to be testing in either the hardware or software solutions. Network monitor the solution is still required
Monitors Control and Bearer Circuitry Health through Non-Selectable Background Diagnostics	Designed by the manufacture of the hardware solution.	There are no bearing circuits to be testing in either the hardware or software solutions. Network monitor the solution is still required

Diagnostic Operation	**Current Implementation**	**VoIP Implementation**
Detects Control and Bearer Circuitry Failures Producing Relevant Alarms and Error Reports	Designed by the manufacture of the hardware solution.	There are no bearing circuits to be testing in either the hardware or software solutions. Network monitor the solution is still required.
Provides Bearer Interface Circuitry Support Background and Selectable Diagnostic Testing	Designed by the manufacture of the hardware solution.	System monitor the solution is still required.
Allows Control Circuitry Diagnostic Testing of Bearer Circuitry	Designed by the manufacture of the hardware solution.	There are no bearing circuits to be testing in either the hardware or software solutions.
Selects Diagnostic Testing at the Administration Terminal	Designed by the manufacture of the hardware solution.	Done with the network monitoring and management tools, for many of the vendors' solutions.
Accesses Alarm and Error Reporting at the Administration Terminal Providing Detailed Information Addressing Detected Failures	Designed by the manufacture of the hardware solution.	Done with the network monitoring and management tools, for many of the vendors' solutions.
Intercom Operation	**Current Implementation**	**VoIP Implementation**
Expands Point-to-Point MC Intercom Circuit Capability through Multi-Party Conferencing	Design feature	Design feature

Reliable Operation	**Current Implementation**	**VoIP Implementation**
Provides n+1 Single-Point Failure Configuration Control Circuitry for Each Conference Switch	Designed by the manufacture of the hardware solution.	The hardware or software solutions use redundant systems. Since it is IP-network based units do not been to be located near the IP-PBX or redundant units.
Provides Redundant Control Circuitry Shadow On-Line Control Circuitry Allowing Single-Point Control Circuitry Failure Rapid Recovery	Designed by the manufacture of the hardware solution.	The hardware or software solutions use redundant systems. Since it is IP-network based units do not been to be located near the IP-PBX or redundant units.
Automatically Switches On-Line and Off-Line Control Circuitry	Designed by the manufacture of the hardware solution.	The hardware or software solutions use redundant systems. The switch over is taken care of by DNS, or clustered servers.
Storage Operation	**Current Implementation**	**VoIP Implementation**
Provides Permanent Non-Volatile Storage of Conferencing, Interface and System Configuration Data	Designed by the manufacture of the hardware solution.	The configuration is store and managed between the redundant systems.

Telephony Operation	Current Implementation	VoIP Implementation
Provides Multi-Party Conferencing for Vital and Tactical Communication	Design feature	Design feature
Functions as a Telephony-Based Switch with Commercial Standard Control and Bearer Circuitry	Designed by the manufacture of the hardware solution.	The design doesn't require bearing circuits, and is developed on the SIP RFC 3261, and other specifications and drafts.
Provides the Control Circuitry Switching Mechanism Route Bearer (Voice) Data between Conference Users or Conferees	Design feature	Design feature
Provides Conference Switch Bearer Circuitry Consist of Non-Dedicated Digital Interface Links and Voice Processing Circuitry for Conferencing	Designed by the manufacture of the hardware solution.	The design doesn't require bearing circuits, and is developed on the SIP RFC 3261, and other specifications and drafts.
Provides Interface Circuitry with Digital Links Connection to the Host Telephony Unit Administered by the Conference Switch Control Circuitry at the Administration Terminal for Configuring the Interface Settings	Designed by the manufacture of the hardware solution.	Depending of vendor solution, they have web interfaces or configuration on the device. Connection to the device is through the IP-network.
Provides Open Architecture Interface Settings Using Commercial Telephony Standards and Protocols	Depends on the vendor of the conferencing system and the PBX	The different solutions are all developed around IETF SIP specifications and drafts.
Telephony Operation	**Current Implementation**	**VoIP Implementation**
Allows All Conference Switch Units To Accommodate 460 Simultaneous Conferees through 198 Different Conferences Minimum	Depends on the vendor of the conferencing system and the PBX	This will determine vendors since several of them can't handle the numbers. External conferencing hardware maybe required for larger systems; where smaller numbers can be handled in software versions.

Unit Structure	Current Implementation	VoIP Implementation
Integrates Centralized Control Circuitry and Bearer Circuitry into the Same Housing	Depends on the vendor of the conferencing system and the PBX	There are no bear circuits the solutions are single server.

3.12.5 Electronic Call Accounting System

The Electronic Call Accounting System (ECAS) is used on naval vessels for call accounting of incoming and outgoing calls. In the corporate environment it is referred to as call detail record (CDR). Call account data captured for outgoing calls include the calling number, outgoing trunk/link used, destination digits dialed, time/date call was initiated, and the total amount of time that call was active. Call accounting data captured for intra call traffic should include the calling number caller ID, called number caller ID, time/date the call was placed, and duration that the call was active.

The following Table 3-29 provides a derived baseline for the ECAS. The baseline lists the functions and capabilities by functional subheadings, that relate to a VoIP implementation.

Table 3-29. ECAS Derived Baseline

General Connection	Current Implementation	VoIP Implementation
Uses Shipboard Approved Commercial Standard Connectors	Depends on the vendor the PBX	Call accounting requires that the call pass through a B2BUA server. For external call, recording off of the media gateway maybe done. This will need to be evaluated. Most IP-PBXs have some form of CDR.
Telephony Connection	**Current Implementation**	**VoIP Implementation**
Connects to Each Independent Host Telephony Unit Controller for Ship wide Call Traffic Reporting	Depends on the vendor the PBX	Dependant on vendor solution, different levels of reporting can be gotten. Could not determine how CDR is handled with redundant servers for the different vendors.
Provides Connections Conforming to Host Telephony Unit Signaling Requirements	Depends on the vendor the PBX	Dependant on vendor solution, different levels of reporting can be gotten.

General Operation	Current Implementation	VoIP Implementation
Captures Call Traffic of Selected Interface Links and Trunks	Depends on data collected configuration	Depends on data collected configuration
Records All Incoming and Outgoing Trunk Calls	Depends on data collected configuration	Depends on data collected configuration
Records Call Traffic on a Single Station Basis	Depends on data collected configuration	Depends on data collected configuration
Records Call Traffic for Ship's Administrative Communication Management	Depends on data collected configuration	Depends on data collected configuration
Verifies Long-Distance Off-Ship Calling Charges and Track On-Ship Harassment Calls	Depends on data collected configuration	Depends on data collected configuration. External calls may pass through the media gateways, and authentication can be required.
Uses Standard Commercial Hardware without Application-Unique Modification	Depends on the vendor the PBX	Depends on the vendor the PBX
Integrates into the Host Telephony Unit Manager Station or Operates as a Stand-Alone Unit	Depends on the vendor the PBX	Depends on the vendor the PBX
Uses a Standard PC with Unmodified Commercial Software	Depends on the vendor the PBX	Most vendors make if available through an authenticated web interface. As well as have export features so the information can be gotten into other applications, if required.
Uses Licensed and Registered ECAS Operation, Monitoring, Management, and Maintenance Software	Depends on the vendor the PBX	Depends on the vendor the PBX
Provides Software For Shipwide Call Traffic Recording of All Host Telephony Unit Interface Calls and Selected Station Calls	Depends on the vendor the PBX	Depends on the vendor the PBX

Storage Operation	Current Implementation	VoIP Implementation
Electronically Stores Captured Data For Generating and Printing Various Call Traffic Reports	Depends on the vendor the PBX	Depends on the vendor the PBX. Most have printing and export features.
Provides the Host Telephony Unit Called Number, Incoming Link/Trunk Used, Calling Party Caller ID, Date/Time Call was Received, and Duration Call was Active for Incoming Host Telephony Unit Call Captured Data	Depends on the vendor the PBX, and configuration of their offering	Depends on the vendor the PBX, and configuration of their offering
Provides the Host Telephony Unit Calling Number, Outgoing Link/Trunk Used, Destination Digits Dialed, Date/Time Call was Initiated, and Duration Call was Active for Outgoing Host Telephony Unit Call Captured Data	Depends on the vendor the PBX, and configuration of their offering	Depends on the vendor the PBX, and configuration of their offering
Provides the Calling Number Caller ID, Called Number Caller ID, Date/Time Call was Placed, and Duration Call was Active for Intra-Host Telephony Unit Call Captured Data	Depends on the vendor the PBX, and configuration of their offering	Depends on the vendor the PBX, and configuration of their offering
Telephony Operation	**Current Implementation**	**VoIP Implementation**
Provides Call Accounting of Incoming and Outgoing Calls to the Host Telephony Unit from Interface Links and Trunks	Depends on the vendor the PBX, and configuration of their offering	Depends on the vendor the PBX, and configuration of their offering
Allows Ship's Force to Capture Host Telephony Unit Call Traffic of Selected User Devices	Class of server is used to force collection of date.	Class of server is used to force call to be process through a man-in-the-middle so the information can be gathered.

Unit Structure	Current Implementation	VoIP Implementation
Provides Grade B Shock Qualified Hardware when Installed Outside the Manager Station	COTS hardware needs to be evaluated and hardened as required.	If hardware solution is used then, COTS hardware needs to be evaluated and hardened as required. If software solution is used then the server it is located on will require to be hardened as well as the rack that it is placed into.

3.12.6 Voicemail

The Voice Mail (VM) system is used on naval vessels for voice mail functions at administrative telephones. It is associated with the end device and not an individual person. It allows users to record and retrieve voice mail messages, save or delete voice mail messages, and record personal greetings. The VM system has user password protection, records and announces the date and time for voice mail messages, and displays the presence of received voice mail messages. The following Table 3-30 provides a derived baseline for the Voice Mail. The baseline lists the functions and capabilities by functional subheadings that relate to the VoIP implementation.

Table 3-30. VM Derived Baseline

General Connection	Current Implementation	VoIP Implementation
Provides Shipboard Approved Commercial Standard Connectors	Design features, and are availability from the vendor.	Connectors for a VM system would be CAT5 or fiber for the IP-network connection.
Telephony Connection	**Current Implementation**	**VoIP Implementation**
Provides Connections Conforming to Host Telephony Unit Signaling Requirements	Design features, from the vendor.	Connectors for a VM system would be through the IP telephony network.

Unit Display	Current Implementation	VoIP Implementation
Displays the Presence of Received Voice Mail Messages Ready for Retrieval	This would be shown on the end device. Usually is the use of a light.	The RFC 3842 defines a way for a user agent to find out about voicemails and other messages that are waiting for it. Its primary purpose is to enable the voicemail-waiting lamp on most business telephones.
User Interface	**Current Implementation**	**VoIP Implementation**
Allows Users and Interfaces Accessing Configured Administrative Telephones to Record Voice Mail Messages to Configured Voice Mailboxes	Vendor dependant, done through the phone interface.	Vendor dependant, done through the phone or done through a web interface. Some allow a mix of features from both methods. This is not defined by SIP specifications and is the design by the supplier of the systems.
Allows Users to Retrieve Voice Mail Messages Locally at the Configured Telephone or Remotely from Other Host Telephony Unit User Stations or Interfaces	Vendor dependant, done through the phone interface.	Vendor dependant can be done through the phone or some allow email or access through a web interface to retrieve their VMs.
Allows Users to Save or Delete a Retrieved Voice Mail Message	Vendor dependant	Vendor dependant

User Interface	**Current Implementation**	**VoIP Implementation**
Allows Users to Record a Personal Greeting	Vendor dependant, done through the phone interface.	Vendor dependant, done through the phone or done through a web interface.
Provides User Password Protection	Vendor dependant, done through the phone interface.	Vendor dependant, password maybe controlled but VM system or be a IP-network authentication.
General Operation	**Current Implementation**	**VoIP Implementation**
Applicable, but not Applied, to All Administrative Telephones	Controlled by class of service or configuration or both.	Controlled by class of service or configuration or both.
Provides Host Telephony Unit or Stand-Alone Standard PC Voice Mail Operation, Management, and Maintenance Software	Vendor dependant	Vendor dependant
Uses Standard Commercial Hardware without Application-Unique Modification	COTS hardware/software implementation	COTS hardware/software implementation, supplied with the IP-PBX in most cases.

3.12.7 Recording

There are two types of recording that are done on Navy vessels. The first is recording of defined end devices depending on their location in the vessels. The other is microphone recording is a single device used on naval vessels for continuous speech recording of selected talk groups and microphone stations. The derived baseline for the recording system is provided in Table 3-31.

Table 3-31. Derived Baseline For Recording System

Microphone Recording	Current Implementation	VoIP Implementation
The recording of defined extensions	Class of service, use of vendor or 3rd party device	Class of service or feature code, use of vendor or 3rd party device. SIP doesn't define a method of recording calls. It is done with the collection of the RTP stream, with either Man-in-the-middle or Promiscuous mode device. The draft-sriram-sipping-poc-lip-02 is for lawful intercept that may lead to other methods of recording calls, by what will be exposed by the lawful intercept requirements.
Storage and retrieval of the stored recording	Stored short term to local device	Stored short term to local device, then move to permanent offline storage.
Long term storage of the recordings	Procedure is defined for moving them off recording device and onto permanent storage.	Procedure is defined for moving them off recording device and onto permanent storage.
The Microphone Recording system has the capability to continuously record 16 speech channels maximum selected from talk groups and microphone stations referenced to the ship's master time source.	The use of COTS equipment is used, and is hardened as required.	Depending on the vendor used, it may require two different devices. On for audio recording and the other for IP packet recording.

3.12.8 ICSCU Dedicated Station

The Dedicated Station (DS) is a single device used on naval vessels for direct telephone communication without dialing capability. Only the Integrated Communication System Control

Unit (ICSCU) software program determines its function. The Dedicated Station has a front mounted jack for accessory handsets, headsets, microphones, and external loudspeakers. The DS has an indicator labeled "ON" displaying power and functional status.

3.12.8.1 Emergency Phone

An emergency phone is installed at the Ship Control Console and is an example of ICSCU dedicated station. It's function is to receive emergency phone calls from anywhere within the ship. Once an emergency call is placed this phone will ring with both an audible and visual indicator. To answer, the off-hook switch is depressed. This unit is not capable of initiating a phone call. The unit is painted red. See the following Figure 3-49 for a view of the emergency phone. The call can be also "direct or group picked" from another station depending on how the system was configured.

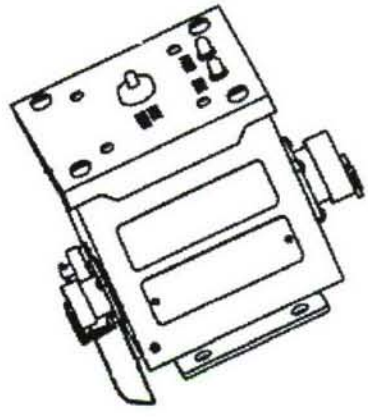


Figure 3-49. Emergency Phone

3.12.8.2 Dedicated Station Derived Baseline

The following Table 3-32 provides a derived baseline for the Dedicated Station. The baseline lists the functions and capabilities of the ICSCU Dedicated Station by functional subheadings that relate to the VoIP implementation.

Table 3-32. Dedicated Station Derived Baseline

Telephony Communication	Current Implementation	VoIP Implementation
Functions as ISDN Digital or Conventional Analog Device	Depends on the vendor's implementation	Would be based on a SIP phone that works on the IP-network. The phone would expose no UI.
General Connection	**Current Implementation**	**VoIP Implementation**
Provides Single Connector for the User Device	Hardware design	This feature not effected with VoIP implementation, use current design.
Provides Connector Access from the Front	Hardware design	This feature not effected with VoIP implementation, use current design.
Provides MIL-C-5015 Connector for Two Systems	Hardware design	This feature not effected with VoIP implementation, use current design.
Second Front Connector (User Connection) Conforms to Commonality Requirements	Hardware design	This feature not effected with VoIP implementation, use current design.
Unit Display	**Current Implementation**	**VoIP Implementation**
Provides One Illuminated "ON" Indicator for Power and Functionality	Hardware design	Would light when there is power from the PoE, (Red) and when authenticated with the IP-PBX. (Green) as a possible solution.
Audio Interface	**Current Implementation**	**VoIP Implementation**
Accepts an External Loudspeaker Serving as a Hands-Free Device whose Receive/Transmit Function is Controlled by a Full Function Telephone or Terminal	Hardware design	This feature not effected with VoIP implementation, use current design.

Telephony Interface	**Current Implementation**	**VoIP Implementation**
Functions as Host Telephony Unit Addressable	Hardware design	Could be implemented as a SIP phone, and authenticate with the IP-PBX.
User Interface	**Current Implementation**	**VoIP Implementation**
Does Not Provide Controls	Hardware design	This feature not effected with VoIP implementation, use current design.
General Operation	**Current Implementation**	**VoIP Implementation**
Operates the Same Way Regardless of the System Software Program	Hardware/software design	The program would be independent of the SIP IP-PBX that it would be install on using SIP RFC 3261 compliance.
Audio Operation	**Current Implementation**	**VoIP Implementation**
Sends and Receives Audio and PTT Signaling	Hardware design	RFC 4354, is one of the specifications as well as several drafts that need to be consulted for the PTT functionality to be implemented.
Capable of being a Dedicated Handset/Headset Station Communicating to a Particular IC Circuit Allowing the User to Connect a Handset/Headset to Listen and Depress the PTT Switch to Talk	Hardware design	RFC 4354, is one of the specifications as well as several drafts that need to be consulted for the PTT functionality to be implemented.
Capable of being a Dedicated Microphone Station Transmitting to a Particular IC Circuit Allowing the User to Connect a Microphone and Depress the PTT Switch to Talk	Hardware design	RFC 4354, is one of the specifications as well as several drafts that need to be consulted for the PTT functionality to be implemented
Capable of being a Hands-Free Loudspeaker Station when the Operator is not Able to Use His Hands for PTT, Hold a Handset, or Wear a Headset	Hardware design	RFC 4354, is one of the specifications as well as several drafts that need to be consulted for the PTT functionality to be implemented.

Audio Operation	**Current Implementation**	**VoIP Implementation**
Capable of being a Dedicated Alarm Station Initiating a Contact Closure Signal Using the PTT Function to the Host Telephony Unit Initiating a Particular Ship's Casualty Alarm	Hardware design	Initiating an alarm is outside of the SIP specification. This can be done with a alternate protocol like SOAP that could be developed to run along side the SIP protocol. RFC 4354, is one of the specifications as well as several drafts that need to be consulted for the PTT functionality to be implemented.
Telephony Operation	**Current Implementation**	**VoIP Implementation**
Not Dial Capable	Hardware design	Hardware design, no UI
Unit Power	**Current Implementation**	**VoIP Implementation**
Receives Power from the Host Telephony Unit	Hardware design	Unit is powered from the IP-network connection with PoE
Unit Structure	**Current Implementation**	**VoIP Implementation**
Does Not Exceed 4 in. Wide x 4 in. High x 4 in. Deep in Physical Size	Hardware design	The phone card will be a non-COTS, to conform to the size restrictions.
Does Not Exceed 5 lbs in Physical Weight	Hardware design	The phone card will be a non-COTS, to conform to the size restrictions.
Does Not Exceed 5 W Heat Dissipation to Air	Hardware design	The phone card design will need to be designed to maintain this requirement. This should not be an issue since a Polycom IP601 with display and hub only uses 4 watts at ideal.

This page intentionally left blank.

3.13 Graphical User Interfaces

3.13.1 Introduction

The communication terminal for use onboard surface ships needs to direct the user to the quickest method to achieve his set task within the users' duty station. For the past several years, advances in Graphical User Interface (GUI) design, Human Factures Engineering, and pure processing power have made the development of products more intelligent for the end user. To leverage this new technology and methods, this section will address specific requirements that a sailor would expect to find in a new Voice over IP (VoIP) communication terminal. This document targets the developer as it describes the subtle issues that must be included in the design of the communications terminal.

3.13.2 Communications Terminal

3.13.2.1 Definition and Function

The VoIP communication terminals are used at communications intensive locations. Each VoIP terminal will be capable of supporting four IP phone calls. A typical operator interface will include a colored flat panel display with a touch screen for user selections. The display consists of multiple screen pages, each customized for the intended location of the communication terminal. On startup, the tactical screen will be displayed. The tactical screen provides the essential communications most used for a particular location. The second screen page provides for "quick calls" (speed dial) to other stations often called by terminal location. Both the first and second screens will contain a common area for handling and processing phone calls, status and caller ID information. In addition to a shared common area, utilitarian screens will always be accessible from the tactical and speed dial screens. For example, a single push button will display the dial keypad. The dial keypad will allow the user to dial a specific number or to program the speed dial buttons. Later sections will describe Sample screens and their functionality.

3.13.2.2 Requirements

The following requirements list has been compiled from pre-existing communications terminals already installed on Navy vessels. Ships force personnel have exercised many options. The minimum requirements for new communication terminal development are:

- Shall use a full color flat panel display for button presentation
- Shall use a touch screen display for button selection
- Shall have button activation for telephone calls, intercom calls and radio calls
- Shall have a speed dial (48 activation buttons) calling screen
- Shall have a keypad screen with standard telephony keypad functions
- Shall have a user configuration screen to select which active connection is left ear, which active connection is right ear, and which active connection is left and right ear when binaural headset output is selected as left/right
- Shall have a bold and contrasting display between telephony calls and radio calls
- Shall have a bold and contrasting display between telephone calls and intercom calls
- Shall have a bold and contrasting display for each active call's operation mode

- Shall have a bold and contrasting display for the presence of encrypted voice messages received off-ship (detect) that remains illuminated until encrypted voice messages are not detected
- Shall have a button to place a radio call in cipher (encrypted) mode
- Shall have a button to place a radio call in plain (unencrypted) mode
- Shall have a button to mute or activate the internal loudspeaker during telephone calls
- Shall have a button to mute or activate an external loudspeaker during radio calls
- Shall have a button to switch a call between transmit mode and monitor-only (mute) mode
- Shall display the active call status on the speed dial calling screens
- Shall display the active call status on the keypad screen
- Shall display the active call endpoint
- Shall display the caller id station name
- Shall display the caller id dialed number for active calls to interface trunks
- Shall display the caller id dialed number if the station name is not available
- Shall have a PTT (Push to Talk) switch in the handset
- Shall have user level ability to archive a profile after making a change
- Shall provide night mode colors Red, Blue for the GUI.

3.13.2.3 Communications Terminal Equipment

The next generation Communications Terminal Equipment shall be constrained by some physical requirements. The physical size, power characteristics and CPU processing power must be considered. For example, the size of the flat panel color display has a direct impact on the size of the graphical user interface. From a software developer's perspective, the design time effort should include an investigation into an automatically sizeable GUI. The following internal and external requirements do not address the size of the next generation unit but address a minimum set of components required. Specific physical requirements for qualification such as Grade "A" Shock and Vibration for surface ships have not been determined at this time, therefore it has been excluded from the requirements.

3.13.2.4 Internal Components

Internal components refer to components located within the Communications Terminal.

- A high end single board computer
- A real-time or near real-time Operating system that supports the Session Initiation Protocol (SIP) Stack.
- Two High Speed Network Interface Cards (NICs)
- Graphics processing capability
- Touch screen controller
- Internal loud speaker and microphone for telephone calls
- Internal Non-Volatile storage

3.13.2.5 External Components

External components refer to components located either on or connected to the Communications Terminal.

- Full color flat panel display
- Touch Screen capability
- Two User headset jacks (two individual users, or one user and one supervisor)
- Two external headsets
- Four external speaker connectors
- A Push to Talk (PTT) button
- A Screen dimming button

3.13.3 Graphical User Interface (GUI)

3.13.3.1 Target User

The graphical user interface is the most important interface to the end user. The GUI must provide capabilities for call processing, which includes Call Forward, Call Pickup, Call Drop, Call Transfer, Call Hold, Call Conferences, Call Priority and Call Override or break in. In addition to call processing, the GUI must provide capabilities for unit configuration. The following list defines the types of data required for effective operation of the communications terminal.

- Speed dial button definition
- Customized ring tones
- Customized colors for each call type
- IP-Address configuration
- Retrieve and store user configuration
- Keypad and volume control
- Password protected supervisory profiles
- Separate voice volume control for each call
- Separate ringer volume control for each call

3.13.3.2 Types of User Operation

The user will have the capability to make various types of phone calls from the Communications Terminal. All calls will use the Session Initiation Protocol (SIP) Stack and communicate through a SIP server via the IP packet network. Specific details regarding call setup will not be addressed here; rather the types of calls that can be initiated will be addressed.
Types of communications that may be established from the communications terminal:

- IP Voice calls
- Radio Calls
- Broadcast calls
- Intercom calls
- External Voice calls
- Conferences calls

3.13.3.2.1 IP Voice Calls

IP Voice Calls provide for the ability to make normal telephone calls to specific phone numbers or stations throughout the entire ship.

3.13.3.2.2 Radio Calls

Radio calls are normal IP voice calls routed through a media gateway to the radio transmitter. Radio calls can be initiated and received at the communications terminal. Radio calls can also be encrypted or un-encrypted.

3.13.3.2.3 Broadcast Calls

Broadcast calls provide for the ability to make announcements through the announcing system to specific areas of the ship or to the entire ship.

3.13.3.2.4 Intercom Calls

Intercom calls provide for communications from the initiator to other predefined groups of stations.

3.13.3.2.5 External Voice Calls

External calls provide for communications through a media gateway to public switched telephone networks (PSTN's).

3.13.3.2.6 Conference Calls

Conference calls provide the ability to connect a group of stations together and communicate two-way with each other.

3.13.4 GUI Developers Role

The developer's role in the GUI development is to present a user interface that is efficient and functional while attempting to minimize the number of operator actions required to navigate. The developer must see the user interface through the eyes of the user. The developer must also carefully select the types of user controls. Many graphics libraries contain pre-defined user controls for the developer to implement. However, this GUI must utilize a touch screen controller which makes many pre-defined user controls not usable. In later sections of this paper, several examples of pre-defined user controls will be presented and discussed. User controls that can be operated using a finger instead of a stylus or mouse are desireable.

Considerations must also be given to building portable, reusable code. The developers should refer to reference [98] where the authors explore the benefits of Energy-Efficient GUI Design. In reference [98] the authors categorize GUI design by its purpose, input-centric, content-centric or hybrid. For our purposes, the Communications Terminal is an input-centric design. However, the techniques mentioned in reference [98] make specific recommendations regarding colors, color patterns, and color sequences. Each color handling techinque utilizes different amounts of power. This may not be applicable to a fixed communications terminal on board Navy Ships, however if the GUI is ported to execute on a Handheld device, then the power consumption recommendations are highly applicable.

3.13.4.1 Button Characteristics

The primary user control on the communications terminal will be the button. The button is a user control that can be programmed to perform different functions. Grouping many buttons together based on functionality determines how the GUI screen layout will be defined.

3.13.4.2 Button Size and Placement

The developer must review who the target user is when determining button size and placement. The communication terminal is a touch screen application with the user's finger as the pointing device. With that thought in mind, the developer must analyze the user requirements for the quantity of buttons per screen and create a button that meets those requirements in size and functionality.

In other touch screen applications onboard ship, size and placement vary based on the function of the user's screen. The common theme is that the buttons are large enough to be pressed/depressed with ease. Since our requirements stipulate 48 speed dial buttons, the developer must determine if the screen size chosen can effectivly support 48 speed dial buttons on a screen. It may not, given that the average button is about ½ to 1 inch square (see Figure 3-48). The key thing to remember is that the users (the sailors) must be able to perform their duty under extenuating circumstances. The user must be able to depress any button when wearing fire protectant gloves. The requirment alone limits the size of the button. Button placement goes hand in hand with screen layout. The grouping of like functionality greatly lends itself to positive user feedback. If you make the interface difficult to use, you are straying away from the primary premise "Ease of Use".

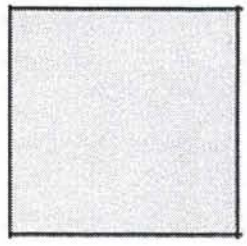


Figure 3-48. Button Example

3.13.4.3 Button Behavior

A typical user control button derives its behavior from its function. If the function is a speed dial, then that particular button is used to initiate a predefined call. Programmatically speaking, pressing a button causes an event callback into the event handler of the call processing class. The button passes all defined information that the button object itself contains. Other examples of button behavior are:

- Reverse video when the button is depressed to provide positive feedback to the user that the button was actually depressed. (momentary)
- Momentary state – button selection, feedback given, button returned to normal display state.
- Selected state – button selection, button stays depressed, feedback to the operator is the depressed state. Operator depresses button in depressed state to toggle the button to the unselected state.
- Button blinking or designated button colors to attract the operator's attention or differentiate call groups.

3.13.4.4 Button Functionality

Button functionality addresses what kinds of actions or functions can be assigned to buttons. As mentioned above, our requirement stipulates 48 speed dial buttons. That means the developer must provide 48 buttons for the user to define as speed dials, provide the user a mechanism to configure the speed dial buttons and provide a mechanism to navigate the GUI. Along with the speed dials, another critical area is Call Processing. How does the user answer a call to the Communications Terminal? The answer is a button, or a call button group would alert the user to answer the call. Reviewing our requirements again, we see that the user must be able to answer several types of calls. This is where the button behavior comes into play. When a call is received, a predefined permanent button group will display the incoming call (Button Blinking), the incoming call type, the caller-Id information and call status. The user will then select the momentary button (Call 1 Select) to cause the call processing class to process the button event and route the audio to the headset. Figure 3-51 depicts a notional button group.

Call 1 Select	Call 2 Select	Call 3 Select	Call 4 Select
Call 1 Status	Call 2 Status	Call 3 Status	Call 4 Status
Call 1 Clear User1/User2	Call 2 Clear User1/User2	Call 3 Clear User1/User2	Call 4 Clear User1/User2

Figure 3-49. Call Button Processing Group

In Figure 3-49, depressing the Call Select button answers an incoming phone call. The button functionality for each group changes somewhat depending on the type of call. For instance, if an incoming radio call were assigned to the Call 2 button group, the status would indicate if the call is encrypted or non-encrypted by text and by color. The color selection for radio encrypted and non-encrypted calls is defined in the Crypto Colors section 3.13.7.2. No color deviation is allowed on this standard color scheme. Referring back to our requirements list, there are many examples of button functionality that are required. One particularly notable requirement is Night Mode Capability. That means that the night mode button must toggle between three screen colors. Those screen colors are full color, red, and blue. The night mode screens will be discussed later in detail.

3.13.5 Controls

In modern Graphhical User Interface environments, a collection of controls has become standard and their use is well understood by many users. The collection consists of :

- Buttons
- List Boxes
- Menu's
- Radio Buttons
- Check Boxes
- Combo Boxes
- Scroll Bars
- Pop-Up dialog boxes

Most if not all are utilized in many GUI applications where a mouse or stylus is the primary pointing device. However, in this application where a user's finger is the primary pointing device, only a subset of the collection can be implemented. That subset contains Buttons, Pop-Up dialog boxes and maybe radio buttons and check boxes. The others require too much precision from the

pointing device to operate. In reference [98], the authors present arguments for not implementing some of the standard controls. They recommend alternatives that require less power to operate. Their approach utilizes tabbed interfaces to group selections of buttons which are very easy to operate. The developer of the communications terminal GUI should try to implement similar controls. In Figure 3-50, the Ringer Volume control group has three combo boxes and each has several selections the user can select. However, observe where the user has to hit the screen to make a selection. Although it is not impossible to hit the down arrow with your finger on the touch screen, it is not easy for the user. However, the checkbox control used here is not that difficult for the user to select. The focus has to be on usability and not on developer convenience.

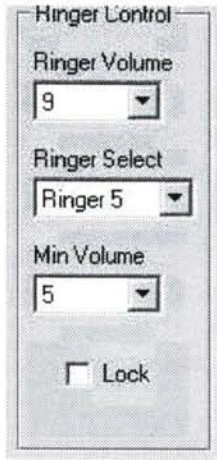


Figure 3-50. Ringer Control with Combo Box

Similarly, the menu control is another widely utilzed control. Figure 3-51 depicts a Microsoft Excel spreadsheet, opened to a new project. Examine how precise the user would have to be with his finger as the stylus to select menu items. The Help menu selection has been chosen with a mouse pointing device. Without a keyboard or mouse, and only the user's finger, the Help menu is cumbersome at best to use. The desired method would be to provide the user with a button selection to perform a group of tasks and that button opens a new window or a tabbed interface containing the configurable items. For every opened utility window, the developer must provide a close button to return to the primary screen.

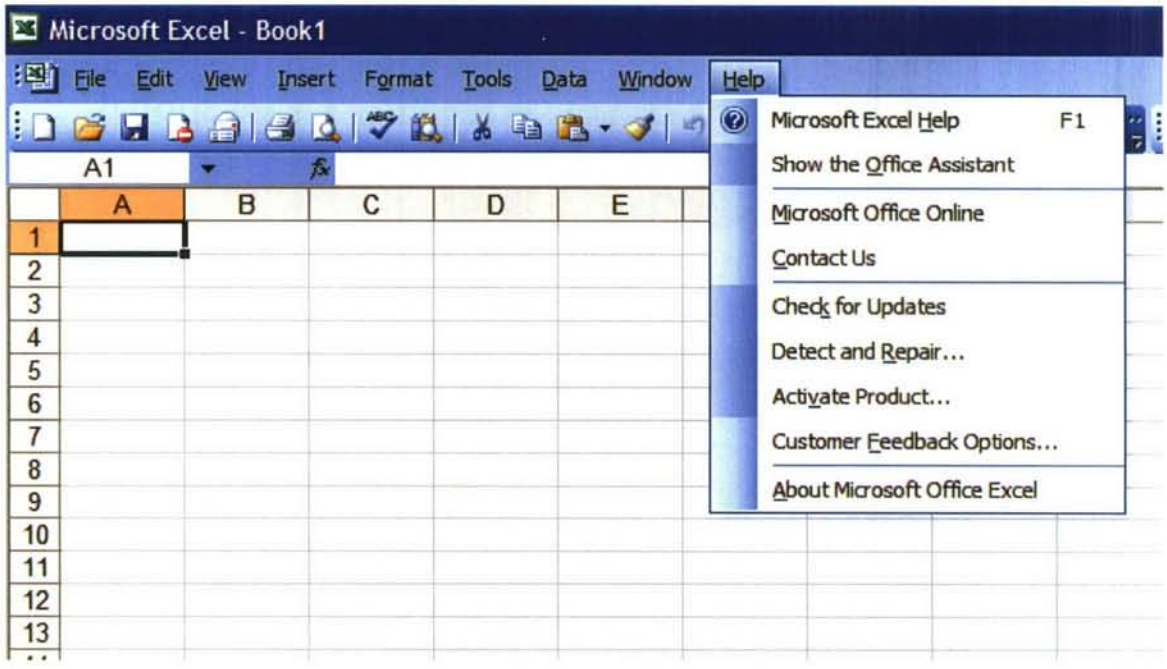


Figure 3- 51. Menu Selection

3.13.6 Screen Layout

The primary goal of the software developer should be to minimize the number of button selections required for the sailor to perform their duty efficiently. The first question the developer should be asking is how big is the display? That answer will limit the size of the controls. Our requirements state that 48 speed dial buttons can be defined. Given the button functionality, behavior and size requirements mentioned above, the GUI might not accommodate 48 speed dial buttons on one screen. Therefore, a sample GUI design with two screens, each containing 24 speed dial buttons will be presented.

The primary screen (Screen 1 or Tactical Screen) will be split horizontally into two sections, a Permanent Screen Section and a Variable Screen Section.

3.13.6.1 Permanent Screen Section

The permanent screen section will contain fixed controls that are present on all screens except utility and configuration screens. The fixed section will contain the call processing button groups as depicted in Figure 3-52 and any navigation and utility/configuration buttons. Figure 3-53 depicts a notional screen displaying the permanent button section layout. The utility and configuration buttons will cause additional screen (dialogs) to pop-up and allow the user to perform other functions. As mentioned earlier, any utility or configuration screen will implement a close or exit button to return to the calling screen. Two of the configured controls "Screen 1" and "Screen 2" control the variable screen section with regard to the speed dial buttons only. The developer could argue that all utility and configuration screens be displayed only in the variable screen section. This would allow the user to answer calls during minor configuration. The

decision would have to be based on the screen size, the number of buttons and type of configuration interface presented to the user.

Hold	Pickup	Utility	Call 1 Select	Call 2 Select	Call 3 Select	Call 4 Select
IP Configuration	User 1	User 2	Call 1 Status	Call 2 Status	Call 3 Status	Call 4 Status
Screen 1	Screen 2	Keypad/ Volume Screen	Call 1 Clear User1/User2	Call 2 Clear User1/User2	Call 3 Clear User1/User2	Call 4 Clear User1/User2

Figure 3-52. Notional Permanent Screen Section

One of the key utility buttons will be the Keypad/Volume Screen button. This button is an example of a combined utility button. This button's action will be to pop-up a floating window that provides another selection between the Keypad and Volume screens. The developer should target a maximum selection depth of three clicks or button selections when presenting configuration options to the user. Figure 3-53 depicts a notional Keypad/Volume screen. Figure 3-54 depicts a notional Keypad screen and Figure 3-55 depicts the Volume screen. In Figure 3-54, note that the user has the ability to place a call from the Keypad screen.

Figure 3-53. Notional Keypad/Volume Screen

1	ABC 2	DEF 3	CLEAR
GHI 4	JKL 5	MNO 6	BACK SPACE
PQRS 7	TUV 8	WXYZ 9	CALL
*	0	#	

Figure 3-54. Notional Keypad Screen

CALL 1 INC	CALL 2 INC	CALL 3 INC	CALL 4 INC
25%	25%	25%	25%
CALL 1 DECR	CALL 2 DECR	CALL 3 DECR	CALL 4 DECR

Figure 3-55. Notional Volume Screen

3.13.6.2 Variable Screen Section

The Variable Screen section is the area above the permanent screen section. This part of the GUI will change depending on the button function and behavior. The first of the 24-button Speed Dial Screens will be the Primary / Tactical Screen displayed in the Variable Screen section. Typically, the users' duty station defines this screen. The Tactical Screen contains the most frequently dialed numbers. The lesser dialed numbers will be pre-programmed on the second Speed Dial Screen. Figure 3-56 depicts an example of a 24-button speed dial screen.

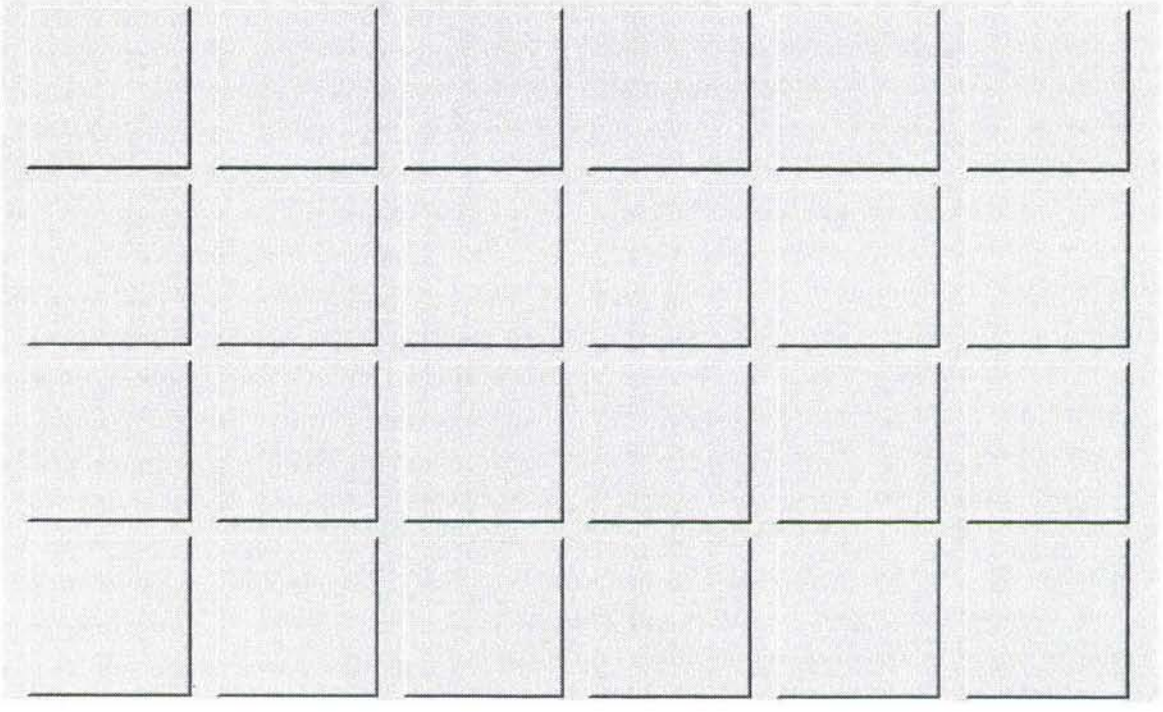


Figure 3-56. 24-Button Speed Dial Screen

3.13.7 Configuration Screens

The developer will provide a mechanism for programming the button data. The button data will consist of the phone number, the call type and a button text label. The user could substitute an icon that is more representative than a text label. A pre-defined set of icons and a mechanism for displaying and selecting the icons will be incorporated into the button programming class. The developer may also allow the user to assign pre-defined ring tones to certain types of calls. Again, the ring tones and the mechanism to play and select them will be incorporated into the button programming class.

3.13.7.1 Button Colors

The developer will have the ability to determine the button colors that are not user-definable and the ones that are. Currently only encrypted (radio) calls are set programmatically. The user will have the ability to define a color for each call type. The developer should either provide a limited color palette or provide the system color palette. Figure 3-57 depicts the typical color palette for a Microsoft ® Windows system. Most commercial operating systems with graphics processors will provide their own color palettes. This color palette requires a mouse or stylus for color selection. A touch screen selectable color palette must be designed into the application.

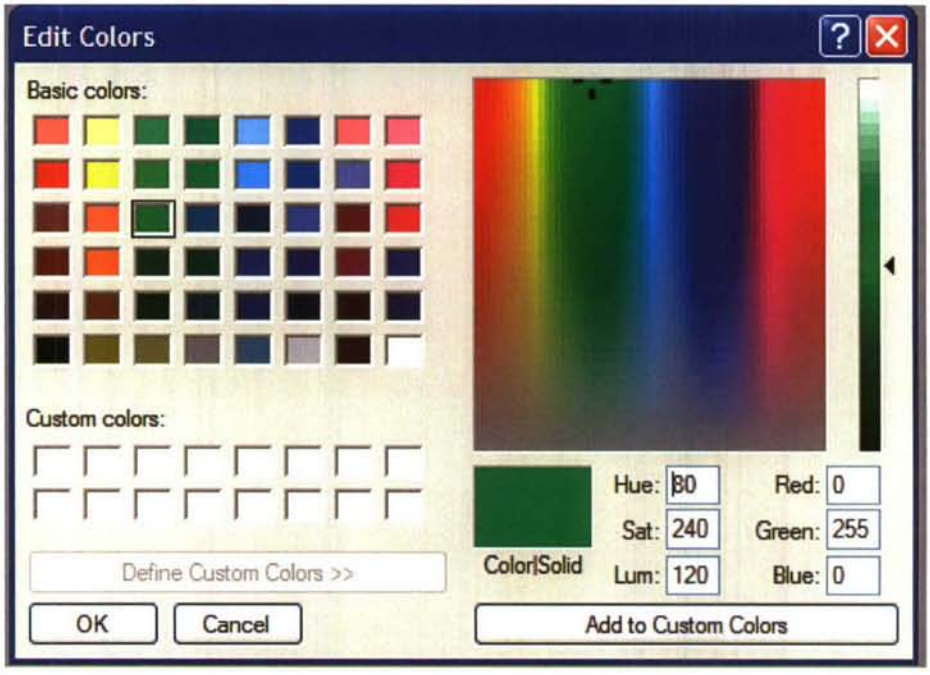


Figure 3-57. MS Windows Color Palette Selection

All speed dial buttons that have a color assigned for the call type will display that color. Figure 3-58 displays a notional screen defining the color purple as the call type.

Figure 3-58. Call Type Button Color Assigned

3.13.7.2 Crypto Colors

Colors for inbound radio calls that are encrypted and un-encrypted follow the color standard used in the TA-970 Secure Red Telephone. The colors Green, Yellow, Red and Blue are not configurable by the user.

- Encrypted radio calls are color-coded green
- Un-encrypted radio calls are color-coded red
- Red Telephone in detect mode is color-coded yellow

- Red Phone and radio disconnected is color-coded blue

3.13.7.3 Audio Selection

The developer must provide independent audio selection for each active connection. The audio of the active connection is configurable. The audio will be assigned to the left, right or both ears of the headset or to the external speakers. The application must also provide a muting / monitor capability for the active connection. Since the communications terminal supports two users headset jacks (two individual users, or one user and one supervisor), the application must also provide a mechanism to switch users to answer their respective calls. Audio selection can occur any time after the call has been answered.

3.13.7.4 Volume Control

Figure 3-57 above depicts a notional screen for volume control for the voice portion of each connection. In addtion to separate voice volume controls, separate ringer volume controls must also exist for each connection. The voice volume information from Figure 3-53 and Ringer Volume Control from Figure 3-59 should be combined make one Volume Control Screen. Figure 3-60 shows the combined Volume Control Screen. This grouping enables the developer to define one button in the permanent section for volume control.

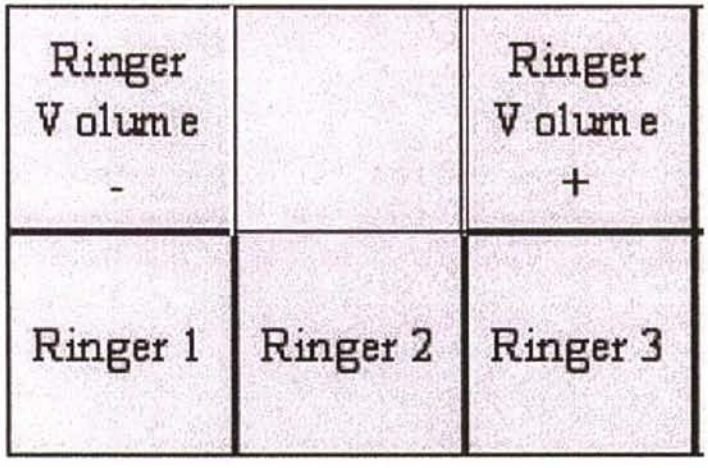


Figure 3-59. Notional Ringer Volume Control

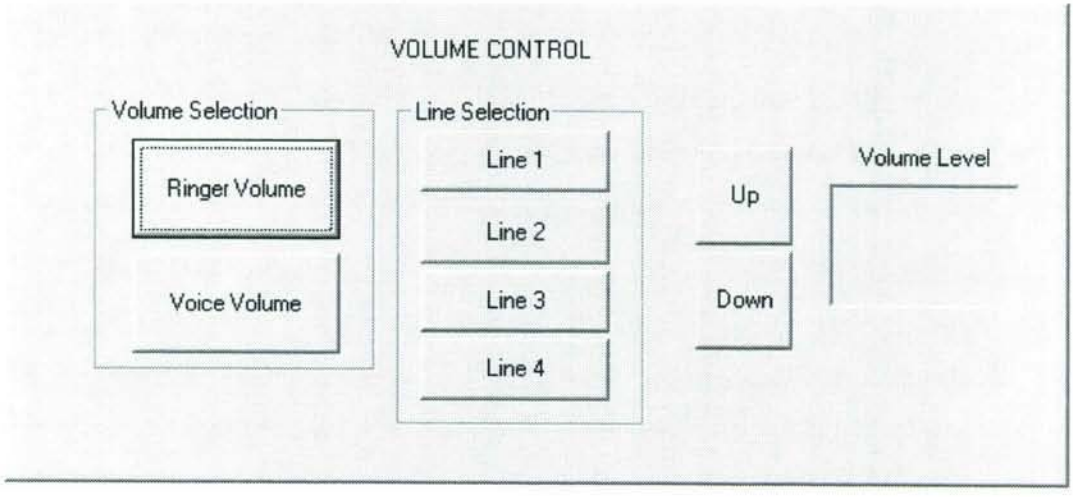


Figure 3-60. Notional Combined Volume Control Screen

3.13.8 Night Mode Operation

Night mode operation refers to operating the GUI display in reduced lighting situations (at night). Communication terminals that reside on the bridge of a ship require the terminal to have a dimmer control for the backlight display and the GUI to change to either "Red Text" on a black background or "Blue Text" on a black background. The blue text is required for night vision goggles.

The developer should carefully consider what button behavior is defined when in full color mode and when in night mode. The button behavior in night modes may vary greatly from its day mode counterpart and may not be readable. Consider a button's call type is defined to be the color red, what is the button's behavior when in the red night mode screen? The same holds true if icons were implemented. In full color mode, icons are viewable but the developer must decide how icons will be handled during night mode operation. Every screen, icon, button, graphic that is displayed in the full color screen must support all night mode colors.

3.13.9 Profile Maintenance

Once a user defines a communications terminal with speed dials, ring tones, volume and ring levels, the entire collection of configurable properties is known as a profile. Currently communications terminals on board Navy ships refer to the configuration items as part of the terminals' properties. For the new VoIP terminals, there will be several profiles associated with each generic VoIP station. The first profile is the supervisory controlled profile that requires a password to open. Second, there are the user profiles that can be stored by unique user login. The developer must again provide a useful mechanism to allow users to easily view, load and store profiles.

3.13.9.1 Supervisory Profiles

Supervisory profiles require the administrator password to open the profile for modification. Supervisory profiles for a station contain one-time setup items that are not changed very often. Take for example, the IP addresses required for VoIP terminals. The new VoIP terminals may require dual homed capability. This means that each VoIP terminal must maintain, open and bind

to two unique IP addresses. The developer must display the active IP connection to aid troubleshooting if required. Other types of supervisory setup items are per-call and line-basis options. Call preemption is a per-call option and call priority is a line basis option.

3.13.9.2 User Profiles

User profiles are initially setup by the function of the duty station where it is installed. The default profile will contain preset speed dial buttons, volume and ring controls. However, each user can define a specific profile with different ring tones, speed dials etc., and load their saved profile when they are on duty. This flexibility allows the user to personalize their profile to fit their working environment.

3.13.10 Call Preemption

VoIP call connections can be subjected to preemption for several reasons. The primary two reasons outlined in reference [99] "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events" are Access Preemption Events and Network Preemption Events RFC 4411.

Access Preemption Events occur when a higher resource priority session is initiated. The lower priority active session is terminated.

Network Preemption Events occur when a higher resource priority session requests increased bandwidth from the router. The router must take action to service the higher resource priority request and terminate lower active resource priority sessions. Each type of preemption event will provide feedback to the communications terminal. The developer must provide either a specialized ring tone or visual acuity.

3.13.11 Call Priorities

The following passage taken from reference [100] "Communications Resource Priority for the Session Initiation Protocol (SIP) RFC 4412" covers why the need for resource priority scheduling is required. "During emergencies, communications resources (including telephone circuits, IP bandwidth, and gateways between the circuit-switched and IP networks) may become congested. Congestion can occur due to heavy usage, loss of resources caused by the natural or man-made disaster, and attacks on the network during man-made emergencies. This congestion may make it difficult for persons charged with emergency assistance, recovery, or law enforcement to coordinate their efforts." On Navy ships, emergencies can and will occur and they require higher priority IP bandwidth. To the user this would just mean placing an emergency call that is color-coded. However, to the developer, whatever color chosen for emergency calls will be reserved and must be not be available to the user. The ability to set each individual call priority is not completely defined. However, the SIP server has the capability to interrupt lower priority resources when the need is realized. If the SIP server interrupts an active session, the initiator of the active session will be notified. The developer must provide call interruption status to the user via a specific ring tone or via a visual indication.

3.13.12 Summary

The developer has a great many decisions to make in order to define a user friendly, efficient and functional Graphical User Interface for the next generation VoIP communications terminal. As previously stated, the developer's role in the GUI development is to present a user interface that is efficient and functional while attempting to minimize the number of operator actions required to navigate. The developer must visualize the user interface through the eyes of the user. That

statement demands that the developer completely understand all user requirements and translate those requirements into a modern graphics design. The developer must hide the complexity of the VoIP terminal behind an easy to operate user interface. The next generation VoIP terminal will support four active connections with advanced user controls which allow the operator to place one call into each ear-piece of the headset. Allowing two simultaneous users provides dual functionality where each user can be connected to two active calls.

3.14 IAC Security

3.14.1 Introduction

VoIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units, and mobile units. In addition to end-user equipment, VoIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Most of these components have counterparts used in data networks, but the performance demands of VoIP mean that ordinary network software and hardware must be supplemented with special VoIP components. Not only does VoIP require higher performance than most data systems, critical services, such as Emergency 911 must be accommodated. One of the main sources of confusion for those new to VoIP is the (natural) assumption that because digitized voice travels in packets just like other data, existing network architectures and tools can be used without change. However, VoIP adds a number of complications to existing network technology, and these problems are magnified by security considerations. [21] VoIP has inherent weaknesses and is vulnerable at multiple points in the framework. VoIP must be secured in order to ensure the availability of the voice system, and to protect the content value and integrity of voice conversations.

The following information was obtained from a Cisco slide presentation on the security threats that exists today. [101]

- Recent trade publications and new reports state that Identity theft is the #1 growing trend.
- 99% of all enterprises network ports are open
- Any laptop can plug into the network and gain access to the network
- 75% of attacks that caused monetary loses were from the inside
- Highest source of loss was theft of proprietary information
- Insider attack by disgruntled employees was listed as likely source by 77% of respondents.

3.14.2 Background

Firewalls, gateways, and other such devices can also help keep intruders from compromising a network. However, firewalls are no defense against an internal hacker. Another layer of defense is necessary at the protocol level to protect the voice traffic. In VoIP, as in data networks, this can be accomplished by encrypting the packets at the IP level using IPSec, or at the application level with secure RTP, the real-time transport protocol (RFC 3550). However, several factors, including the expansion of packet size, ciphering latency, and a lack of QoS urgency in the cryptographic engine itself can cause an excessive amount of latency in the VoIP packet delivery. This leads to degraded voice quality. Careful network design decisions will greatly improve latency.

Packet networks depend on a large number of configurable parameters for their successful operation: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as call processing components (call managers) and other programs used to place and route calls. Many of these network parameters are established dynamically every time network components are restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack [102].

3.14.3 Equipment Involved with Security

3.14.3.1 End Instrument (EI)

An EI is the device that interacts with a user. The EI is usually indistinguishable from traditional telephone sets. Most VoIP systems also support soft phones, which use software running on a common PC to emulate the EI. [38]

3.14.3.2 Call Server

Call servers provide call routing and handle certain services for EIs.
They act similarly to an End Office switch or a Private Branch eXchange (PBX) in the TDM network. They go under various names, such as IP-PBX, proxy, soft switch, Call Session Control Function, gatekeeper (from ITU H.323 terminology), call manager, and local call controller (usually a low capacity switch). Call servers provide two primary roles. First, they provide services for the EI (e.g., registration, presence, advanced call features). Second, they route calls to users on other switches or to other networks (e.g., the PSTN). [38]

3.14.3.3 Media Gateway (MG)

Media Gateways bridge VoIP networks to other networks such as the PSTN. Some MGs provide additional media functions, such as an announcement server or conference bridging. [38]

3.14.3.4 Voice Mail (VM)

As the name suggests, voice mail servers provide voice mail service. VM servers are often paired with the call server such that they service the same set of users. [38]

3.14.3.5 Session Border Controller (SBC)

Session border controllers sit on the edge of a network to isolate the VoIP servers from the public network. Due to incompatibilities between VoIP protocols and firewall or Network Address Translation (NAT) devices (primarily because of the separation of signaling and bearer traffic), SBCs operate in place of a firewall (or in parallel with one). SBCs process signaling messages to open ports for all sessions in and out of the network and block all other traffic. [38] They can also be placed in front of Call Servers to process security at the hardware level.

3.14.3.6 Data Services

Like most IP-based applications, the VoIP servers and EIs require certain data services to operate. Most servers need DNS to process SIP messages. Protocols, such as Remote Authentication Dial In User Service (RADIUS), Simple Network Management Protocol (SNMP), and syslog, are used for management. [38]

3.14.3.7 Routers & Switches

Routers, Ethernet switches, gateways and data servers makeup a typical VoIP network. These network devices provide the logical and physical connectivity of the network. These devices should be considered a viable target for "hackers".

3.14.4 Voice Security

3.14.4.1 Types of Threats

3.14.4.1.1 Theft of Service

Toll Fraud is one type theft of service and is likely the most common attack or exploit that will be seen in the early stages of VoIP deployment. The attack would take the form of an unauthorized user "hacking" and seizing control of an IP Phone and initiating outbound local or long distance calls. Commercial companies will be concerned primarily with toll fraud while government agencies have concerns over disclosure of sensitive information.

Unauthorized Access to or modification of billing records is another theft of service category. A user typically gains access "via hacking" to the centralized billing records and modifies, deletes or alters the records. Commercial companies and government agencies are very concerned since this theft of service affects a larger scale than a single line utilized in toll fraud.

3.14.4.1.2 Unwanted Contact

Unwanted Contact is defined as any contact that either requires prior affirmative consent or bypasses a refusal of consent. Several types of unwanted contact include harassment, extortion, and SPAM. [103]

3.14.4.1.3 Harassment

Harassment is any form of unwanted communication, which embarrasses, intimidates, vexes, annoys or threatens the receiver of the communication with actions, which are improper under the law. [103]

3.14.4.1.4 Extortion

Extortion is any act to induce another to do or refrain from any conduct or give up any freedom, right, benefit or property, under a threat of loss or harm to the person, their reputation, property or the health, safety, reputation or welfare of anyone they know. [103]

3.14.4.1.5 SPAM

Any unwanted lawful content, such as pornography or solicitations of lawful products and services. [103] Content of this type includes Spam Over Internet Telephony (VoIP) (SPIT).

3.14.4.2 Denial of Service (DoS)

The primary goal for Denial of Service attacks is to disrupt network and system operation. The primary target for DoS attacks are system and network resources. This happens to be one of the most common types of attacks faced by data networks. For VoIP, the attack would simply bombard the call processor or managing application with an inordinate amount of simultaneous requests that cannot be processed, causing the application to essentially shut down and deny service to authorized users. Initiated calls in process would be abruptly terminated and newly initiated calls would be unsuccessful.

The following list contains different types of DoS Attacks:

3.14.4.2.1 Flooding

Flooding by definition indicates that more message requests are active on the network than can be processed. There are several different types of flooding: [103]

- Request flooding
- User call flooding
- User call flooding overflowing to other devices
- Endpoint request flooding
- Endpoint request flooding after call setup
- Call Controller flooding
- Directory Service Flooding
- Request Looping

3.14.4.2.2 Malformed Request and Messages

The specifications for control messages in many VoIP implementations are deliberately open-ended to allow for the addition of additional capabilities over time. The downside of this type of specification is that it is not possible to test an implementation either for correct processing of all valid messages or for accurate recognition of invalid messages. As a consequence, valid but complex messages are at risk of being discarded, and the processing systems themselves are at risk if they are sent sufficiently devious invalid messages. The ability of complex invalid messages both to be accepted by a call processing element and to trigger self-destructive behavior in that element creates the threat of DoS via "killer messages." [103]

3.14.4.2.3 Quality Of Service Abuse

Quality Of Service (QoS) abuse involves an attacker violating the QoS negotiated at call setup. For example, the "hacker" could utilize a different media coder from the original coder negotiated at call setup.

3.14.4.2.4 Spoofing Messages

Spoofing Messages is just another way a "hacker" can introduce or insert invalid IP messages into the VoIP signaling path. Depending how well constructed the inserted signaling messages are, they could be accepted as valid messages. The VoIP system now contains valid and invalid signaling messages, which could consume resources and or disrupt call processing.

3.14.4.2.5 Call Hijacking

Once the "hacker" has successfully obtained access to the VoIP network, they have several means to interfere with normal call operation. One common mechanism is to hijack a call in progress by intercepting the end point communications to the call processor. The 'hacker' then impersonates the compromised endpoint and responds to all packets from the call processor. In effect, the 'hacker' has stolen the credentials of a valid endpoint to use maliciously.

3.14.4.2.6 Network Services Denial of Service

A "hacker' may also be able to consume all the available bandwidth on your network by generating a large number of packets directed to your network servers. Typically, these packets are Internet Control Message Protocol (ICMP) ECHO packets, but in principle they may be anything. In addition to network bandwidth, "hackers" may be able to consume other resources that your systems need in order to operate. For example, system data structures, disk storage space, network router and switch ports. Any compromise to system level resources causes traffic backlog, flooding and quality of service issues.

3.14.4.2.7 Physical Intrusion

VoIP Physical Intrusion refers to the compromising of critical network components that are contained within a building, a locked room or closet. Any number of network disruptions can be initiated when physical security of the VoIP components has been compromised. For example, a "hacker" could change port assignments and port security, delete routing tables, insert worms, viruses or even add bogus accounts with sufficient rights on the network. Many network interruptions are possible when physical access to critical network components is not controlled.

3.14.4.2.8 Power Disruption

When network infrastructure components (network servers, switches, routers) lose power, all communication capability of the VoIP and data networks will be lost. Proper network survivability procedures including battery backup or alternate power sources for all major network components are critical. Without alternate power sources for all critical components, the system would be extremely vulnerable to power disruption attacks.

3.14.4.2.9 Resource Exhaustion

Resource exhaustion often refers to interruption of service due to lack of available network resources. Certain types of flooding or SPAM can cause a network or system resource to become bogged down or unresponsive. Typically when some type of flooding is active on the network, multiple network components can demonstrate signs of resource exhaustion.

3.14.4.3 Impersonation or "Spoofing" Threatens Data Integrity

Impersonation is defined to mean altering data to intentionally make it false. Four common types of impersonation or "spoofing" are Identity, Authority, Rights and Content, which are described below. Each type plays an important role in the collection, presentation, and concealment of a sophisticated multi-stage attack known as Phishing.

3.14.4.3.1 Identity

Identity impersonation or fraud is probably the most familiar type of misrepresentation known to the public. Excluding privacy concerns that often mask the identity of a caller, VoIP identity impersonation involves fake caller-ids, fake names or organization names, tampered e-mail, and false presence information. Once a VoIP identity has been compromised, voice calls are placed at the expense of the legitimate account owner.

3.14.4.3.2 Authority

Authority impersonation is defined as either bypassing a legitimate authentication mechanism with a compromised authentication mechanism or presenting false credentials to an authority mechanism to gain access to the system.

3.14.4.3.3 Rights

Rights impersonation is defined as obtaining a false user right that would normally not have been granted to the user.

3.14.4.3.4 Content

Content impersonation or misrepresentation is the platform of choice for "hackers' to glean confidential information. Whether it be an entire bogus website asking for financial information or phone calls with official sounding voice content, each plays a significant part in gathering confidential information. Content misrepresentation plays a large part in phishing schemes. Believable content draws unsuspecting users into the complex world of phishing where personal data is usually compromised.

3.14.4.3.5 Phishing

"Phishing" is a form of Internet fraud that aims to fraudulently acquire sensitive information. Phishing utilizes some or all of the impersonation types listed above. Phishing in the VoIP space contains many similar techniques used in Internet e-mail phishing schemes. VoIP phishing is

presented to the end user as a compromised phone number with legitimate looking (spoofed) caller-id information and asking for your user-id and password.

3.14.4.4 Eavesdropping or "Man in the Middle Exploit"

VoIP Eavesdropping is defined as unauthorized third parties monitoring call signal packets. Eavesdropping provides a 'hacker" with access to user names, passwords and phone numbers and potentially confidential information contained with the VoIP conversation. The following list outlines information that can be gleaned from Man in the Middle Attacks (MitM).

- Call Pattern Tracking
- Number Harvesting
- Conversation Reconstruction
- Voicemail Reconstruction
- Fax Reconstruction
- Video Reconstruction
- Text Reconstruction

3.14.4.5 Interception and Modification

This type of VoIP attack allows the "hacker" to see the data and signaling process end to end. The "hacker" then has the capability of Black Holing calls (dropping entire call), or rerouting calls, degrading or altering the quality of the call, and providing false caller id information.

3.14.4.6 Media Access Control (MAC)Attacks

Insufficient port security subjects the network to MAC Flooding Attacks. Content Addressable Memory (CAM) is the forwarding table for a switch and is filled dynamically based on the source MAC Address. The CAM table stores MAC addresses available on physical ports with their associated VLAN parameters. On most Network switches, CAM tables have a fixed size. If the packet destination MAC Address is unknown the switch floods the frame within the VLAN. If a "hacker" continues sending unknown destination addresses, the CAM table will eventually fill. Once the CAM table is full, traffic without a corresponding CAM entry will be flooded out to every port on the VLAN, technically making the switch act like a HUB. This CAM overflow will cascade to other switches on the network and create network resource and Denial of Service issues.

3.14.4.7 DHCP Attacks

Dynamic Host Configuration Protocol (DHCP) is a protocol for assigning dynamic IP addresses to devices on a network. Dynamic addressing allows a device to have a different IP address every time it connects to the network. DHCP also supports a mix of static and dynamic IP addresses. DHCP can actually lead to trouble for a network. When a host sends out a DHCPDiscovery packet, it listens for DHCPOffer packets and accepts the first offer it gets. Part of the accepted DHCPOffer is the address to which the host should set its default gateway. If a "Rogue" DHCP is on the network the potential exists for that rogue server to respond to the DHCPOffers If the host uses the DHCPOffer from the rogue server, the host could end up using the rogue server as its default gateway or DNS server. Rogue DHCP servers provide fake Domain Name Servers (DNS) and allow for Man in the Middle attacks.

3.14.5 Threat Defense Strategies

VoIP networks represent high-value targets for attacks and represent a greater risk to network security than most other network applications. It is imperative that the voice network and supporting data networks are secured as tightly as possible to reduce the impact that an attack can have on either network. Segregating voice traffic from data traffic greatly enhances the security and availability of all services. Further subdivision of the voice and data networks can enhance security. Reference [7] The following subjects touch on security at several different layers. The primary defense strategy is to apply security to many levels. The lower the level of exploitation the more options and tools the "hacker" has at their disposal.

3.14.5.1 Layer 2 Protections

Layer 2 switches found at the access layer provide high port density for both host and IP phone connectivity as well as Layer 2 services such as QoS and VLAN membership. "Layer 2 network segregation is the second layer in our layered defense approach to VoIP security. Voice traffic must be isolated from data traffic using separate physical LANs or Virtual LANs. The combination of data and voice segregation and segmentation using VLANs along with a switched infrastructure strongly enhances the security posture of the system. This also helps mitigate call eavesdropping and other attacks." Reference [7]

3.14.5.2 Voice Virtual Local Area Networks

Reference [7] states that VLAN technology has traditionally been an efficient way of grouping users into workgroups to share a specific network address space and broadcast domain regardless of their physical location on the network. Hosts within the same VLAN can communicate with other hosts in the same VLAN using layer-2 switching. In order to communicate with other VLANs, traffic must transit through Layer 3 devices where it can be filtered and routed. VLANs can offer significant benefits in a multi-service network by providing a convenient way of isolating VoIP equipment and traffic from the data equipment and traffic. When VLANs are deployed, excessive broadcast and multicast packets present in the normal data traffic will not disrupt VoIP services. As with data networks, VoIP equipment and instruments should be logically grouped using multiple VLANs such that IP Phones share their VLANs only with other IP Phones, gateways share VLANs with like gateways, and so on. Each type of VoIP device would have mutually exclusive VLANs. This forces Layer 3 routing and thereby enables all the filtering capabilities of the Layer 3 devices.

Reference [7] also suggests grouping certain VoIP devices together:

- Call processing and voice DHCP servers
- Directory servers
- Message servers and/or servers that might be accessed from both the data network and the VoIP network.
- Gateways – possibly multiple VLANs for multiple types of gateways
- Wide Area Network (WAN) Access firewalls
- VoIP phones with possible subdivision by department or organization
- Data workstations with soft phones.
- VoIP device management

Reference [7] The voice network will be subdivided into multiple VLANs to segregate VoIP devices by type and function. At a minimum, this shall include five VLANs containing the following:

- call control servers, message servers (voice-mail
- e-mail, unified), gateways
- VoIP phones
- workstations with soft phones.

Once a user or device has connected to the network, services that the client has access to should be based on individual need and only if that individual or workstation is authorized. This restriction can only be implemented by first determining if the individual, workstation, or IP phone is authorized to connect to the network and then insuring that it is assigned to the appropriate VLAN. Several methods used today for authenticating Layer 2 access and VLAN membership are as follows:

- Port security
- Port authentication with 802.1X
- VLAN Management Policy Server (VMPS)

3.14.6 Port Security

The port security feature provided by most switch vendors can be used to block input to the access port when the MAC address of the station attempting to access the port does not match any of the MAC addresses specified for that port, that is, those addresses statically configured or auto-configured (i.e., "learned). The maximum number of MAC addresses that can be configured or learned (or combination of both) is also configurable. Reference [8]
Port Security threats are described in the following paragraphs.

3.14.6.1 MAC Attacks

MAC Attacks flood the VLAN with unknown destination addresses. This attack will eventually fill the CAM table. To resolve this attack port security limits must be added and the number of allowed MAC addresses allowed per interface port limited.

3.14.6.2 DHCP Attacks

Rogue DHCP servers provide fake (Domain Name Servers) DNS and allow for Man in the Middle attacks. To resolve this attack DHCP Snooping must be utilized.

3.14.6.3 DHCP Snooping

To protect VoIP systems from Rogue DHCP Servers, a technique called DHCP Snooping needs to be implemented. DHCP Snooping dynamically builds and maintains a database using information extracted from intercepted DHCP messages. The database contains an entry for each un-trusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces.

DHCP Snooping creates the following features:

- Binds IP addresses to MAC Addresses
- Sets up Trusted and Un-Trusted Interfaces
- Defines ports that can issue DHCP replies
- Limits the rate of DHCP messages that can be received
- Resets if the link is lost.
- Drops all replies from non-trusted DHCP Servers.

Address Resolution Protocol (ARP) is the protocol that links MAC & IP Addresses. The switches need to block Gratuitous ARP (GARP) issued by the IP phones. This will prevent malicious devices from assuming the identity of something else to become the Man in the Middle.

ARP Spoofing is when a hacker sends fake MAC/IP address bindings to redirect traffic to the hacker. This breaches confidentially and integrity. The solution again is DHCP Snooping. DHCP Snooping will learn trusted bindings and drop all non-trusted bindings.

3.14.7 Port Authentication with 802.1X

While technologies, such as MAC filtering and ACLs, are used to enhance overall network security, the IEEE 802.1X Port Based Network Access Control specification provides another level of network protection. Authentication through IEEE 802.1X provides the ability to limit network access based on a client profile. A client profile typically contains the client identification and access privileges. Data cannot be passed through the switch and onto the LAN until the client's identification has been verified. There are several benefits gained by implementing 802.1X on all edge or access layer switches. The secure authentication allows a client to be recognized and granted access privileges from the location he or she logs on. It can also account for a client's activity while they are connected to the network. The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before allowing connectivity. The switch port state determines whether or not the client is granted access to the network. Reference [8]

The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before allowing connectivity. The switch port state determines whether or not the client is granted access to the network. The port starts in the "unauthorized state." While in this state, 802.1X access control only allows Extensible Authentication Protocol Over LAN (EAPOL) traffic through the port to which the client is connected. The EAPOL traffic facilitates the authentication process between the client and the access servers. When a client is successfully authenticated, the port transitions to the authorized state allowing all traffic for the client to flow normally. Only one client can be connected to the 802.1X-enabled switch port. Reference [8]

EAPOL is a delivery mechanism and does not provide the actual authentication mechanisms for the protocol. When utilizing 802.1X, an Extensible Authentication Protocol (EAP) type must be chosen to define how the authentication is to take place. The specific EAP type resides on the authentication server and within the operating system or application software on the client devices. During negotiation, the switch sends the identity to an authentication server. EAP is defined by the IETF and can be further researched at (http://www.ietf.org). The 802.1X standard describes how to send and receive EAP over IEEE 802 LANs (EAPOL). In order to deploy 802.1X, an

authentication method/type must be selected in order to transmit inside this EAPOL envelope. The following are some methods that may be considered and are described in greater detail in Reference [8].

- Transport Layer Security (EAP-TLS)
- EAP Tunneled Transport Layer Security (EAP-TTLS)
- Protected EAP
- Lightweight EAP (LEAP)
- EAP-MD5

3.14.8 VLAN Management Policy Server (VMPS)

A VLAN Management Policy Server allows a switch to dynamically assign VLANs to users based on the workstation's MAC address or the user's identity when used with the User Registration Tool. A switch is configured and designated as the VMPS server while the remainder of the switches on the segment act as VMPS clients. The VMPS server opens a UDP socket to communicate and listen to client requests using VMPS Query Protocol (VQP). When the VMPS server receives a valid request from a client, it searches its database for a MAC address-to-VLAN mapping. If the assigned VLAN is restricted to a group of ports, VMPS verifies the requesting port against this group. If the VLAN is allowed on the port, the VLAN name is returned to the client. If the VLAN is not allowed on the port, the host receives an "access denied" response when VMPS is not configured in secure mode or the port is shut down if in secure mode. Reference [8]

VQP is an UDP-based protocol that does not support any form of authentication and the data is transmitted in clear text. This makes its use in security-sensitive environments inadvisable. An attacker who is able to spoof VQP could prevent network logins with a DoS attack to the VMPS server or even join an unauthorized VLAN. Furthermore, a VMPS database configuration file is nothing more than an ASCII text file that is stored on a TFTP server and downloaded to the VMPS server at startup or when the VMPS server is first enabled on the switch. As noted in previous sections, a network component should not use TFTP to upload or download configuration files. For these reasons, VMPS must not be used to provide port authentication or dynamic VLAN assignment. Reference [8]

3.14.9 Switch Management

Reference [8] states that securing administrative access to all switches is critical to maintaining stability and integrity within the network infrastructure. Administrative access to any switch by unauthorized personnel provides a mechanism to not only disrupt service at the core or access layers, but also break down the security provided between VLANs, including the access to the network's Out-Of-Band (OOB) management VLAN. In order to control and authorize administrative access, an authentication server that provides user authentication as well as authority level validation will be implemented

Reference [8] outlines the following rules for securing switches:

- An Authentication server is required to gain administrative access to all switches
- Only one account defined on the switch for Administration access
- Each user will have an account (username/password) to access the switch.
- Each user account will be assigned the lowest privilege allowed to perform their duties.
- Access will be removed from unused accounts when no longer required
- Passwords are not visible when viewing switch configurations.

Out of Band switch management utilizes the console port or OOB – VLAN. The local console port will be required to timeout from inactivity when an Administrator has logged in. In-Band switch management utilizes the data network path and is not recommended. This would expose username/password and device info to the data network and is susceptible to network sniffing. In-Band switch management can be locked down with Access Control Lists (ACL's) and encryption. However, from a security standpoint, the preferred method for switch configuration is via OOB access.

3.14.10 VLAN and VLAN1 Management

By default, all ports, including the internal sc0 interface, are configured to be members of VLAN 1. In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to transport Layer 2 control plane traffic such as the following:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- VLAN Trunking Protocol (VTP)
- Uni-Directional Link Detection (UDLD)
- Port Aggregation Protocol (PAgP)

This is all untagged traffic. As a consequence, VLAN1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly. The risk is even greater if VLAN1 is also used for user VLANs or the management VLAN. In addition, it is unwise to mix management traffic with user traffic making the management VLAN an easier target for exploitation. Reference [8]

3.14.11 Layer 3 Protections

3.14.11.1 IP Address Segregation

Reference [7] states that further subdivision of the voice and data networks can enhance security. Logical segregation of VoIP components and data components can be accomplished at both Layer 2 using Virtual Local Area Networks (VLANs) and Layer 3 using IP addressing. Layer 2 and Layer 3 separation provide a derived security benefit of address hiding. Knowing the address of one layer does expose the addressing of the other layer. Switches, routers and firewalls provide Access Control Lists (ACL's) to control traffic between different network components. To segregate IP addresses, the network devices can be grouped and addressed by component type. That is to say that call managers, Media Gateways, Voice Mail, and IP phones will be grouped into logical subnets or VLANs. This subnet will use a different major address range than the local data network. It could also be argued that Non-Routable RFC 1918 "Private IP Addressing" could be

utilized to separate the VoIP network from the data network. This type of addressing would reduce the possibility of voice traffic finding its way onto the data network and data network traffic finding its way onto the voice network.

3.14.12 VoIP Security Protocols

This section provides details about security protocols available to secure VoIP systems. It presents a few such technologies along with a brief description of each. Some protocols have deficiencies that need to be addressed before considering them for use in a DoD network.

3.14.13 Internet Public Key Architecture

Because the Internet is an openly connected system of hosts, security over the Internet depends on the procedures for one host to authenticate another. Symmetric techniques, such as shared secrets and passwords, scale poorly since each host needs to maintain a secret for every other host before communicating with that host. A number of systems on the Internet today use a public key infrastructure. The most common example is secure HTTP. Other examples include S/MIME for e-mail and digital rights management (DRM) systems. In such a system, each host has a public certificate and a private key. Public key cryptography has a number of properties that make it suitable for authentication in an open network. Signing and verifying digital signatures are basic operations for public key algorithms, such as Rivest, Shamir, Adleman (RSA) [104] and Digital Signature Algorithm (DSA) [105]. (In fact, the only two operations DSA provides are signing and verifying.) In general, these algorithms work by first calculating a hash (e.g. MD5 [106] and SHA [107]) of the data being signed, and then performing a calculation on that hash with the private key. To verify the signature, the user starts with the original data, calculates the hash, and then performs a calculation on the hash and the public key such that the output is true if the signature is valid and false otherwise. For RSA, the signing procedure amounts to encrypting the hash; the verification procedure decrypts the signature and compares the results with the original hash (the signature is verified if and only if they match). With public key cryptography, each user has a key pair: a private key that the user holds as a secret and a public key that can be published. This is in contrast to traditional symmetric cryptography (e.g., DES [108] and AES [109]) where there is a single key used for both encryption and decryption.

With public key cryptography, it is possible for two parties who have no prior association to communicate securely (though a Man in-the- Middle (MitM) attack at this point is possible). To support authentication and to avoid the MitM attack, public key systems use a trusted third party, the Certificate Authority (CA), to vouch for the authenticity of the public key and the identification of the key's owner. Systems like these are called Public Key Infrastructures (PKIs). Typically, one uses a certificate that contains these data: the public key, the owner's identity, and the CA's digital signature. Certificates like these often use the ITU-T X.509 data format [110]. It is also possible for one CA (e.g., a root CA) to distribute responsibilities to supporting CAs. In such a case, the root CA signs the certificates of the other CAs. This creates a hierarchical trust relationship between CAs (up to the root CA).

For example, given Alice's certificate, Bob can validate its authenticity by verifying the CA's digital signature. For authentication, the underlying protocol needs to have Alice sign some unique data (e.g., a timestamp or a random nonce generated by Bob). This step requires the user (presumably Alice) to apply Alice's private key. If Bob verifies Alice's signature in the response,

he knows that Alice signed it because the valid signature demonstrates that the user possessed (and used) her private key, which, by assumption, only Alice knows.

It is important to note that the CA is only used during the certificate enrollment process where the CA signs the initial certificate request. During normal operations, no communication with the CA is required.

Note that the security of the system relies entirely on the assumption that the private key is held in secret. Anyone who obtains (e.g., steals) a user's (or CA's) private key may impersonate that user. Also note that the parties need to have a common trusted CA. Typically, each host is provisioned with a list of trusted CAs. For example, a typical web browser today might ship with 100 different CA certificates from 40 different companies (e.g., VeriSign, RSA Security Inc., Thawte, etc.).

Another concept for PKI is certificate revocation. Certificate revocation is the process of revoking (or invalidating) potentially compromised certificates. For example, if a user loses a computer containing his private key, he might request that the CA provide a new certificate and revoke the old one. That way, if the private key were stolen, the thief would not be able to use the revoked certificate to impersonate the original owner. Protocols, such as Online Certificate Status Protocol (OCSP) RFC 2560[37], exist for checking or distributing certificate revocation lists (CRLs) from CAs. Although most CAs and some applications (e.g., Firefox) support protocols like OCSP, they are rarely used today. Periodic or manual installation of CRLs is more common. The DoD has adopted the PKI concept for its networks [111]. The PKI system for the DoD is based on the public X509 specification, with certain added constraints [103][112][9].

3.14.14 Transport Layer Security

Transport Layer Security (TLS) is a standard RFC 2246 [113] for secure connection-oriented Internet sessions. The IETF created the open standard which is nearly identical to Netscape's Secure Socket Layer (SSL) Version 3.0. These protocols are commonly used for securing World Wide Web (WWW) traffic as HTTP over TLS (RFC 2818[114]; https://). TLS is generally used with public key encryption algorithms (e.g., RSA or DSA) during the initial handshake to establish authentication and to exchange ephemeral session keys.

During this handshake, both parties exchange public key certificates. The certificates use the standard ITU-T X.509 data format and follow procedures described, for example, in RFC 2459[115] (Internet X.509 Public Key Infrastructure Certificate and CRL Profile). Certificates can be generated on the spot, which are called self-signed. The CA or trusted host signs other certificates. The certificate has a field for the CA to sign. Anyone can verify the authenticity of an X.509 certificate by performing specific calculations (specified by the public key cryptosystem, e.g., RSA). In the next exchange of messages in the TLS handshake, each participant signs a nonce (random number or timestamp provided by the other participant) with his private key and sends the result back. The public key algorithm provides an algorithm to verify that the signature is valid (i.e., that the signer knows the private key necessary to calculate the correct signature). This step provides authentication and protects against the possibility of a MitM attacker.

For securing HTTP, it is common for the client to authenticate the server, but not for the server to authenticate the client. That is, the client validates the authenticity of the server's public key certificate, and the server automatically accepts the client's certificate as valid. This is usually

[9] More information about the DoD PKI system can be found at http://iase.disa.mil/pki/.

acceptable for WWW traffic because (a) client support for certificates is a recent development and (b) when user authentication is required, username/password authentication is easier to manage.

In the context of this report, all TLS sessions will use mutual authentication. Mutual authentication means that both parties validate the certificates they receive in the initial handshake of the TLS protocol. This process not only provides authentication of the server's identity, but also authenticates the client (e.g., the EI).

3.14.15 Secure RTP (Secure Real Time Transport Protocol)

Secure Real-Time Transfport Protocol (SRTP) RFC 3711[116] increases confidentiality and integrity to standard RTP. It does so by encrypting the payload part of the RTP packet and appending an HMAC authentication value over the contents of the original RTP packet. Figure 3-61 shows the format of an SRTP packet. The green portion (payload and padding) is encrypted. The orange portion (usually only the authentication tag is used) contains cryptographic values (e.g., the Hashed Message Authentication Code (HMAC) value). The yellow portions (primarily the header fields, which are defined in RFC 3711) are passed in cleartext. Thus, the content of the yellow portions is visible to an eavesdropper, though the Authentication Tag protects an attacker from modifying the yellow fields without being detected.

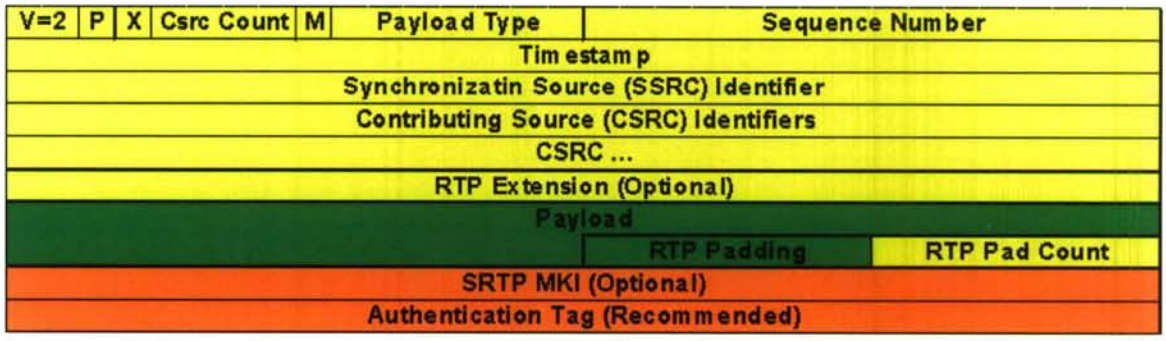


Figure 3-61. SRTP Packet Format

SRTP requires a shared master SRTP key. The standard defines a procedure to generate other keys, such as the encryption key and the authentication key from the master key. Instead of stating a specific protocol to exchange the master SRTP key, the standard relies on the signaling protocol to exchange the key.

Session Description Protocol (SDP) Security Descriptions for Media Streams (RFC 4568[22]) is emerging as the de facto standard for exchanging the master key. SDP assumes that the signaling protocol (e.g., SIP) provides its own security (e.g., using TLS or IPSec) and passes the key (otherwise in the clear) inside the SDP body within a SIP message.

Alternatives, such as Multimedia Internet Keying (MIKEY [117][118]), negotiate key exchanges by exchanging cryptographic data over multiple SIP messages. Such techniques may be useful when traversing un-trusted servers (e.g., across multiple providers). Interoperability with MIKEY solutions is difficult today due to issues such as algorithm negotiation and compatibility.

3.14.16 IPSec Internet Protocol Security

IPSec is a set of IETF standards (e.g., [119]) for securing Internet traffic. IPSec operates at Layer 3 (the network layer) and hence protects any type of Internet traffic, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP), regardless of the application. Commercial Virtual Private Network (VPN) solutions commonly use IPSec for secure remote access.

IPSec can operate in either of two modes, transport mode or tunnel mode (Refer to Figure 3-62). In transport mode, the original IP header is unmodified (passed as cleartext). In tunnel mode, a new outer IP header encapsulates the original IP header, such that the original IP header can be encrypted and protected end-to-end. Tunnel mode may be used between routers (or VPN gateways) to protect the privacy of the end hosts behind each router or gateway.

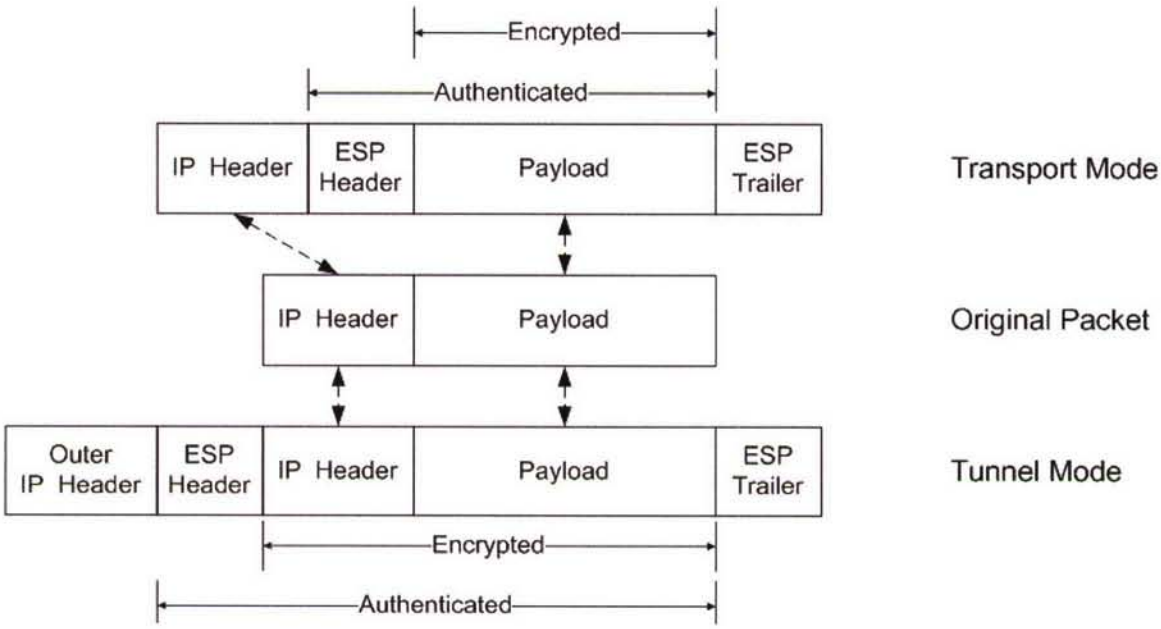


Figure 3-62. IPSec Modes

Transport mode is slightly more efficient than tunnel mode because tunnel mode needs to pass both IP headers. This overhead is usually insignificant, but for protocols with numerous, small packets (as would be the case for RTP), an overhead of 20 bytes per packet is large compared with a 32-byte RTP packet from a G.729 compressed codec.

IPSec defines two protocols, Authentication Header (AH)[120] and Encapsulated Security Payload (ESP)[121]. It also defines an abstract protocol, Internet Security Association and Key Management Protocol (ISAKMP)[122] for key management. Internet Key Exchange (IKE)[123] is the de facto standard protocol that implements ISAKMP.

The AH provides authentication (and integrity) over the entire IP packet (except specific mutable fields, such as Time to Live (TTL) and checksum that are expected to change as the packet is routed), but does not provide encryption. This mechanism provides integrity and authentication, but does not provide privacy.

The ESP provides encryption and authentication (and integrity) for the packet payload, but not for the IP header. We assume that the authentication value is always provided, though, strictly speaking, the standard makes its use optional. Although the standard allows use of both AH and

ESP in the same packet, this combination is almost never used since ESP provides authentication by itself.

Hosts (or gateways) use IKE to exchange the session keys (used for encryption and authentication) securely for an IPSec session, or Security Association (SA). The actual key exchange uses the OAKLEY key determination protocol (described in RFC 2412[124]), which is a simple variation of the famous Diffie-Hellman (DH) key exchange. The original DH exchange [125] is vulnerable to a MitM attack. The OAKLEY algorithm adds a cryptographic value to the exchange then requires an operation using either a pre-shared secret or private key (with a public key certificate) to authenticate the keying material used in the DH exchange in order to prevent the MitM attack.

The IKE protocol uses a four-message exchange to establish the shared key. Older versions of IKE (e.g., RFC 2409[126]) supported a few different message exchanges requiring different numbers of messages. The protocol typically runs on UDP port 500.

The most common VPN gateway implementations use IKE to set up (and rekey) an SA. That SA is then used to secure a tunnel mode IPSec session with the ESP. In scenarios where IPSec runs to the end host, tunnel mode and transport mode are equally common.

In the recent past, the only options for providing IPSec were (a) use of a VPN gateway or (b) an IPSec host client. The VPN gateway sits on the network (like a router) and passes all traffic through an IPSec tunnel (in tunnel mode) to a remote location, where another VPN gateway decrypts the packets. The IPSec host clients support remote access VPNs by forcing *all* traffic to and from the host across a tunnel mode IPSec tunnel to a remote access server, which decrypts the IPSec packets and passes the packets as if they were generated from a host, collocated with the server.

In recent years, OS support for IPSec has improved dramatically. IPSec is an add-on to Ipv4 but is native to Ipv6. IPSec support is tied to the OS's IP stack and routing functions. This gives engineers a considerable amount of flexibility in how they configure IPSec. For a typical server, the administrator might add virtual IP interfaces over a single physical Ethernet interface. The administrator could then create IPSec sessions (in either transport mode or tunnel mode) between the virtual IP interfaces and interfaces on remote hosts. For example, one virtual IP interface could connect to a management network using tunnel mode and another virtual interface could connect to another host (e.g., a log host to archive billing records) using transport mode. The network route table inside the OS would select the appropriate IPSec tunnel based on each packet's destination IP address; any packet using an address not assigned to one of the IPSec routes would use the default (public) interface to send the packet unencrypted. This type of flexible OS configuration (which Solaris, Linux, and recent Windows operating systems support today) allows hosts to apply IPSec selectively to certain hosts or networks and to communicate with hosts on other networks without IPSec, thus supporting encrypted and non-encrypted sessions from the same host.

3.14.17 Conclusion

Security is probably the most important part of a converged network consisting of voice and data streams. Aside from the normal security issues revolving around e-mail, network infrastructure and virus scanning, security for the voice must be designed up front. There is no point to deploying a VoIP system without ensuring that the data network is as secure as possible. Adding

VoIP to an existing installation requires a robust security analysis prior to making design decisions since security features to lock down the VoIP system can and will have an impact on data throughput.

Firewalls, gateways, and other such devices can also help keep intruders from compromising a network. However, firewalls are no defense against an internal hacker. Additional layers of defense are necessary at the protocol level to protect the voice traffic. In VoIP, as in data networks, this can be accomplished by encrypting the packets at the IP level using IPSec, or at the application level with secure RTP, the real-time transport protocol (RFC 3550). However, several factors, including the expansion of packet size, ciphering latency, and a lack of QoS urgency in the cryptographic engine itself can cause an excessive amount of latency in the VoIP packet delivery. This leads to degraded voice quality. Careful network design decisions will greatly improve latency.

Remember that VoIP is data and is transmitted in digital packet form. This means that the voice transmissions can be now attacked, hacked, intercepted, manipulated, re-routed and degraded just as any data packet on the data network can. Viruses, worms, Trojan horses, denial of service attacks and hijacking are all possibilities on the VoIP network.

Security must be implemented in a layered approach. This means that security has to involve the entire system. Each component must have a focus on security. Starting with the End Instrument (IP Phone) by hiding the phone/network parameters. Next the Call Servers, Media Gateways, Session Border Controllers and all Routers, Switches and Firewalls must all be locked down requiring administrative access for management changes and UserId/Password for use. Also, many of the data network precautions such as virus scan software and an effective patch management system need to be in place to keep the soft phones, servers and Personal Computers up to date. Next all voice streams and call signaling should be encrypted, ideally end-to-end. Voice should be encrypted with Secure RTP (SRTP) using 128-bit AES. Signaling should use SSL/TLS wherever possible or alternatively IPSec can be used to encrypt everything.

From a purely network approach security can be applied by segregation. Each type of VoIP equipment type should be allocated to their own Virtual Lans (VLANs). VLANs are used to segment voice components and to segment the data network. Softphones that require access to both the voice and data VLANs should be allocated with care. Security studies from National Security Agency (NSA) and Defense Information Systems Agency (DISA) strongly suggest not using softphones or greatly limiting their use.

Physical network security with regards to critical network components, computer rooms, wiring closets, server rooms must have their access controlled at all times. Many network disruptions can be initiated when physical security of the VoIP components has been compromised.

Software management and updating require secure access. The following list outlines some common management recommendations:

- Remote management should only be performed over encrypted connections.
- Proper password management techniques should be used.
- Any default passwords must be changed. Passwords need rotation.
- System actions should be logged with appropriate audit capabilities.

- Only secure connections should be used for web access, i.e. Secure Socket Layer/ HyperText Transfer Protocol Security (SSL/HTTPS).
- Set software loads should be encrypted and tamper-proof.
- Network Service provider should run the minimum of services required.
- Connection of a set to the system must require an initial authentication and authorization." [127]

To summarize, all VoIP traffic should be encrypted. There are multiple options including VPNs, SRTP (Secure RTP) and IPSec, but making sure that the selected encryption method is efficient and fast is a critical design issue. Otherwise, performance and throughput may be negatively impacted. Actively monitor for unauthorized or non-compliant technologies supporting the VoIP network. This includes identifying devices with non-standard configurations. Make VoIP servers physically secure by adopting technologies such as firewalls and intrusion detection. Use firewalls that can handle the unique attributes of VoIP traffic. Require all users to login to access the VoIP network. A VoIP handset should be treated no differently than a user's computer where network access is governed by login and password.

This page intentionally left blank.

3.15 IPv4 vs. IPv6 Comparison

3.15.1 Executive Summary

In general, no significant increase in bandwidth should result from the increased header size of IPv6 as analyzed in the scenarios in 3.15.3.8 with different size payloads. On the other hand, due to the increased address space and by intended modification of the header, many benefits are designed into IPv6, such as, auto-reconfiguration, improved multicasting, address aggregation, flow treatment for QoS, and additional security features.

It was also analyzed and indicated why IPv6 routing elements should perform better as some of the performance bottlenecks such as, fragmentation, checksum processing, and addressing reduces the processing functions. Except in bandwidth-limited tactical or radio networks where only short, interactive messages are communicated, IPv6 should not pose any issue. In such cases, compression techniques can mitigate the impact further.

In any case, such networks need to be tested and compared for their efficiency as well as capability of satisfying requirements in assured services, assured delivery, and information assurance.

3.15.2 Introduction

IPv4 has been a strong catalyst to the worldwide adoption of today's Internet and facilitated many packet switching networks around the world. The initial RFCs written in the 1980s (RFC 760, RFC 761, RFC 791, RFC 792, and RFC 793) were instrumental in TCP/IPv4 implementation. However, the protocol planners did not anticipate the worldwide interest and commercial growth possibilities as they expected it to be a communication vehicle for research entities within the US Government research agencies and Universities only. The phenomenal growth of packet switching networks and the demand of hosts requiring new IP addresses have created issues with a depleted address pool. The historical allocation of IPv4 addresses from the 32-bit address field in the IPv4 packet header by Classes has created a very uneven distribution. Adding to the issue of depleting address pool, the exponential growth of new applications enabling various multimedia services with mobility, and local (home or premises) networking requires IP addresses for a myriad of devices, such as, mobile phone-data-video equipment, PDAs, game-boxes, and all sort of home devices. IPv6 is the intended successor of IPv4 to counter the addressing issue. While the address size is the most obvious difference between IPv4 and IPv6, IPv6 contains other additional features that bear a comparison. These are addressed in the following sections.

3.15.3 Comparison

There are a number of features of IPv6 that will have a positive impact on network performance and its relationship to real-time applications such as VoIP and VioIP on an data network. These features are summarized in Table 3-33 and are discussed in further detail in the following sections.

Table 3-33. Feature Comparison Summary

Topic	Ipv6	Ipv4	Section
Large Address Space	128-bit address	32-bit address	3.15.3.1
Header	40 bytes	20 to 60 bytes	3.15.3.2
Anycast	New routing scheme	Not available	3.15.3.3
Multicast	Integral	Optional	3.15.3.4
Auto-configuration	Stateless & Stateful	Stateful	3.15.3.5
NAT Relevance	Not necessary	Relevant/Useful	3.15.3.6
Scoped-Address	Available	Not available	3.15.3.7
Overhead	40 bytes (fixed) per packet	20 bytes (min) per packet	3.15.3.8
Routing Protocols	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Neighbor Discovery (ND)	RIP, OSPF	3.15.3.9
Address Aggregation	Produces smaller routing tables	Potentially large routing tables	3.15.3.10
Link-Layer Address Resolution	Uses ND	Uses Address Resolution Protocol (ARP)	3.15.3.11
Checksum	Not part of the IP header	Part of the IP header	3.15.3.12
Fragmentation	Handled by end-hosts	Handled by routers	3.15.3.13
QoS	Uses "Flows" for optimized routing.	Performed by examining and parsing multiple header fields	3.15.3.14
Security(IPSec)	Integral	Optional	3.15.3.15

3.15.3.1 Large Address Space

IPv6 introduces a 128-bit address field compared to a 32-bit address field in IPv4 to support more addressing levels. In a rudimentary way, it indicates that there are 2^{128-32} or 2^{96} more addresses available in IPv6. However, due to the way IPv4 addresses are sub-netted, defined for multicast, reserved for future and experimental use, sub-netted with variable length subnet masks, and scoped, the actual contrast is less obvious than the simple factor.

The IPv4 32-bit address space was classified in the way shown in Figure 3-63:

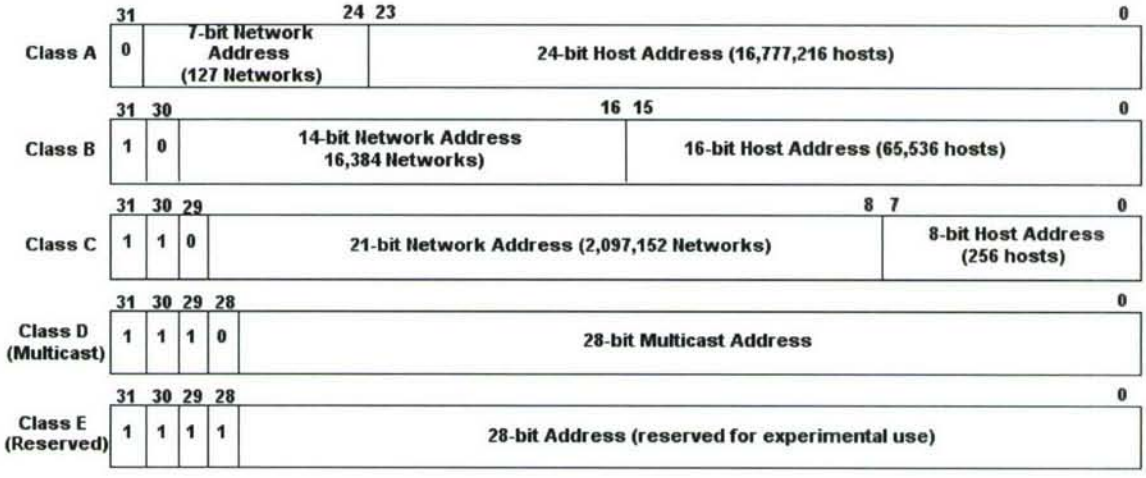


Figure 3-63. Ipv4 Address Allocations

This indicates that $7/8^{th}$ or the majority of the IPv4 address space is designated for global unicast addressing, and relatively little $1/16^{th}$ being designated for multicast, and another $1/16^{th}$ for future use.

IPv6 defines three types of addresses – unicast, multicast, and anycast, including some special sub-types of global unicast, such as IPv6 with embedded IPv4 addresses. In IPv6 the prefix of 001 identifies global unicast addresses, so $1/8^{th}$ of the address space or 2^{125} such addresses are designated.

3.15.3.2 Header

The IPv6 header has a new format that is designed to keep header overhead to a minimum. This is achieved by moving both non-essential fields and optional fields to extension headers that are placed after the IPv6 header. The streamlined IPv6 header is more efficiently processed at intermediate routers.

IPv4 headers and IPv6 headers are not interoperable. IPv6 is not a superset of functionality that is backward compatible with IPv4. A host or router must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats. The new IPv6 header is only twice as large as the IPv4 header, even though IPv6 addresses are four times as large as IPv4 addresses. Figure 3-64 and Figure 3-65 show the header formats of IPv4 and IPv6 respectively.

<table>
<tr><th>Bits 0-3</th><th>4 - 7</th><th>8-15</th><th>16-18</th><th>19-31</th></tr>
<tr><td>Version</td><td>Header Length</td><td>Type of Service</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Options (10 max.)</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Figure 3-64. IPv4 Header Format

<table>
<tr><th>Bits 0-3</th><th>4 - 7</th><th>8-11</th><th>12-15</th><th>16-23</th><th>24-31</th></tr>
<tr><td>Version</td><td colspan="2">Traffic Class</td><td colspan="3">Flow Label</td></tr>
<tr><td colspan="3">Payload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Figure 3-65. IPv6 Header Format

In IPv6, five fields from the IPv4 header have been removed due to the fields either not being needed by IPv6 or being implemented through the extension headers. These changes to the header format will improve the packet processing speed of routers. The IPv4 header fields removed are described in Table 3-34.

Table 3-34. IPv4 Header Fields Removed from IPv6

IPv4 Field Removed	Reason for Removal	Impact on Routing Performance
Header Length	Not needed in a header with a fixed length. The IPv4 header has a variable length.	Increases router performance since headers of fixed length are easier to parse then headers of variable length.
Identification	This field is used to identify packet fragments during the re-assembly of the packet. Not needed since IPv6 routers do not do packet fragmentation.	Increases router performance since fragmentation is relegated to the end-hosts and is not a router function. In IPv6 the router does not need to perform packet fragmentation.
Flags	This field consists of two flags and is used to determine if a router should perform fragmentation and whether or not more fragments are to follow the current one. Not needed since IPv6 routers do not do packet fragmentation.	Increases router performance for the same reason as stated above.
Fragment Offset	This field is used to determine the byte position of the current fragment within the packet. Not needed since IPv6 routers do not do packet fragmentation.	Increases router performance for the same reason as stated above.
Header Checksum	Low risk of removal since the media-access (layer 1) and transport layers (TCP & UDP) also perform checksum calculations.	Increases router performance since routers do not have to generate or check checksums on the IP header. Checksums are already performed at the media-access and transport layer (TCP & UDP). The risk for undetected errors and misrouted packets is minimal.

3.15.3.3 Anycast

Anycast is a network routing and address scheme whereby data is routed to the "nearest" or "best" destination as viewed by the routing topology. Anycast addresses are a new type of addressing introduced in IPv6. It is used for sending a packet to the nearest node in a group of addressee for applications such as locating appropriate closest servers. These addresses are taken from the unicast address space. There is no syntactic distinction between an IPv6 anycast and an IPv6 unicast address. However, there are differences in the natures of unicast and anycast communications and changes at other layers of the protocol are required to use anycast.

In anycast, there is a one-to-many association between network addresses and network endpoints: each destination address identifies a set of receiver endpoints, but only one of them is chosen at any given time to receive information from any given sender. Anycast is best suited to connectionless protocols (generally built on UDP), rather then connection-oriented protocols such as TCP that keep their own state, since the receiver selected for any given source may change from time to time as optimal routes change, silently breaking any conversations that may be in process at the time. For this reason, anycast is generally used as a way to provide high availability and load balancing for stateless services such as access to replicated data.

3.15.3.4 Multicast

IPv4 and IPv6 are both capable of supporting multicasting, except that multicasting is included as an integral part of IPv6 and as such enable features that have no analogs in IPv4. For example, IPv6 has all-routers multicast addressing, which allow a node to find and communicate with routers (Neighbor Discovery or ND) without knowing their unicast address ahead of time. IPv6 multicast does not require setting up tunnels as used in IPv4 multicast to get around the common one-to-one mapping between interfaces and IPv4 addresses. Instead, multicast support is direct in IPv6 as IPv6 supports assigning several addresses (scoping) to an interface.

3.15.3.5 Auto-configuration

One important goal for IPv6 is to support node Plug and Play. That is, it should be possible to plug a node into an IPv6 network and have it automatically configured without any human intervention. With IPv4, configuration could be done in one of two ways, either manually entering the IP address into the device to be configured or automatically through a Dynamic Host Configuration Protocol (DHCP) server. Both methods require some level of human interaction. IPv6 introduces another means of IP configuration that does not rely on a DHCP server but instead determines its address from the content of received router advertisements.

IPv6 supports the following types of auto-configuration:

- **Stateful auto-configuration**. This type of configuration requires a certain level of human intervention because it needs a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server for the installation and administration of the nodes. The DHCPv6 server keeps a list of nodes to which it supplies configuration information. It also maintains state information so the server knows how long each address is in use, and when it might be available for reassignment.
- **Stateless auto-configuration**. This type of configuration is suitable for small organizations and individuals. In this case, each host determines its addresses from the contents of received router advertisements. Using the IEEE EUI-64 standard to define the network ID portion of the address, it is reasonable to assume the uniqueness of the host address on the link.

Regardless of how the address is determined, the node must verify that its potential address is unique to the local link. This is done by sending a neighbor solicitation message to the potential address. If the node receives any response, it knows that the address is already in use and must determine another address.

3.15.3.6 NAT Relevancy

Network Address Translation (NAT) is used in the current IPv4 to hide internally used addresses from globally routed ones to circumvent the issue rising from a depleted address pool in IPv4 address space. It is a band-aid solution that is useful in IPv4 but it presents challenges to many applications such as Ipsec and applications requiring end-to-end control over QoS. With a large address space in the IPv6 network, the need for NAT is minimized [128].

Hosts behind NAT-enabled routers do not have true end-to-end connectivity and cannot participate in some Internet protocols. Services that require the initiation of Transmission Control Protocol (TCP) connections from the outside network, or stateless protocols such as those using User Datagram Protocol (UDP), can be disrupted. Unless the NAT router makes a specific effort to support such protocols, incoming packets cannot reach their destination. Some protocols can accommodate one instance of NAT between participating hosts ("passive mode" File Transfer Protocol (FTP), for example), sometimes with the assistance of an Application Layer Gateway, but fail when both systems are separated from the Internet by NAT. Use of NAT also complicates tunneling protocols such as IPSec because NAT modifies values in the headers that interfere with the integrity checks done by IPSec and other tunneling protocols.

End-to-end connectivity has been a core principle of the Internet, supported for example by the Internet Architecture Board (IAB). Current Internet architectural documents observe that NAT is a violation of the End-to-End Principle, but that NAT does have a valid role in careful design.

It has been argued that the wide adoption of IPv6 would make NAT useless, as it is a method of handling the shortage of IPv4 addresses. However, this argument does not take into account the natural firewall provided by NAT.

3.15.3.7 Scoped-Addressing

IPv6 addressing allows scoped addressing including scoped multicast address. For example, there is a link-local scope that can refer only to neighbors, along with scopes for interface-local, site-local, organization–local, and global. This is used for Neighbor Discovery for auto-configuration.

3.15.3.8 Overhead

The overhead in IPv4 and IPv6 packets in relation to the Maximum Transmission Unit (MTU) has long been an object of study for enhancing bandwidth and performance efficiency. In a cursory examination, the IPv4 base header is 20 bytes, while the IPv6 base header is double as much, or 40 bytes long. However, the 20 extra bytes is not a relevant concern unless the links are bandwidth constrained. W. Eddy has analyzed the impact of IPv4 and IPv6 overheads [129] and compared the overhead in ratio to the Packet Data Unit (PDU) in 4 different cases as shown in Table 3-35.

Table 3-35. Overhead Ratio To Packet Data Unit

Case No.	Description	% Overhead OH/PDU	
		IPv4	IPv6
1a	Empty Payload (header only)	100	100
1b	Maximum Payload (65,515 byte)[10]	.03	.06
2a	68 bytes[11]	29.41	58.82
2b	1280 bytes[12]	1.58	3.13
3	1400 bytes[13]	2.78	6.42
4	200,000 bytes (Jumbogram)	.03	.02

Case 2b shows that with reasonably large size PDUs, as would be used by large data transfer applications, both protocols contribute only a few percentages. Even though the IPv6 overhead is twice that of IPv4, a 3.13% overhead is inconsequential to processing and overall network performance.

It should be noted that the larger the number of fragments the smaller is the difference in percentages between IPv4 and IPv6. Even more importantly, fragmentation is handled very differently in IPv4 and IPv6. Specifically, in IPv6 as contrary to IPv4, fragmentation is not router functionality. Fragmentation is relegated to end hosts in IPv6, if needed. This is beneficial in terms of router performance.

[10] The assumption is that the Path MTU is greater than the PDU.
[11] The minimum IPv4 MTU minus the IPv4 base header size.
[12] The minimum IPv6 MTU minus the IPv6 base header size.
[13] Fragmented into 2 packets, one with payload of 1260 bytes and another with 140 bytes because of the MTU of 1280 bytes (IPv6 minimum).

3.15.3.9 Routing Protocols

The routing algorithms that are used with IPv4 (e.g., Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) can all be used with IPv6. As such, the different variations of distant vector or link state routing algorithms work similarly, but the difference in address space obviously require some modifications. IPv6 includes routing extensions, including provider selection, host mobility, and auto-readdressing.

3.15.3.10 Address Aggregation

Inter-domain routing tables in IPv4 are very large due to limitations in aggregation imposed by the way IPv4 addressing blocks are assigned (refer to section 3.15.3.1), each address comprising of both the network and host addresses. In IPv6, the subnet addresses of large number of end-sites can be aggregated hierarchically under each backbone provider address, and the global routing table stores information regarding how to reach the backbone provider networks. This has great benefit as the routers stores optimal routing tables, do not need to use large amounts of memory, and the lookups and filtering are much faster.

3.15.3.11 Link Layer Address Resolution

IPv4 uses ARP, while IPv6 uses ND (Neighborhood Discovery) to resolve IP addresses within a subnet into corresponding link layer addresses. ARP operates on top of the link layer while ND operates by using Internet Control Message Protocol for IPv6 (ICMPv6) on top of IPv6, the IP layer. ND is highly extensible and can be used for a number of purposes, namely, security (authentication of network elements and resolution protocol messages), automatic prefix and interface identifier configuration, and MTU advertisement.

3.15.3.12 Checksum

IPv6 designers decided to drop the "Header Checksum" field of the IPv4 header for better routing and protocol performance. Most link layer protocols have efficient checksum capability including retransmission and error-correction. Also reliable application or transport protocols also implement checksums. So, the IPv4 checksum method was deemed unnecessary and of little use.

3.15.3.13 Fragmentation

IPv4 and IPv6 take completely different approaches to fragmentation. In IPv4, fragmentation of a datagram can occur at any point in the network where a particular link's MTU is too small to accomodate the entire packet assuming the "Don't Fragment"bit is not set (i.e., in IPv4, fragmentation is a router-level function). In IPv6, a router never fragements a packet. If an IPv6 packet is larger than a link MTU, then an ICMPv6 "Packet Too Big" message is sent to the packet's source, and the packet is dropped.

Fragmentation has been removed from a router's responsibilities in IPv6, and is strictly an end-host's task to perform, as needed. For this reason, the header overhead during a fragmentation scenario in IPv4 and IPv6 has to be specially compared, since it is static across the path in IPv6, but differs after the router that performs it in IPv4. We assume that from a prior failure or Path Maximum Transfer Unit (PMTU) probing, the IPv6 end-host already knows that fragmentation is required here, so that a failed transmission does not factor into the overhead computed.

3.15.3.14 Quality of Service (QoS)

Both IPv4 and IPv6 have one octet in their headers (Service Type in IPv4, and Traffic Class in IPv6) to enable service distinctions. A differentiated services compliant network node identifies the IP packets and provides specific processing and forwarding behavior indicated by the value in the octet. IPv4 and IPv6 work very similarly in this respect.

However, such QoS treatment is totally different from treatments such as, signaling at every hop and flow-state considerations. IPv6 has included a 20-bit header field called Flow Label to classify traffic with specific performance needs into flows for optimized routing. It was intended to be used by a source to label sequences of packets for which it requests special handling by the IPv6 routers, such as special QoS or "real-time" service. In IPv4, flows can only be classified by a more processing intensive mechanism of examining and parsing multiple header fields.

3.15.3.15 Security

Both IPv4 and IPv6 can be used in conjunction with the IPSec suite of protocols. The operation of IPSec protocols is basically identical whether they are used with IPv4 or IPv6. TLS protocol is similarly agnostic to IP version since it runs over the transport layer. Both TCP and Stream Control Transmission Protocol (SCTP) can run TLS and both will run over IPv4 and IPv6. Additionally the X.509 format for certificates used in IPSec and TLS, has encoding methods for both IPv4 and IPv6 addresses. So the two prevalent security architectures, IPSec and TLS, do not have significant differences in use between IPv4 and IPv6.

IPv6 nodes are required to support both Authentication Header (AH) and Encapsulating Security Payload (ESP) parts of IPSec. However, since IPv6 core functions do not rely on IPSec and only support for manual keying is required, such implementations of IPv6 are not inherently more secure. The same IPSec features can also be implemented with IPv4. Still, there are other considerations that are favorable for IPv6 in terms of security.

- Firstly, the widespread use of NAT poses hindrances towards deploying end-to-end security in IPv4.
- Second, end-system privacy or the ability of an IPv6 end-system to use stateless address auto-configuration to change its address without using external servers (such as DHCP) has no equivalent in IPv4.
- Topology Hiding is another technique that involves changing the prefix referring to a subnet, rather than the Interface Identifier. This prevents an attacker from being able to determine related addresses from a known address.
- Another security feature in IPv6 is the optional Secure Neighbor Discovery (SEND) extension allowing hosts to authenticate ND messages. It uses cryptographically generated addresses to prove addresses without IPSec or certificate management or any other security infrastructure. IPv4 has no analog.

In summary, although there are no distinctions between IPv4 and IPv6 from the security capabilities that IPSec and TLS (the two most prevalent security architectures) can offer, IPv6 has certain other security features that have no analogs in IPv4.

3.16 Commercial Off the Shelf Vendor

Several different vendors were contacted through phone calls and in person. The larger IP-PBX vendors, quotes were gotten from them to compare the cost of their systems and the number of components in a complete system. We used a small test bed for the quotes that were limited to an IP-PBX, 10 phones and analog and digital media gateways. Each product offering was then compared to the requirements and questions were returned to the vendors on how would they fulfill the different requirements. This included requirements like "Voice Precedence System", and if it was implemented already and if it could be implemented and how. A down selected group of vendors were sent a questionnaire to complete that covered key areas that would be required for an installation on a Navy vessel. The results are summarized in Appendix S. The last question was an open-end request for a system design. Most of the vendors responded with separate documents that explained their offering in general. The COTS review covered IP-PBXs as well as end devices and the network infrastructure that would connect them together and support the QoS. No specialized devices were found in the vendors that responded for use on Navy vessels. This was because their products could not be exposed the shock and vibration that is required on a vessel.

See Appendix S for each manufacturerfor answers and literature on their product lines. Several other vendors were looked at for other products other then the PBX. We looked at vendors of SIP native phones, wireless technologies, supporting servers and supporting media gateways. They will be covered in following sections.

3.16.1 Vendor Questionnaire Review

All six down select vendors that were sent questionnaires and all of them responded with differeing degrees of completeness. The last question vary the greatest from nothing, to chapters from the manuals, to well designed solutions. The questionnaire was broken into 17 main sections each one with a group of sub questions. The format was to determine if the vendor supported a feature and if so get more details on their implementation.

3.16.1.1 Conference Calls

All of them support conference calls with a vast variation in number of users that can be supported at a single time. Most vendors' solution uses an additional piece of hardware but for smaller requirements it is also done in a software solution. The vendors that are hardware manufactures relied on the hardware solutions where the software companies used software versions or third party solutions.

3.16.1.2 Intercom Calls

All the vendors require that the end point must support the auto-answer and have a speakerphone. Each of the vendors has implemented it in software as a part of their current offering.

3.16.1.3 Group Page

The ability to group page is not supported by all the vendors, but will be in the near future. The method of implementation varies between vendors, from software to the use of third party equipment.

3.16.1.4 Priority Calls and Multi-Level Precedence and Preemption

All but one vendor supported "Priority Calls" and "Multi-Level Precedence and Preemption", the methods of implementation varies between the vendors using Class of Service (CoS), to configuration by individual phones.

3.16.1.5 Call Park and Un-Park

Are supported by all of the vendors. Most of the vendors use a feature code method, but a couple vendors use dedicated extension that the call is forward to to park or an extension that is called to un-park the call.

3.16.1.6 Directed and Group Call Pick-up

All the vendors supported the directed and group call pick-up. Again the method of implementation varied between vendors.

3.16.1.7 Call Recording

The number of channels and the method used varied by vendor for call recording. In many cases they use a man-in-the-middle method that becomes a weak link in the system, since all calls that are being recorded must pass the RTP stream through the single device. There are several other vendors that specialize in call recording that resell their solutions to the major manufactures or directly to the end consumer. Some of these companies use a promiscuous mode to look at the traffic on the network and record calls per a defined filter. This removes the issue of a single point of failure. In many cases continuous recording of an area is required only a few of the vendors have this ability. It was also very end device dependant for the vendors that do support continues recording. The third party vendors' solutions have support for this feature.

3.16.1.8 Software Development Kits

The non open-source based products all have Software Development Kits (SDK), to write custom code for end devices that support SIP. The SDK support most of the SIP features from the RFC 3261, as well as some draft RFCs. Some of the vendors also support their own proprietary protocols in the same SDK. All the vendors support native SIP end devices, they are limited to the RFC 3261 feature list.

3.16.1.9 Media Gateways

Each of the different vendors support connections to PRI, BRI, analog, and Ear-and-Mouth though the use of media gateways. Some of the vendors have their own media gateways but others use third party ones. See section 3.16.6 for information on some third party media gateways and descriptions of their products.

3.16.1.10 Support for RFC 3261

All the vendors support RFC 3261, and some include support for other draft RFC. Some of the vendors also have proprietary protocols that run on top of SIP to add features that are not currently available with native SIP from RFC 3261.

3.16.1.11 Play Re-recorded Files

The ability to play pre-recorded files for things like announcements and alarms. Even though most have the ability to play pre-recorded files the functionality is very limited, requiring a separate method being used for this feature.

3.16.1.12 High Availability

All the vendors have a solution for high availability (HA), using either a cluster server approach or a distributed architecture that would allow the system to continue working even with lost of a part of the system. Different vendors solutions had different ability to have limited downtime during the switch over. Some could maintain the current calls, where others would drop the calls, but all would handle the next call that came in after the failure was recognized. Many of them rely on Domain Name Services (DNS) for the functionality.

3.16.1.13 OEM Phones Circuit Boards

None of the phone-manufacturing vendors will OEM their phones for hardening. Several of the company, even thou they answered no, there is historical history of them doing it, if the requirements are presented and it makes sense for them to do so. If we are working with native SIP, then the use of non-vendor phones will not be an issue.

3.16.2 Vendor Review

3.16.2.1 Alcatel

Alcatel responded to the questionnaire and showed that several of the features could not be done with the native SIP. In places they stated the RFC that would be required to support the feature. A design of a system pulled from a different project was used to show their capabilities, as shown in Figure 3-66. From reading their literature, it appears that they are also very able to fulfill the requirements, but not with native SIP, but with Universal Alcatel (UA) which is their own proprietary protocol that runs on top of H323. In the future releases they say that UA will be on top of SIP, until the required drafts are completed and made into RFCs, and then they will support native SIP. A benefit is that they can supply the complete system from the network infrastructure including the wireless network to the IP-PBX, and supporting servers.

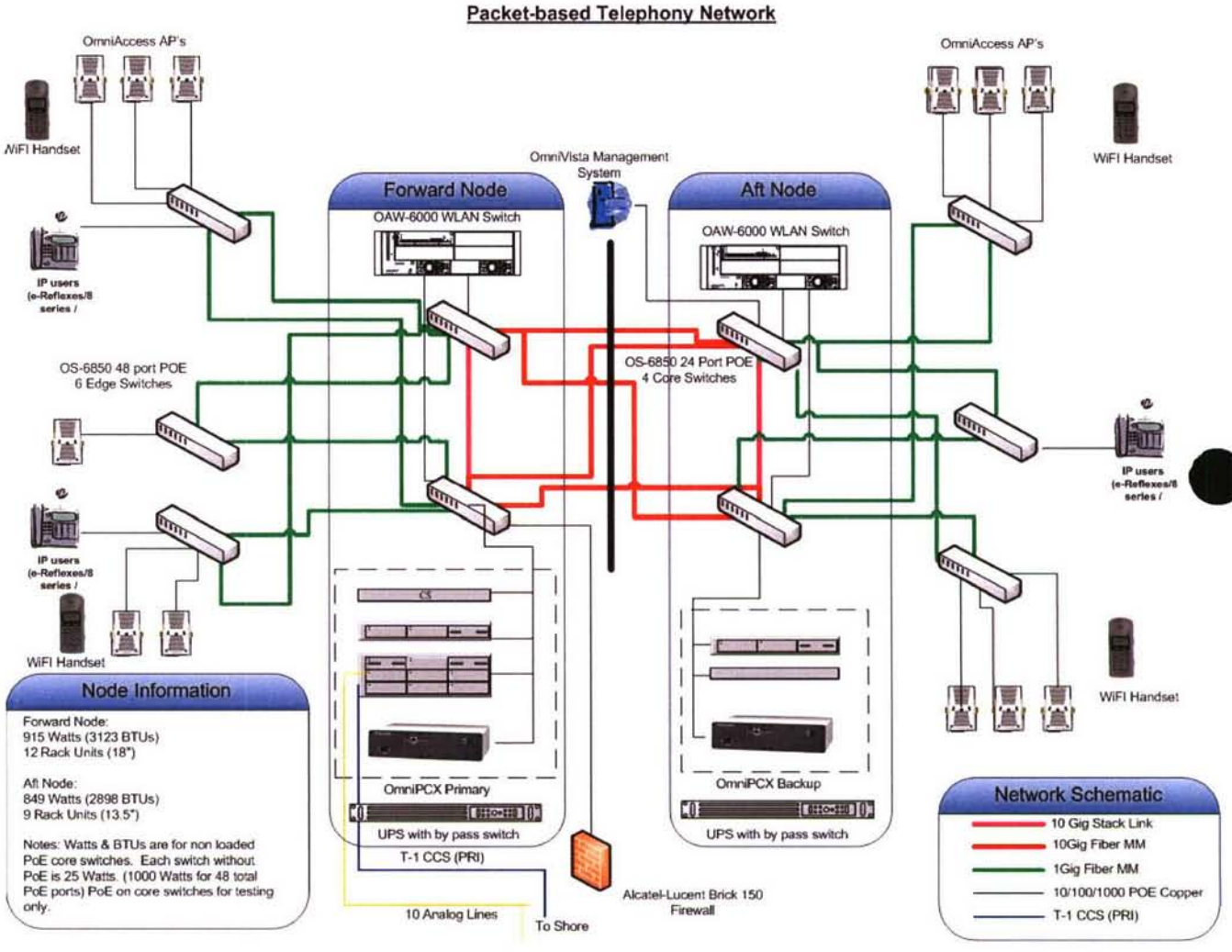


Figure 3-66. Alcatel Packet-Based Telephony Network

3.16.2.2 Cisco

Cisco's response to the questionnaire had several areas that they didn't respond to. The overall response was very good, and layout their current offering very well. The response to the final question was geared to an enterprise solution. Figure 3-67 is a Cisco diagram that shows what their offering includes.

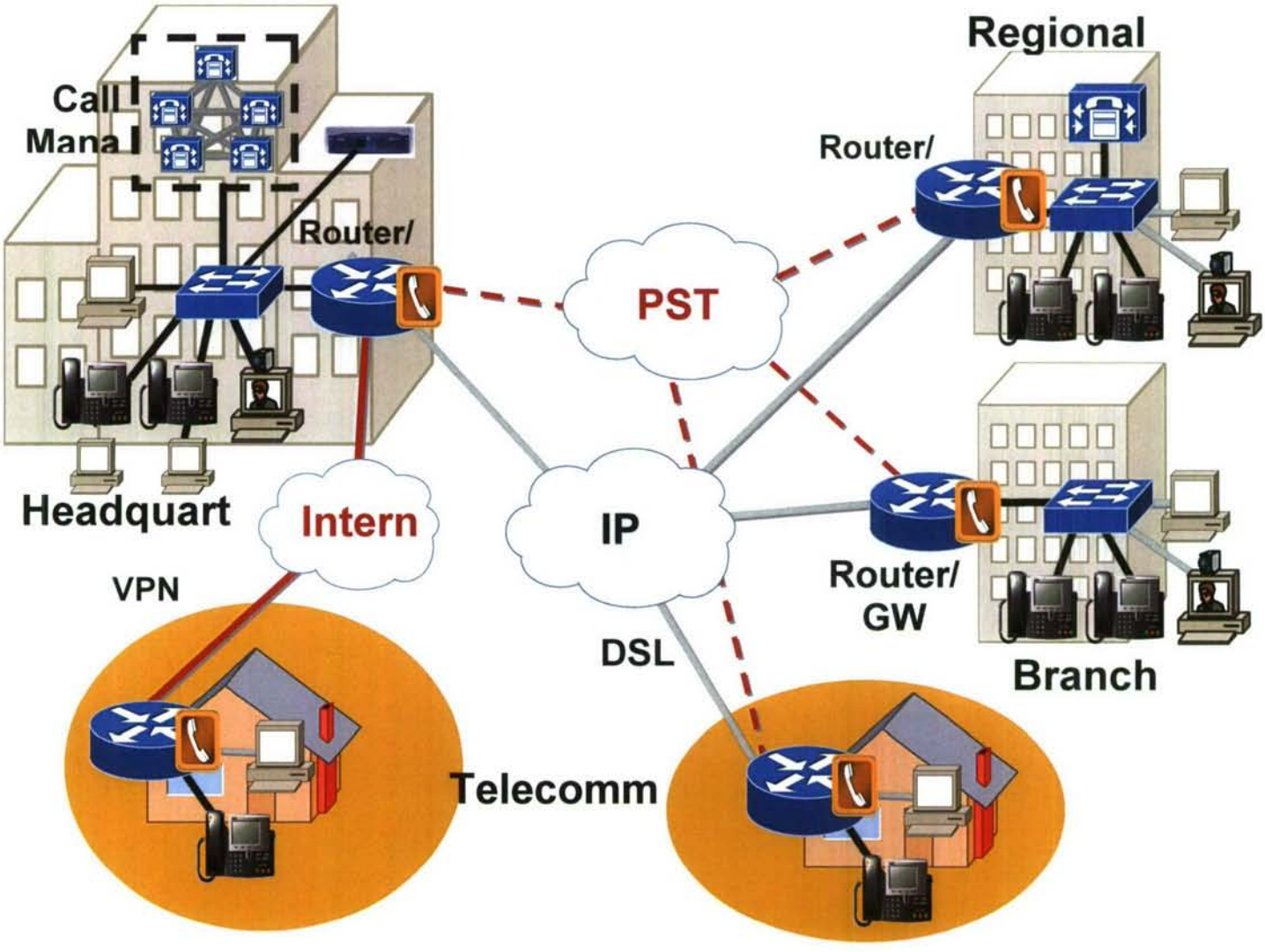


Figure 3-67. Diagram of Cisco's System

3.16.2.3 Digium

Digium is one of the first Open Source companies that got into this market. Their open source version is called Asterisk. In the past they only sold the software, but that has changes and they now will sell full systems. The company manufactures telephony cards that they integrate into their software solutions. They have their own open system protocol that they use called Inter-Asterisk eXchange (IAX), which will allow for more feature-rich communication between servers. All phones will be connected via SIP. They recommended a small clustered server that can handle the necessary connections as well as all the features and functions that are expected of the solution. This cluster would contain two call manager servers and two servers that would handle the external connections. Figure 3-68 is a representation of their recommend solution.

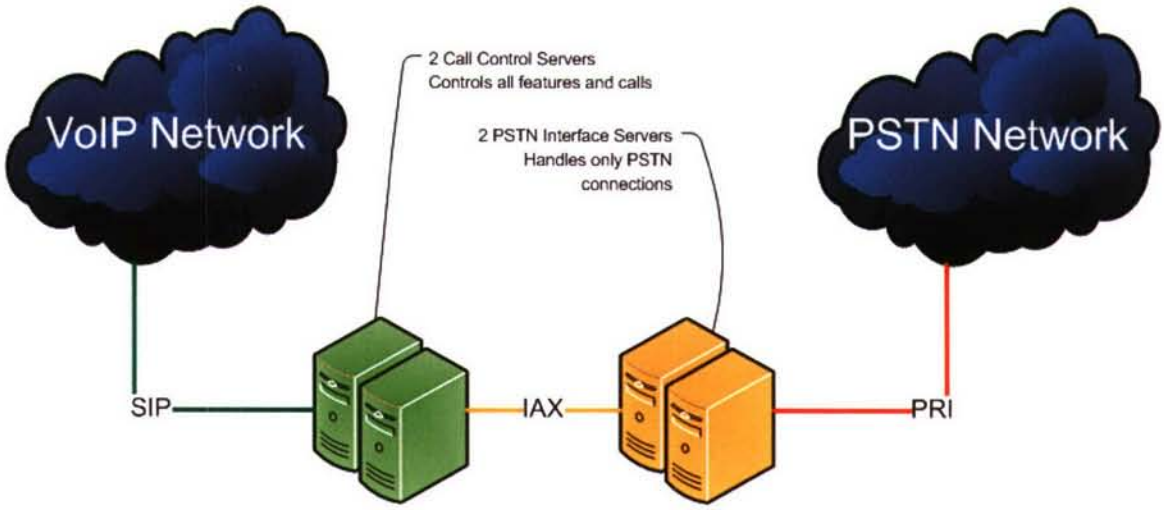


Figure 3-68. Digium Asterisk System

3.16.2.4 Sphere

Sphere Communication's fundamental strategy is founded on an "open system" approach that allows for the selection of industry standard telephony devices (IP telephones, media gateways, USB audio devices, etc.). Refer to Figure 3-69. Further to our "open system" strategy Sphere leads the industry in communications Web Services capabilities and provides a set of standard SOAP/XML defined services that allow easy and open access to Sphere's communications features.

The Sphericall software and surrounding elements (IP Telephones, Media Gateways) have been accredited and approved by DISA as part of the PBX1 testing and Certification performed at the JITC (Joint Interoperability Test Command). A letter of accreditation confirms our ability to pass the critical Information Assurance tests that are part of the PBX1 Certification.

Another critical element of our architecture is its fault tolerance. As a distributed software application, Sphericall automatically retains knowledge of an enterprise-wide calling plan. The distribution of this intelligence provides the ability to ensure that calls are handled under numerous fault scenarios. Sphericall manager software provides a full range of PBX features, sophisticated IP call control, and a robust administrative interface for system management. Sphericall managers are constructed using inexpensive open source servers running Microsoft's Windows 2004 operating system and the core Sphericall manager software. The foundation of the Sphericall VoIP solution is an implementation of multiple Sphericall managers, ensuring redundancy to guarantee call set-up and termination for 99.999% system reliability.

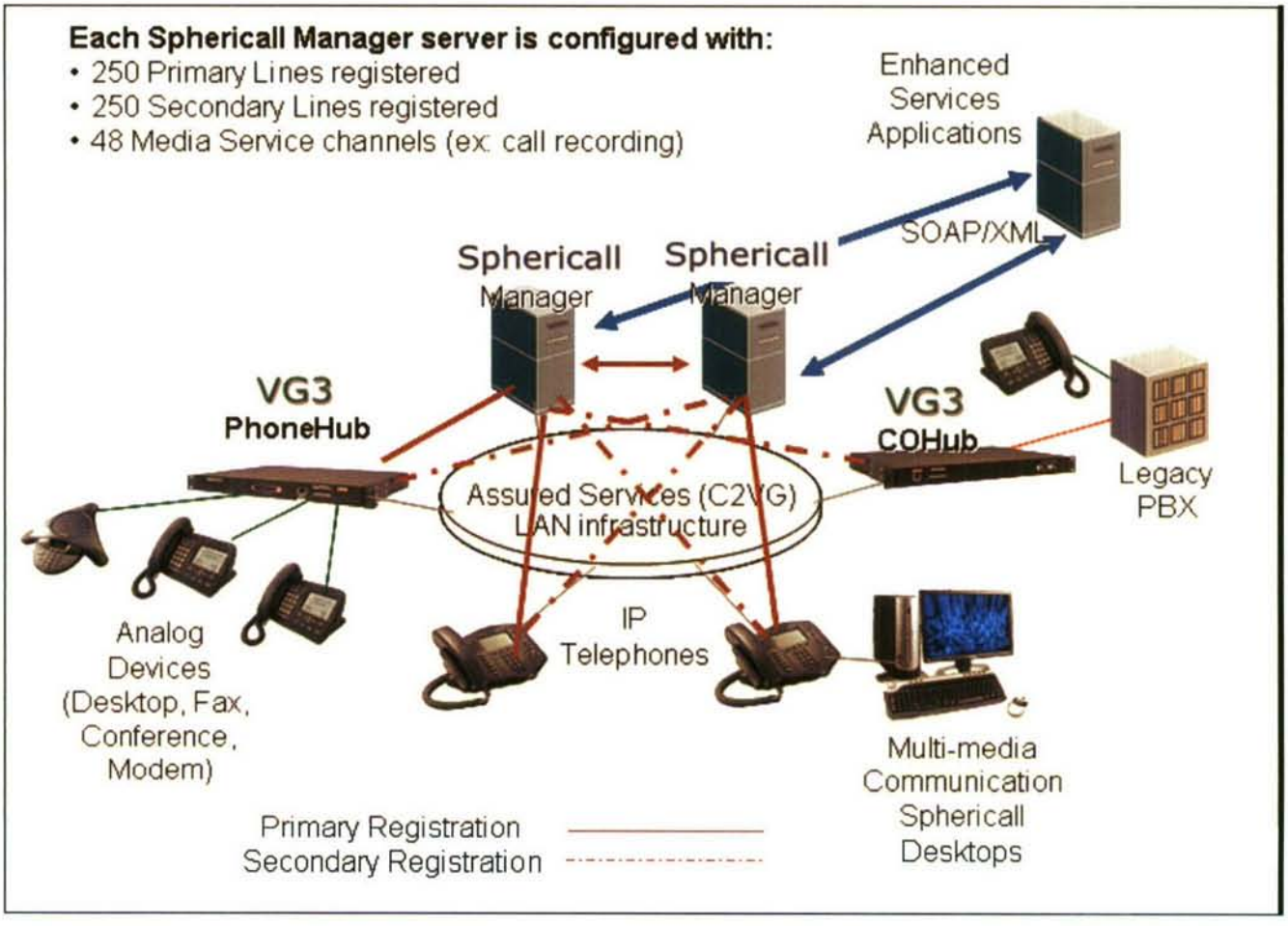


Figure 3-69. Sphere Communication Open System

3.16.2.5 Avaya

Avaya is a hardware provider that built and sold TDM PBXs. Their new products support VoIP and have good support for SIP. They are on many communities to move SIP forward to fulfill all the requires that are needed in a solution. They are in the process of being purchased, and moving into a more software based company, since the margin on hardware is decreasing and being coming a very hard market place to be a leader. The answers to the questionnaire were good showing that they can do the majority of the features required. The areas that they can support there are third party companies that can fill the gaps. Their answer to the last question (Recommended Solution), was very limited in details" This would be an S8720 High Reliable design with SIP endpoints. Right now, we are limited to the 46xx product family but will support SIP on the 96xx and the 16xx product line soon." Even though the shortness of this answer the rest of the materials collected for them shows a good support for SIP and the direction the company is taking should result in a very good product that merits more review in the future.

3.16.2.6 Pingtel

Pingtel is a company which opened up its product to the Open Source Community a number of years ago. The open source version is called sipXpbx. It is completely based on SIP RFC and drafts. This product like Sphere is the closest to an open system. The product that they sell goes through quality assurance testing and has some added features that are not in sipxpbx. They are not able to do many of the features in the questionnaire, because of the limitation in native SIP

when you adhere to the RFC. This is a very limiting factor for their product, but it is a truly open system, that the other vendors can't claim. They chose not to answer the last question (Recommend Solution), but they only have a couple products, so the design is very straight forward compared to the other companies that are being reviewed here.

3.16.2.7 Redcom

Redcom chose to not respond to the questionnaire, since their product is very different then the ones that the other vendors have. They have created TRANSip that is added to their current PBX to give them a VoIP connection. This allows more flexibility but relies on the core switch for many of its functionality. More details of this solution can be found in the appendixes.

3.16.3 VoIP Phone

A review of the specifications of several different phones manufacturers and a comparison of their specifications was conducted. Refer to Table 3-36. There are two different groups of proprietary phones that can have SIP added by a firmware change. The other group is phones that are designed for SIP. Both types of phones can be updated with firmware updates to improve the functionality and updates from the manufacture as they come out. The updates may also be to support new SIP RFCs that have been ratified. When the phones are implemented, they should be evaluated and if there are firmware updates they should be updated to the latest version. In many cases there are multi files to be updated on the phones, for different functionality. In most implementations a TFTP server or compliable server is setup so the phones can get updates when they are booted up. The configuration of the phone may also be stored on the server so the phone will get configuration updates when it is connected to the network. Many of the phones also allowed the administrator to force a restart that would then download the configuration and updates and install them on the phone.

Table 3-36. VoIP Phone Comparison By Manufacturer

Feature	Polycom	Polycom	LG-Nortel	Aastra	Snom	Snom	Grandstream	Grandstream
Model	IP601	HD IP650	LIP-6812	9133i	300	370	BudgeTone 200	GXP-2000
SIP	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
Web Admin	**Y**	**Y**	**U**	**Y**	**Y**	**Y**	**U**	**Y**
Micro Browser	**Y**	**Y**						
QoS		**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
PoE	**Y**	**Y**	**Y**	**Y**	**N**	**Y**	**Y**	**Y**
Hub	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
#Lines	**6**	**6**	**11**	**9**	**2**	**12**	**1**	**4**
Intercom	**Y**	**Y**						
G.711	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
G.723					**Y**	**Y**	**Y**	**Y**
G.729a			**Y**		**Y**	**Y**	**Y**	**Y**
G.729b	**Y**	**Y**	**Y**	**Y**			**Y**	**Y**
G.732.1			**Y**		**Y**	**Y**	**Y**	**Y**
G.722	**Y**	**Y**			**Y**	**Y**	**Y**	**Y**

From the research done it was determined that the different companies have a range of phones from single line to multi line designed for office users to executives. They range in features, but all of them support the basic ones. Some phones are designed for video conferencing, but were not evaluated in this review. They all seem to support G.711 and G.729 codexes. The calling features for all the phones looked at were basically the same with small variation on minor features. The price range of the phones is from about $160 to $700 for the ones that were evaluated. In many cases it appears to be the general quality of the phone that makes the biggest difference. Some of the manufactures develop the phones for home and home-business users, where others design them for corporate use, and they seem to be better designed and consequently more expensive. None of the manufactures advertise any kind of OEM'ing of the phones or circuit boards on their web site. Manufactures were hesitant to discuss it, unless then number of phones was in the thousands per order with quotes for the year. None of the phones looked at would meet any of the environmental or impact requirements that present end devices are certified to.

In the embedded section, phones on a circuit card are reviewed. In many cases these solutions are similar to the above phones without the casing, and allow modification of the programming so new features can be added as required.

The Polycom has a couple features that are unique to their phones. Micro-Browser lets the phone connect to an external web server to display applications on the phone display. Intercom is a feature that has to be supported by the IP-PBX that the Polycom phone is

attached to. A code is sent to the phone as a parameter on the invite line, this instructs the phone to come off hook automatically; but it doesn't mute the microphone.

3.16.4 Wireless Product Vendors

Wireless products will play a major role in the upcoming future. See the section Mobile Communications, for more information on the technologies that are available currently and in the near future. Some technologies lends it self to the internal vessel usage where others lend them selves to being used in the up environment. In the Mobile Communications section it evaluates the technology that will fit best for the use in both environment. In this section we have sampled a few of the companies that have innovated products. There are many other companies in this space that have not been evaluated.

3.16.4.1 LGS

Bell Labs Innovations has the smallest GSM BSR system in the world. This family of products comes in two sizes. The Macro BSR is a rack-mounted version with coverage of about seventeen miles. Where the Pico BSR is a notebook-sized device with coverage of about three miles. The units are equipped with it's own call manager functionality, giving GSM phones and other phones on the data network connectivity. The draw back to the system is the spectrum, and how the cellar phone companies own it. A relationship needs to be developed, or the system needs to be turned off when the vessel approaches port so it doesn't interfere with land based cellar service. This type of technology as been implemented on the medical ships, so the reservists doctors can be reach using their personal cellar phones while on board; reducing the time to get in touch with the doctors while on duty.

3.16.4.2 Vocera Communications

Vocera Communications is a voice activated system that is limited to a small precise vobalulary. The use wears a small button around their neck or clipped to them, that they initiate the process. Because of the limited vocabulary and the voice recognition it is limited functionally in this noisy enviroment at this time. As the technology is expanded their product may add benefits for the hand free user in the future.

3.16.4.3 Spectralink

Spectralink Corparation's NetLink Wireless Telephones are used with the SpectraLink Voice Priority (SVP) server. Spectralink is now part of Polycom. To connect to the main PBX the calls must be routed through a media gateway. They have been in this market segment for a while, and have fine tuned they currect offering to work with their dedicated systems. Their wireless network is formed around the 802.11b technologies that requires the extensive use of site surveys to impliment and then to maintain the network when adding new APs. They use a proporitary protocol to connect the phones to their SVP servers.

3.16.4.4 Alcatel

Alcatel OEMs the phones from Spectralink in a SIP version that are sold as their wireless phones to be used with the WLAN product line. Alcatel's WLAN has the same type of controller that Meru Network (see below) that allows for the installation of the wireless LAN without having to do a site plan. Also it manages the authentication that allows the end devices to travel between access points without issues of jitter and dropped calls.

3.16.4.5 Meru Networks

Meru Networks uses a uniquely engineered Air Traffic Control™ Technology to manage there individual access points. This central controller, manages the access points for several different areas. It allows all the access points to appear as the same so as an end device moves from one to another, it is not required to authenticate its self on each hope. This is major, since the authentication process is slow and would result in jitter at best, but could result in dropped calls. Also the centrol control manages the power output of the so installing them into rooms with metal walls, cellings, and floors allow them to function more efficiently and avoid having to do site surveys to determine the location of each access point. The controllers also manage the quality of service (QoS) so high capacity data can finally coexist with VoIP calls, without the problems of quality of server, that is seen on many other networks. They also have a vast array of access points for different enviropments.

3.16.5 Supporting Servers

3.16.5.1 Recording Servers

Recording is on vessels falls into two different areas, the first is recording of calls that are made on an end device; the other is audio that needs to be captured in critical areas of the vessel. The recording for the IP based end devices is very different than the recording of the audio microphones. The audio microphones are very similar to the TDM type recording of a phone call, where the IP is collected off the network in packets that are then converted and stored on the hard drive. There are two methods of collecting the packets from the network. The first is man-in-the-middle; this requires the RTP packets to pass through a server, and the server takes a copy of each VoIP packet and stores it. This is very CPU intensive as well as adds a single point of failure that is the server doing the collection. It also creates added load to the network since SIP would usually travel between the end devices, in the shortest route that the VLANs and QoS allowed. The preferred method is promiscuous network; this allows the devices to sit on the switch and have all traffic in the switch pass by its port. It then collects the data on stores the VoIP packets that need to be recorded. There are a few different ways to set this up so all the packets pass by the record's network port. If all data is sent through one switch this would achieve it but gives a single point of failure. A better way is to have LAN connections from every switch come back to the recording device. This eliminates the single point of failure.

3.16.5.1.1 Nice

Nice (http://www.nice.com) has a complete line of recording systems. Each of the different recording devices are independent units, but can be administrated from a single

Administration Terminal that requires its only server. Their products cover analog, digital, IP and video. Here are descriptions of the two telephony products.

NiceLog VoIP handling VoIP calls while providing full-time recording, selective, quality management or record-on-demand solutions. It supports H.323, the most widely deployed VoIP gateway, as well as other VoIP industry standards like SIP, and is fully integrated with NICE's Customer Experience Management (CEM) Platform. It uses a promiscuous network connection that allows it to gather packets from the network, but not be a man-in-the-middle. This feature makes the implementation more resilient then devices that have to sit in the middle of the traffic.

NiceCall Focus III is a full-featured, compact recording solution designed to meet the needs of small sites. It provides total recording, quality management, scenario reconstruction and other tools designed to meet the specific needs of these sectors with up to 48 recording channels per capture unit. It also provides a multi-site solution for distributed organizations. Based on a completely new PCI bus design, it utilizes an open architecture without any proprietary boards. It supports many different telephony interfaces including analog and digital as well as ISDN BRI. It maximizes archiving capacity by using the advanced technology compression algorithm G.729A.

3.16.5.1.2 TelRex

CallRex (http://www.telrex.com/callrex.htm) is a promiscuous network implementation that collects the calls from the network. By using this method it does not interfere with the SIP packets as the RTP travels to the individual end devices. Also it is no in the middle of the stream so if there is a failure the call is not dropped. CallRex Professional is designed with a distributed architecture, that for large installations it has a central server and then data collector servers. They also offer a CallRex Express but it is limited to 15 phones.

The CallRex server is connected into the core switch that the packets will travel through. The CallRex may require connections to multiple switches to be able to collect all the packets, if the phones to be recorded are disbursed thoughout the vessel.

3.16.5.1.3 Red Box Recorders

Red Box Recorder (http://www.voiplog.com/red_box_recording_products/) has three core products that they offer. The first is a small system; the RBR 2610 is a single box solution for IP and conventional telephony recording, for small installations with limited number of phones. The next product RBR2620 voiplog® is an IP only recording box that is a 2U 19-inch rack mounted solution. It monitors the incoming and outgoing packet traffic and collects the voice, as that is required. Storage can be internal or external to suite the installations requirements. The last system is the RBR2630 is like the RBR2610, but for sites that require a large system.

The RBR2610 is the solution that is sized right for everything but the largest aircraft carriers. It supports both traditional telephony and IP in the same system reducing the number of servers required for a single sub task. The client interface is developed around web access, so no special software needs to be loaded on the individual consoles.

Witness (http://www.witness.com/index.aspx/)

IMPACT 360 Full-Time Recording is a mixed TDM and IP telephony recorder. It can be setup in two different modes, CTI, if the PBX has it or a VOX and D-channel, so you don't miss any of the call. It is a software only solution, so it uses COTS based computer servers and I/O boards. It uses AES256-compliant encryption to protect data when it's recorded, in transit, and archived. Voice recordings and call detail records are stored together in a single, unified database. You can archive contacts locally on a DVD drive, use a true RAID-5 disk storage option. The browser-based central archive manager, will let you look at the contacts in many different ways. With the use of graphical display and color coding, trends and patterns can be seen in the recorded calls. They also have many added features like speech analytics, that is beyond the current requirements.

3.16.5.2 Play Back and Media Mixing

3.16.5.2.1 Newfound Communications

Newfound Communications (www.newfoundcomm.net) The media mixer allows recorded information to be added to an RTP stream as it passes through the server. This is used for many different purposes, like: adding back ground music, adding information so the caller hears it. Audio effects can easily be initiated by applications and include fade in, volume control, fade out and voice navigation tools such as fast forward, rewind or pause. For second channel audio, the MediaMixer plays many of the popular telephony audio formats (.ulaw, .alaw, .WAV, etc.). They also have a IP Recording product that is developed for VoiceXML (VXML) applications. The solution is very flexible in nature. Newfound Communications is a consulting firm that does custom development for customers in the area of VXML applications as well as the products mentioned above.

3.16.5.2.2 Berbee a CDW Company

(http://www.berbee.com/public/berbeesoftware/InformaCast.aspx)
InformaCast is a robust, full-featured system that allows users to simultaneously push an audio stream and/or a text message to multiple IP phones, InformaCast IP Speakers, the InformaCast Desktop Agent, and overhead paging systems. An administrator can select a prerecorded message or send a live broadcast through either a password-protected web page or the IP phone services menu.

This company products compliment the requirements for an announcing system. They have the amplifiers as well as the pre-recorded play back of files for the alarms.

3.16.6 Supporting Media Gateways

Media Gateway connects different types of networks; one of its main functions is to convert between the different transmission and coding techniques. It is a translation unit between time-division multiplexing (TDM) voice to Voice over Internet Protocol (IP) (VoIP). It is controlled by a media gateway controller, which provides call control and signaling functionality for protocols like Media Gateway Control Protocol (MGCP), Megaco, H.248 or Session Initiated Protocol (SIP).

The Media Gateway is used to interface two differing technologies. Many of the current end devices are analog, digital BRI and PRI, and even proprietary. The units are sold with 1 to 48 channels, to be used. The majority of them are configured using a web page that is contained within the unit. Each manufacturer has their own configuration and features, so a careful review of the them is required to make sure the unit will fulfill the requirements as well as be easily configured.

When looking at media gateways, there are some questions to be considered.

Does the device have the right number of ports and can it simultaneously support all the channels?
Some media gateways have more ports than the number that can be simultaneously used. Also many of them are configured overall, so you have can't have different parts receiving different protocols.

Is the device certified on the VoIP network?
Different manufacturers have their own media gateways as well as ones that have been tested with their products. It removes one possible problem if during the installation and configuration if there are problems. In many cases, this is not possible and you need to go with a media gateway that is not certified with the other equipment, and this needs to be keep in mind.

Does the manufacturer have a way to upgrade the device in the future?
Since the technologies are changing and new RFC are ratified, the ability to upgrade a media gateway is important. Many of them let you do a flash of the bois as the method of upgrade. After a system comes in from the distributor, it should be check and updated before it is used.

What is the packaging and power requirements for the device?
Many of the units come as standalone devices with a separate power supply. Large systems come in 19-inch rack enclosures that use standard AC power cords. Depending on the requirements that maybe critical to being able to meet shock and vibrator testing.

What is the IP type connection and protocol and is it supported on the VoIP network?
The majority of units use a RJ45 CAT5 connection, but some now support fiber to the units. They vary in the different protocols that are supported, some you must configure, but others must be purchased for the correct protocol.

Does it support the codexes that are on the VoIP network?
The VoIP equipment will support one or several different codexes. It is important to reduce the number of codexes used on the network, as the packets move from different devices, a conversaion of the RTP packet maybe required resulting in heavy processor usage in the media gateway or in a VoIP server on the network.

Raytheon ARA-1 *(www.jps.com)*

The ARA-1 is a radio-to-SIP interface, which allows a radio to operate on a SIP network. This brings to existing SIP networks all of the features inherent to a radio system and to radio systems all of the features available with SIP. With this new technology, for example, an LMR system can be used to extend the SIP network into areas of rugged terrain, across bodies of water or into tunnels. Also, the ARA-1 can be used to create interoperability among disparate radio systems as easily as creating a typical PBX conference call.

Even though the product is directed to the radio interface requirement, it should be able to be used to interface any device that uses an audio input as the method of connection. This could include announcing system, or a sound powered telephony system depending on the equipment that it is using.

MediaTech *(www.multitech.com/PRODUCTS/Categories/Telephony/)*
The MultiVOIP® SIP gateway provides toll-free voice and fax communications over the Internet or Intranet. Available in 2-, 4-, and 8-port models, the MultiVOIP gateway connects directly to phones, fax machines, key systems, PSTN lines, or a PBX to provide real-time, toll-quality voice connections to any office on a VOIP network. The MultiVOIP gateway is designed to maximize the investments already made in a data and voice network infrastructure. They also make "BRI VOIP Gateway" in a four and eight channel version. This allows connection to BRI units. For the Navy this is important, since my end devices in the past have been developed to work with BRI as a standard. This will allow the older end devices to be used with the new VoIP system. They also support Ear and Mouth (E&M) that is important for connection to some older equipment. This interface is usually packaged with the analog units or stands on its own.

Linksys *(www.linksys.com)*
Linksys carries a line of small two port analog media gateways. These units are known for being easy to setup and simple-to-use. They connect to Plain Old Telephone Services (POTS), giving you the ability to connect your old analog device to the VoIP network. The unit can be remotely provisioned and supports dynamic in-service software upgrades, or be managed one at a time with an easy web interface that is contained on the unit. Linksys offering is small, it fulfills the niche of limited port units for the analog end device.

Dialogic® *(www.dialogic.com/products/gateways/default.htm)*
The Dialogic® 1000 Media Gateway Series (DMG1000) allows for a well-planned, phased migration to an IP network, making it a smart solution for enterprises looking to enhance their legacy PBX equipment with new VoIP access and applications. Connected between a PBX or a digital handset and a LAN or WAN, the gateway converts proprietary digital PBX messages into a format suitable for transmission over standard IP networks. It supports phones from: Alcatel, Avaya, Ericsson, Fujitsu, Mitel, NEC, Nortel and Siemens. Each unit has eight ports that support H.323, H.450, SIP, and RTP/RTCP VoIP protocols. The unit has to be configured for only one switch as a time, and is several other configurations that are for the overall system.

AudioCodes (www.audiocodes.com)
CPE (Customer Premises Equipment) and Access Devices offered by AudioCodes include analog, BRI, digital, these products are feature-rich interfaces and signaling elements. The MediaPack™ Analog Media Gateway product family is based on AudioCodes' field-proven and best-of-breed VoIP technology. Featuring 2, 4, 8 or 24 analog ports, the gateways connect analog terminals, PBXs or key systems to the IP network using FXO or FXS connectivity. The MediaPack™ BRI Media Gateway product family is based on AudioCodes' field-proven and best-of-breed VoIP technology. Featuring two, four, or eight BRI ports, the gateways connect PBXs or key systems to the IP network using ISDN-BRI connectivity. The Mediant™ 2000 Digital Media Gateway supports up to 16 E1/T1 digital trunks and is intelligently packaged in a stackable 1U chassis designed for smaller locations in the carrier network market. The Mediant 2000 optionally supports a DC power supply (complies with NEBS Level 3) or dual AC power supply.

Squire Technologies *(www.squire-technologies.co.uk)*
Squire Technologies is a UK based company, which combines leading edge SS7 and VoIP telephony products with world-class installation and support services to deliver carrier grade telecom products worldwide. Their scaleable SS7 and PSTN network breakout to VoIP networks facilitating carriers to realize the cost and performance benefits of integrating into an SS7 network. The Media Gateway provides a single one stop SS7 to VoIP product solution offering full SS7 to SIP/H.323 signaling interconnect and TDM Voice/Data conversion to industry-standard VoIP Codecs. Their SS7 media gateway is the only one that we have found. Even though we see limited functionality for vessel usage, it is a product and company that should be followed for future needs and requirements.

3.16.7 Summary

This section only briefly covered some of the COTS products that were reviewed. Since many of the companies have the same product features it was redundant to cover all of them. The products that were covered represent the majority of vendors that are offering VoIP products. The vendors/products that were represented had a feature or well-done documentation. More information is contained in the appendices and the individual vendor's web sites.

The information that was gathered here is dispersed throughout the paper, in support of methods that are used to determine the feasibility of VoIP on Navy vessels. The majority of the time spent researching COTS was the PBX vendors themselves. The research started on the web and gather information from them by email. Presentations by many of the vendors were held at the Henschel's facility. The final part was a questionnaire that was sent out to the vendors to get answers on questions that would show the feasibility of their offerings for implementation on Navy vessels.

3.17 System Integration

3.17.1 Introduction

The transition from the present infrastructure consisting of separate networks that support both internal communications and data network needs to be evaluated for the ability to converge them into a single secure network. The purpose of this commentary is to pull the above material into a single concept that will carry the reader through the thought pattern that was developed as the material was researched and then converged with the present Navy requirements. After compiling the research we looked at the possible benefits that will be realized by the Navy, if all the recommendations are followed. The final sections will layout a conceptual, vendor independent, converged secure system. The design will look at achieving all the stated benefits, while maintaining the required security and ease of use for the sailors and officers.

Figure 3-70 shows a model VoIP network for a non-converged (single security level) architecture. The scenarios described below address convergence of security levels of the VoIP network with the data network. The component architecture includes a few groups of devices:

The Telephony Servers contain a set of servers necessary for the telephony application.
The Data Service Servers provide general data applications (e.g., DNS) that the telephony services depend on.
The end instrument (EI)s connect through access switches distributed throughout the vessel.
The network equipment connects the components.

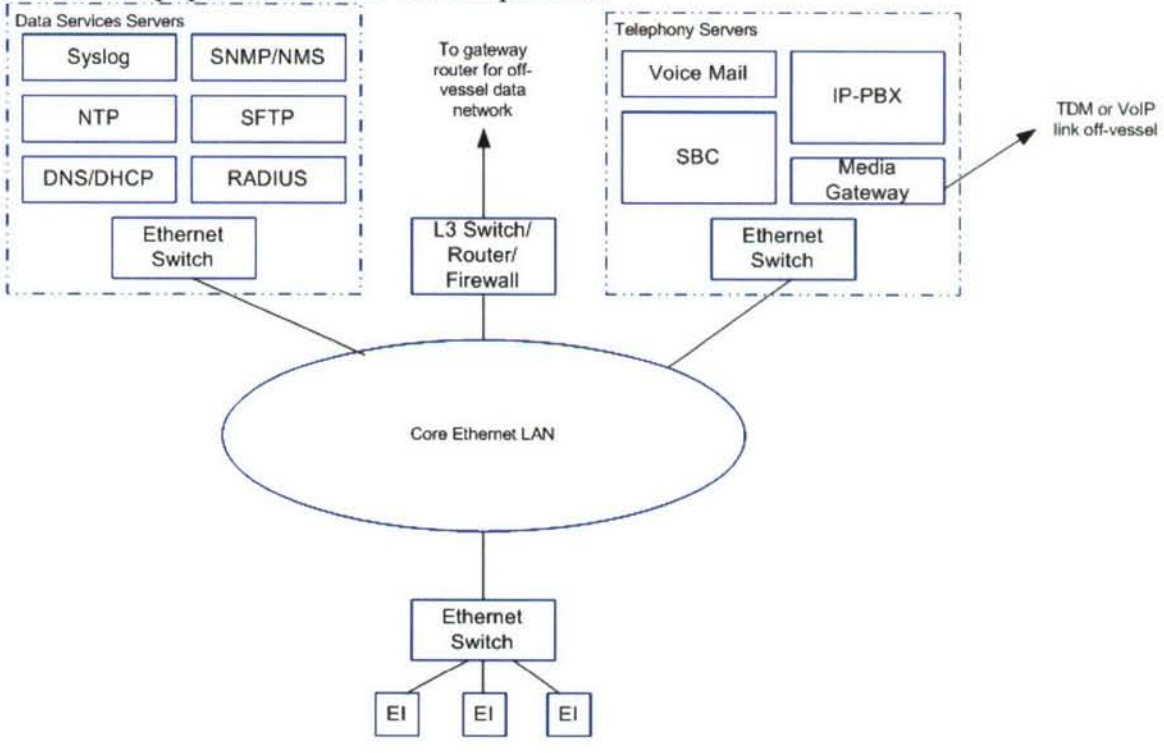


Figure 3-70. Example VoIP System

Note that the diagram does not show redundancy. To meet the system's availability requirements (e.g., less than 12 minutes downtime per year, all devices (except the EI and the EI's link to its

access switch) are either redundant (e.g., primary and backup server) or provide carrier-class availability by replicating each subcomponent (e.g., power supplies, fans, CPU cards, disk drives, etc.). To focus on information assurance (IA) aspects of the design, this piece abstracts away the redundancy. There is no significant effect on the analysis by ignoring redundancy entirely.

3.17.2 Security Topology

The converged network is the first major hurtle that needs to be looked at and decisions need to be made on what the security needs are compared to what is presently done in commercial industry. The present method is separation of the networks keeping dissimilar data on dedicated networks. There are many benefits to this method of security and it has worked for the armed forces for several years. The convergence of data was attempted on the CVN 68, without success, and the new retrofit is separating the data into separate networks (seeFigure 3-71). The design used was developed over 10 years ago, with technology that was available. In the last decade security has changed vastly for IP network security. In the white paper from Bell Labs entitled "VoIP Security Study" they discuss security for the network with a concentration on VoIP security. Another paper from SSC SAN Diego Detachment St Juliens Creek Code 2877, Mr Stuart Shoup called "Naval Secure Voice Vision: Transition and Future Architecture Options" point in the direction of convergence and the discontinued use of stove-pipe initiatives. In this paper, Mr Shoup discusses more of a complete communications system for FORCEnet and the future vision of voice as an integral part of the CANES environment which utilizes common COTS products. In another white paper from Bell Labs called "Intelligent Advance Communications Network Infrastructure" K. P. Das has a few sections that discusses security and VoIP security from the point of view of the network infrastructure. Each of these papers discusses the protocols that can be used to secure IP packets on the network.

All communications are on the same VoIP network with data on the same network.

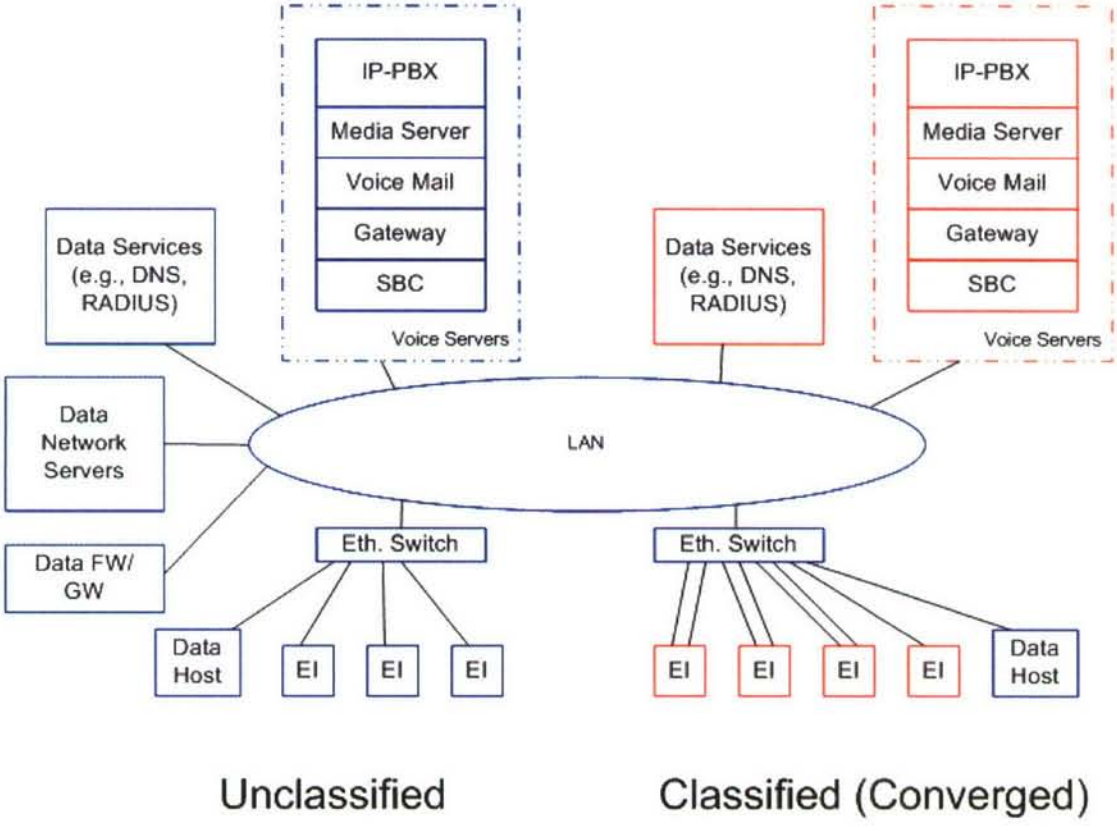


Figure 3-71. Scenario 4–Data Convergence

Notes:

- The figure shows dual-homed EIs. It is also possible to have a single-homed EI that applies its own VLAN tag.
- The data network includes Data Host, Data Network Servers (e.g., e-mail, web server) and a gateway for off-vessel communications.

We assume that the data network uses a system of VPN gateways (e.g., HAIPE) to interconnect sets of classified edge subnets and simple VLANs to segregate the unclassified data traffic. Given that the networks contain legacy applications that cannot provide their own security, this may be the only reasonable option to connect such systems.

This scenario represents further cost savings over the previous scenarios because the VoIP and data networks share a single network infrastructure instead of using one infrastructure for data and a second for VoIP. Further savings are possible by reusing network services, such as NTP and RADIUS, between the data and VoIP networks. The convergence may also facilitate new functionality, such as multimedia collaboration.

3.17.3 Security Architecture

This design describes two possible architectures for securing the VoIP and data networks, which are feasible with currently available technologies. Several of the options (specifically, S/MIME, ZRTP, Skype, DTLS) had deficiencies that eliminated them from consideration. The architectures were selected based mainly on the following criteria:

Use of Commercial off-the-Shelf (COTS) products and COTS-based solutions,
Industry views of the architecture as a reasonable approach to secure VoIP,
Diversity of the architecture, and
Vendor-neutrality of the architecture.

The first architecture (Architecture A) uses protocols defined at the application layer to secure communications. The second architecture (Architecture B) uses IPSec at the network layer to secure the communications and includes an SBC to help offload the computational demands of the cryptography algorithms.

3.17.3.1 Architecture A: Application Layer Approach

The first architecture uses IETF protocols designed to enhance the security of the VoIP protocols. In particular, the SIP signaling uses SIP over TLS and the bearer uses SRTP.Figure 3-72 shows a functional diagram of Architecture A. The SIP specification [89] defines semantics for SIP over TLS. Although the specification requires RFC-compliant devices to support TLS, few devices today use (or even support) TLS. SRTP [130] adds encryption, authentication and integrity to RTP. It uses a format compatible with RTP such that systems supporting RTP (e.g., an SBC) can easily support SRTP provided that

(a) the EIs support SRTP and

(b) the system has a mechanism to exchange keying material.

It is assumed that the Security Descriptions [131] protocol provides the key exchange mechanism. This protocol is emerging as the de facto standard for SRTP key exchanges because it is more efficient and easier to use than alternatives, such as MIKEY [132].

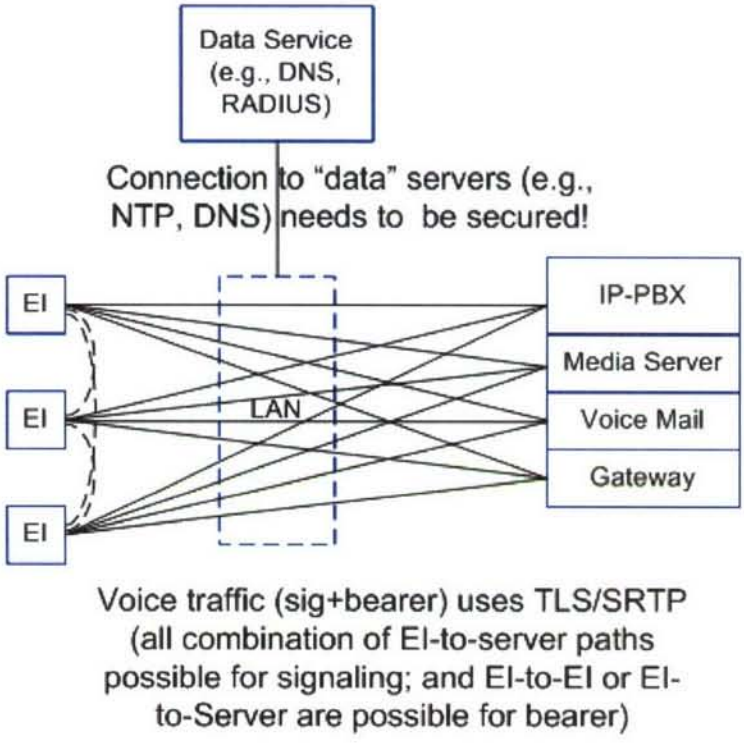


Figure 3-72. Architecture A

3.17.3.2 Architecture B: IPSec Approach

Architecture B uses the IP Security (IPSec) protocol to secure VoIP traffic at the network layer. Figure 3-73 shows a diagram of Architecture B. The diagram has all of the components from Figure 3-72 and an SBC. The signaling and bearer paths use IPSec connections running from the EI and VoIP servers to the SBC. SBCs often include specialized cryptographic acceleration hardware that can support tens of thousands of EIs using IPSec. The architecture forces the bearer streams from each EI through the SBC, rather than having the bearer streams run directly between EIs (both configurations are used in operational networks).

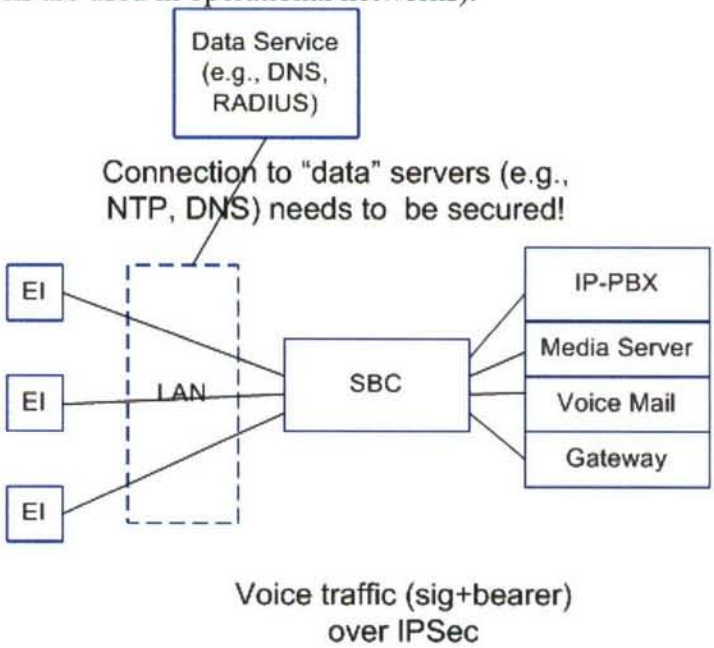


Figure 3-73. Architecture B

The SBC is configured with three physical interfaces. One interface faces the core network to communicate with the EIs. A second interface connects to a small LAN connecting the VoIP servers, which can be isolated from the core LAN. The third interface sits on the management VLAN.

As with the previous architecture, this one does not make any specific recommendations on how to secure the data services that the EIs depend on. While it may be possible to use separate IPSec systems to connect the EIs to a subnet with the data servers (or to use a separate connection for each server), today's EIs lack the CPU resources and configurability to do so. As before, the analysis captures the risks associated with not explicitly securing these protocols. The appendix I "VoIP Security Study", addresses how the EIs can support both encrypted and non-encrypted sessions.

Note that the SBC introduces a potential single point-of-failure. Specifically, if the SBC fails, ongoing calls would fail (the bearer would drop out before the EIs eventually let the signaling session timeout). From a signaling perspective, the single point of failure moves from the IP-PBX to the SBC. For these reasons, SBC vendors design their systems with redundant components (e.g., power supplies, fans, network interfaces, processing boards) and network failover technologies, such as Virtual Router Redundancy Protocol (VRRP), to meet carrier-grade reliability levels (e.g., five-nines of availability) and DoD availability requirements [133].

3.17.4 Recommendations for Security

The results in the previous sections lead to a few conclusions. Between the two architectures, the analysis done in the Appendix I "VoIP Security Study" shows that the level of security is nearly the same, but on each dimension Architecture B scores either the same or slightly better than Architecture A. The analysis shows a clear direct relationship between the amount of convergence and the level of security. The questions become "How much of a security risk is the Navy willing to take to allow convergence?" and "Can the risks be mitigated?"

From a security standpoint alone, Architecture A and Architecture B are similar. There are a few cases where the application layer architecture is unable to protect the privacy of certain headers (e.g., the SRTP headers). The SBC also helps on several security dimensions by isolating the key VoIP servers from the core network. This suggests that Architecture B is more secure than Architecture A. The difference is small enough that an architecture similar to A may be applicable for other systems with different assumptions. For example, the Navy may have different assumptions about how significant the risk of certain threats are or about how existing mechanisms may already mitigate other potential threats. Because the architectures scored fairly close to each other, it is possible that small changes to the architectures (e.g., in how the system protects against potential attacks originating in the core network) may alter the results of the analysis.

Most of the weaknesses between the converged scenarios and non-converged ones fall into two categories. The first category includes weaknesses due to the converged network being managed at the lowest security level (e.g., unclassified). This may lead to a number of security violations. For example, administrators could sniff packets or insert routes that redirect packets from the classified network. The second category includes weaknesses due to protocols that pass the converged network unencrypted. For example, the architectures do not attempt to encrypt the non-VoIP-specific protocols, such as DNS and SNMP. The combination of the two categories leads to risks that are greater than either group alone.

Note that for a different set of assumptions, the severity of the weaknesses becomes reasonable. For example, even though the core network has to operate at the lowest security level, the Navy may require a policy to ensure that the individual network administrators pass a background check (or possess clearances) to mitigate the risk of an administrator intentionally reconfiguring network equipment to reduce the security of the system. Additionally, the network equipment should have mechanisms such as authentication logs and configuration change logs that mitigate these concerns by recording which administrator made such changes.

Similarly, a different set of assumptions could help mitigate the risk of exposing the unencrypted data protocols on the VoIP network (e.g., DNS). For example, the Navy may be comfortable allowing these protocols over the converged core if tighter controls exist on who has access to the converged core. Alternative architectures could be used to provide security for the data protocols. For example, the data protocols for the VoIP network could be routed over an IPSec gateway that is used for the data network such that the unencrypted portion is contained within a physically secure room (e.g., SCIF).

Without any mitigation strategy, the threats associated with the converged network are too significant to justify adopting. With a mitigation strategy, the risks associated with convergence become acceptable, and the best option is the presented design with Architecture B (the IPSec-based solution).

If IPSec is used for all calls, then they are all secured communications; this method may be seen as being too protective. The overhead of IPSec is large compared to the transport layer protocols. If all communications are secured and a method of determining encrypted calls can be determined, can a single switch be used that is RED that all communications passed through? This has a cost saving because of the reduction of the number of switches, compounded if redundancy is implemented. The "Encrypt" could be added to the INVITE as a parameter and only another device that can support encrypt will accept the call. This is a function that SIP will negotiate the parameters between user agents. In the conceptual design two switches are represented, it can be looked at as redundancy or as RED/BLACK separation.

3.17.5 Hardwire Network Infrastructure

The security of the IP packet network leads into the IP network infrastructure. In the past, several different topologies have been used from Frame relay through ATM to IP networks. These different topologies have been used for both communications as well as data in separate networks, for the most part. In a converged network for VoIP it comes down to two architectures.

Two different topologies are considered for the network architecture. The objective is to develop network designs with these two architectures incorporating the requirements and then analyze them from perspectives of overall network design (number and types of network nodes, number and types of network links, and link bandwidths), fault recovery, performance of real-time applications, such as VoIP, Video conferencing, and satisfaction of QoS for different CoS in normal and stressed condition.
It is noted that although there are multiple categories of applications, the Navy vessel is like a self-contained enterprise location and typical topologies and principles that apply to enterprise network design apply. Given the size of the user community and the location, the two topologies that constitute candidate core architectures are:

- Distributed-star
- Mesh/Partial Mesh.

The tree topology was considered as a possible candidate as it supports the client-server and computing-cluster types of application flow models and because it suits applications that require communication and interaction with multiple servers attached to different edge hubs. However, tree topologies are primarily architected for reasons of geographic conformity with user communities as in cable networks. Once some of the nodes in the tree's trunk require higher levels of interconnection due to traffic flow requirements or for additions of network and application level functions, the tree essentially becomes a partial mesh topology. Due to the requirements of numbers and types of traffic flows in a multi-application network, it is envisioned that a partial mesh topology is better suited than a true tree topology.
In the following sub-sections a distributed 2-star topology (with routed interconnection between the star hubs) and a partial mesh topology where certain edge nodes have routing functionalities are discussed. This topology is specific to the interconnection of the edge switches. The common aspect of the two architectures is the edges. The edges in both these cases will support LANs. The user devices will connect to the edge switches through 10/100 BaseT and the core connections (among the edges and the cores) will be GigE. To enable higher performance, there will be multiple functional Virtual LANs (VLANs) that connect users at different edges. Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP) will be used for enabling loop free topologies with sub-second restoration in case of edge failure, switch-over, or addition.

3.17.5.1 Distributed 2-Star

The basic single-star topology features a hub and spoke architecture and is suitable for client-server applications and traffic flows. It is a simple architecture and can be used with modifications or enhancements to enable distributed client-server applications with several hubs (distributed-star). Depending on performance and any special reliability requirement, multiple hubs and multi-homing of the edges to the hubs can result in a highly robust and well performing network. The disadvantage of star topologies is that when the hub fails all devices attached to the hub are affected. Distributed star with hub backups solves that issue to a large extent. The following Figure 3-74 illustrates the distributed 2-star topology we used for designing the network.

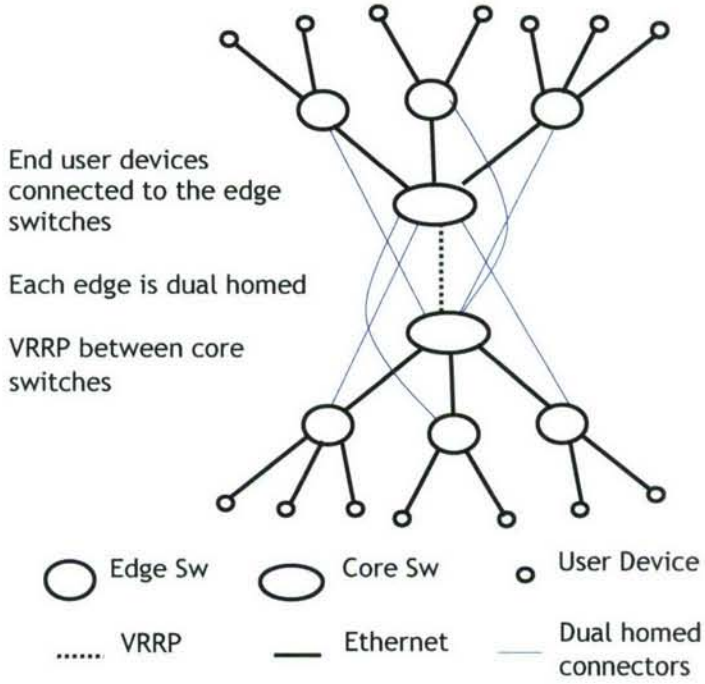


Figure 3-74. Architecture with Distributed 2-star Topology

The user devices can also be multi-homed if there is a need for protection from single failures. This is not shown in the diagram.
This topology can be extended to multi-star (e.g., 3-star) with triple-homing if there are requirements for protection from double failure, or better load balancing of traffic. In general, this will provide better reliability. However, the trade-off will be in terms of added links, complexity in configuration maintenance, and operations. It needs to be assessed through simulation and testing if this adds to the restoration time for failure recovery.

3.17.5.2 Mesh/Partial Mesh

Mesh networks provide the most connectivity by interconnecting the nodes directly. In this case if all the edges are meshed then each edge is only one hop away from each other. This provides better performance, especially for peer-to-peer traffic (like VoIP), since traffic between edge switches does not have to pass through the core routers. The trade-offs will be in terms of added links, complexity in configuration when adding nodes, and operations. In most network designs, depending on the performance requirements (e.g., maximum number of hops, latency, jitter, network reliability) instead of a full mesh a partial mesh suffices. That is the approach taken here. The full network is again a hybrid where the end devices are star-connected to the edges and the edges are partially meshed, based on the traffic flow and performance requirements. Figure 3-75 illustrates the architecture with a partial mesh topology. This connection pattern was chosen so that every edge switch is no more than two hops from every other edge switch. Note that two of the edge switches will be switch/routers, which will be dual-homed to central servers.

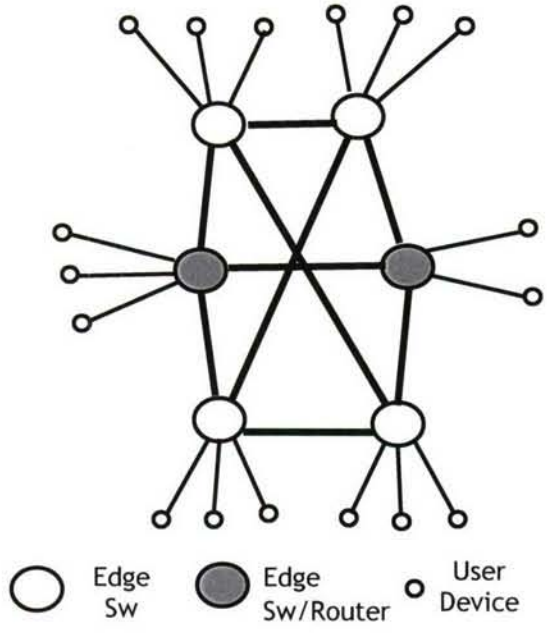


Figure 3-75. : Architecture with Partial Mesh Topology

The conclusion is that both the dual-star and the partial mesh topologies can support the assumed traffic load from the given applications adequately. In both cases, for reasons of optimized load-balancing across the critical node(s) so that a failure at the critical node does not disrupt all or most traffic, VLANs are very useful and needed. Adding VLANs have to be necessarily supplemented with proper operations plan including maintenance and reconfiguration with Multiple Spanning Tree (MST) or per-VLAN spanning tree (PVST). Additional resiliency techniques such as Virtual Router Redundancy Protocol (VRRP) should be utilized for the routers.

3.17.6 Recommendations for Topology

Experience from other large network designs indicate that it is desirable to segregate traffic such that the overlap of traffic types, class of service (CoS), and traffic flow types are minimized. This is better accomplished with VLANs in partial mesh topologies.

The Network Design and Analyses whitepaper also addressed methodologies for enabling QoS with 802.1p user priority in the VLAN tag of Ethernet frame, and Differentiated Services Code Point (DSCP) in the IP packet headers. Using DES, the QoS of a particular CoS with traffic surge conditions can then be analyzed. Similarly the process for studying the behavior of a network after a node failure, specifically how the traffic is rerouted in the post-failure recovery network, the capacity utilization in the new network, and the performance of traffic types in the new network, have been described in the paper.

Link or nodal failure assessment will be a recursive study of first determining the most utilized link or node through survivability analysis, then failing the most utilized link to get to spanning tree re-convergence, and then running flow analysis and DES. The processes were described but given the network characteristics and the traffic load, such simulations were not explicitly carried out.

From the results of these particular designs as well as our theoretical and other practical experience with network designs, it is recommended that the next step should be to put together practical operable networks with converged services and gather real data from monitoring and probing

network elements. This study shows that the network topologies that should be compared are dual core and partial mesh with VLANs. The number of switch/routers in the distributed star design and the meshed design can be increased if the reliability and performance needs to be better. Our expectation is that partial mesh networks will be more scalable (necessary for adding network segments) and perform better in those conditions. The precursor to configuring the "live" network is proper design, i.e., configuring the spanning tree roots and cutoff links, configuring multiple VLANs properly, developing proper routing addresses and routing plans, and developing and implementing proper QoS treatment. These pre-planning functions should be performed using proper tools and experience network designers.

3.17.7 Wireless Network Technologies

3.17.7.1 WiFi

WiFi is the standard technology for wireless local-area data networks. Commercial success and competition (primarily in residential and office environments) has lead to very cost effective equipment. The success has also driven considerable development efforts to improve the bandwidth and signal quality of WiFi devices. Because WiFi is inexpensive and limited in range, it is common (and feasible) to have many access points to cover a small area (e.g., one access point per compartment or for every other compartment).

Initial attempts to provide voice service over WiFi have been only moderately successful. Under good conditions (e.g., a strong signal with few users), VoIP over WiFi operates just like VoIP on a wired network. As additional users contend for the data bandwidth (e.g., transferring files), the quality of the voice call quickly degrades. Similarly, if the signal is weak, there may be short service outages that also degrade voice service. Several advances in WiFi may help address these problems: traffic prioritization with WMM, increased bandwidth, and improved coverage with MIMO (802.11n).

We expect that multipath interference in large, open interior areas (e.g., hangers) will be problematic for WiFi due to delay spread. Unpublished experiences with first generation WiFi equipment in the airship hanger at Lakehurst, NJ support this expectation. Actual measurements with more recent WiFi devices could quickly determine the extent to which multipath degrades WiFi performance.

3.17.7.2 WiMAX

WiMAX provides significant bandwidth improvements over the other technologies. Because it was designed to support data and voice applications, it has provided QoS capabilities from its inception. WiMAX supports protocols (e.g., MIMO and OFDM) that are resistant to most of the impairments found in RF-challenged environments.

WiMax is a new technology. As such, the cost is still relatively high and not all of its features have been proven in the field. The initial WiMAX applications are used primarily for point-to-point connections (similar to what is needed for ship-to-shore).

3.17.7.3 Cellular

Cellular systems provide near-ubiquitous voice coverage at (or close to) toll quality. Commercial pico-cell designs (including base station routers) and distributed antenna systems can be used to create a cellular network extension (or private network) in an RF-challenged environment (usually indoors or underground).

Although cellular technologies support data applications, the data rates are lower than the other technologies. The data rates, however, are constantly improving. Unlike the other data networks, where voice and data compete for the same resources (e.g., a single channel), cellular systems can reserve channel resources. Because channels are independent, the quality of voice and data applications does not degrade (until the system approaches its capacity).

Cellular systems have questionable security. Cryptographic systems in GSM and CDMA use weak key sizes and potentially vulnerable algorithms.

The spectrum issues may affect cellular technologies. In general, voice bands are fairly well standardized because of the industry's push for mobile sets that can operate globally (e.g., otherwise frequent travelers would need several cell phones depending on where they visit). It is not clear that data services (e.g., UMTS) will be able to share the same level of commonality.

3.17.8 Comparison of Wireless Technologies

This section compares each of the wireless technologies vis-a-vis several issues described in previous sections. Table 3-37 summarizes how the technologies differ on each issue.

Table 3-37. Comparison of Wireless Technologies

Issue	WiFi	WiMAX	GSM	CDMA	Comment
Rayleigh Fading	Good (MIMO and OFDM)	Good (MIMO and OFDM)	Okay (MGSK supports equalization)	Okay (spread spectrum)	All modern systems use techniques to tolerate Rayleigh fading.
Delay Spread	May be issue in large rooms (short symbol period)	Good (flexible parameters and long symbol period)	Poor	Poor	Delay spread is an issue on ships in large rooms.
Doppler Spread	Okay (implementation s likely to tolerate only small frequency shifts)	Very good (OFDM is sensitive, but systems designed for high mobility)	Excellent (designed for mobility)	Excellent (designed for mobility)	
Attenuation	Low power (~20dBm)	Medium power (varies ~25dBm)	High power (30dBm average; 40dBm peak)	High power (30dBm average; 40dBm peak)	Attenuation limits range (see Maximum Range below) and reduces Co-Channel Interference (below). Otherwise, attenuation has little impact in comparison.
External Interference †	Okay (MIMO, but low power)	Okay	Okay	Good (DSSS gracefully degrades with strong interference)	All systems are designed to tolerate moderate levels of interference.
Co-Channel Interference †	Good (low power/short range allows multiple devices to reuse channel at moderate distance; though number of channels (3) is small)	Poor (reuse usually depends on careful engineering)	Poor (little protection, e.g., frequency hoping, between reused channels, but many channels available)	Good (DSSS gracefully degrades with CCI; though number of channels (~6) is small)	A fair comparison depends on the number of systems and distance between systems. Having fewer available channels suggests that channels will need to be reused more frequently.

Issue	WiFi	WiMAX	GSM	CDMA	Comment
Data Rate	Very high speed (~100Mbps)	High speed (~75Mbps)	Low (data rates improving)	Low (data rates improving)	Data rates are shared differently between multiple user in each technology and vary with signal strength.
Maximum Range	~100-300m	Up to 30km	~35km	~35km	Typical ranges are often much less than maximum.
Spectrum Issues	Very minor (low power and unlicensed spectrum)	Poor (lacks standard spectrum)	Minor (small number of bands used)	Minor (small number of bands used; not accepted globally)	
Data Traffic	Excellent	Excellent	Poor (low data rate)	Poor (low data rate)	
Voice Traffic	Historically poor (new high speed versions may perform better)	Very good	Excellent	Excellent	
Security	Good (early versions had issues)	Good	Questionable (small key size and non-standard algorithms)	Questionable (small key size and non-standard algorithms)	
Interference					See External Interference, above.
Jamming[†]				Long sequence offers some protection	All technologies are susceptible to jamming. MIMO has better resistance to jamming than other technologies.
Cost	Low	Moderate (high but dropping)	High (inexpensive reduced feature base stations are entering market place)	High (inexpensive reduced feature base stations are entering market place)	
Availability	Currently available	1-2 years (some products available today)	Voice available today; data protocols only supported in commercial (service provider) versions	Voice available today; data protocols only supported in commercial (service provider) versions	
QoS	okay (service classes defined)	okay (service classes defined)	good	good	

Issue	WiFi	WiMAX	GSM	CDMA	Comment
†*External Interference* is random (e.g., Additive Gaussian White Noise) interference from external sources found in the environment. *Co-Channel Interference* is interference from competing systems (e.g., to communication systems using the same protocol and frequency). *Jamming* is interference caused by a potentially capable adversary with the intention of disrupting service (e.g., using high transmit power, bursty timing, or knowledge of the protocols).					

All the systems offer some support to counter Rayleigh Fading. The combination of OFDM and MIMO found in WiFi (802.11n) and WiMAX should provide good protection. The cellular systems have modest protection in their coding techniques.

We expect delay spread to be problematic in medium to large interior rooms. Most potential countermeasures, such as DSSS and equalization, depend on certain properties and consistencies in the multipath signal. Such approaches would be ineffective in such environments because of heavy scattering. WiMAX uses a relatively long symbol period (103μs) and supports configurable parameters for guard intervals. These properties should help WiMAX systems to tolerate the long delay spreads expected in large, metal rooms.

Doppler spread may be an issue for ship-to-ship communication. Cellular technologies and WiMAX, which were designed to support mobility, compensate for Doppler. WiFi needs to provide some mechanism to account for Doppler because OFDM is otherwise sensitive to frequency shifts. It is unclear how much protection WiFi implementations provide.

Attenuation is not necessarily a bad feature for wireless systems. For example, signal loss is essential to prevent co-channel interference. Signal power and receiver sensitivity determine how much signals attenuate and how strong the signal needs to be at the receiver to process the data, respectively. Frequency is not an issue for the technologies and environment considered (low frequencies tend to penetrate obstructions, such as foliage, better than higher frequencies). Range is related to attenuation. Due to their higher transmit power, cellular technologies and point-to-point WiMAX configurations provide excellent range (e.g., 10 km or more). WiFi has a smaller range (e.g., 300m outdoors), but channels can be reused in close proximity (e.g., every compartment or every other compartment inside the ship).

All systems are designed to tolerate some amount of external interference. CDMA gracefully degrades service as interference increase. Spreading the signal energy in time, space, or frequency (e.g., long symbol period, MIMO, and DSSS or OFDM respectively) helps systems to tolerate interference. For the same signal to noise ratio, high power systems can tolerate more noise.

Co-channel interference has many dimensions, which makes comparisons complicated. WiFi, which has only three non-overlapping channels available (excluding 802.11a) is typically deployed in environments where it is subject to some co-channel interference. The impact of the interference often leads to dropped packets, but is seldom detectable by the user. Due to its low power, interfering channels are usually weak. CDMA is very graceful about handling co-channel interference, because each user has its own CDMA code. Because the number of channels is very small (about six) and each cell is large (e.g., 10km radius or more), careful planning is needed in

high density areas to limit the amount of channel reuse. GSM and WiMAX lack specific techniques to handle co-channel interference. Careful planning is generally required.

Data rate is an important metric for data networks. WiFi supports maximum data rates over 100Mbps, which is shared between all users connected to the access point. WiMAX supports data rates around 75Mbps. The protocol supports efficient OFDMA-based bandwidth shared between users. Cellular technologies provide much lower data rates (up to a few Mbps), though data rates are constantly improving. For data applications, bit errors can greatly reduce the end-to-end throughput (e.g., due to TCP timeouts and retransmissions). For all wireless technologies considered, users typically see much lower data rates because the maximum rate requires a strong signal.

Inside a vessel, range will not be a limiting factor for any technology. For ship-to-ship and ship-to-shore, WiFi's approximate 300m range (without special antennas) is probably insufficient. The remaining technologies all support ranges over 10km (with theoretical limits around 30-35km).

Spectrum considerations are an important issue for most of the technologies, except for WiFi. With WiFi, spectrum is probably not an issue because (a) it uses unlicensed spectrum that is close to globally accepted and (b) it has low power and range which makes it unlikely to interfere with other systems in port. Spectrum is an issue for the cellular technologies, but because there are only a small set of bandwidths used, it may be possible to reconfigure the BS's frequencies as needed using software defined radios. Otherwise, the BS can be turned off when in port. WiMAX has not yet established *de facto* standard frequency bands. Instead, several bands exist and new ones are being added. Adjusting to each country's regulations may be an arduous task, particularly in the Pacific where many different bands are being used.

WiFi and WiMAX provide much higher maximum data rates (~100Mbps) than the cellular technologies (a few Mbps). In each case, the maximum single-user data rate is much higher than the typical data rate users would experience. The actual data rate depends on the signal strength and the number of users contending for the same channel.

Cellular networks are optimized for voice. WiMAX has been designed with VoIP support in mind and is expected to provide toll-quality voice service. Voice service with WiFi has traditionally been very low quality (except under controlled conditions). Newer WiFi equipment with higher bandwidth and better coverage (e.g., due to MIMO) should perform better than older systems.

WiFi and WiMAX provide very good security due to use of standard encryption algorithms (e.g., AES) and authentication interfaces (e.g., certificate based mutual authentication using Extensible Authentication Protocol- Transport Layer Security (EAP-TLS). Earlier versions of WiFi had notoriously poor security (e.g., WEP). Cellular technologies suffer from non-standard cryptographic algorithms and short key lengths.

All technologies are susceptible to jamming. In particular, the signal acquisition phase is susceptible in all COTS products. MIMO offers good resistance against jamming because (a) it usually treats jamming like other noise and (b) it has extra degrees of freedom to reconfigure antenna pairs to work around jamming.

Because WiFi is extremely popular in several environments, it is very cost effective. WiMAX is currently expensive, but prices are likely to drop as it grows in popularity. Most cellular systems are geared for the provider market and are very expensive. Reduced-feature pico cell base stations are more cost effective. End user devices (e.g., wireless data cards) are now cost effective.

WiFi is available today. WiMAX is just starting to become available. We expect WiMAX sales to increase over the next couple years. Cellular systems are available today. Over the next several years, cellular systems with increased data rates will become available. Support for specialized (miniature and ruggedized) COTS cellular technologies lags a few years behind the availability of provider-market equipment.

WiFi and WiMAX define service classes to support multimedia sessions. It is not clear if any applications make use of such classes of service. Cellular technologies use separate channels for voice and data eliminating traditional QoS concerns.

3.17.9 Recommendations for Wireless Network Technologies

This report identifies key issues that affect COTS wireless systems in a naval environment. It first identifies impairments to general wireless systems. Next, it examines the different naval applications of wireless to identify those impairments that are most critical. Next, it provides technical background on how different wireless techniques impact the impairments. With an understanding of the technical background, it explores several COTS technologies (WiFi, WiMAX, and cellular) focusing on how well the technologies handle the impairments. The report also examines important issues, such as spectrum issues, applicability to voice and data traffic, security, interference, jamming, cost, COTS availability, and QoS. The report then summarizes the pros and cons of each technology and compares the different technologies.

A ship's metal infrastructure provides a challenging environment for wireless communication. The metal walls reflect signals repeatedly, contributing to multipath effects. Particularly in large rooms, where the signals can travel 50m or more before hitting a wall, the multipath effect can be significant. Although most systems are designed to tolerate some degree of multipath, we expect large interior rooms, such as a hanger inside an aircraft carrier, to create too much multipath interference (specifically, in the form of delay spread) for most wireless systems to handle. The actual performance for wireless technologies within the ship can be assessed best with a site survey, where accurate measurements of wireless equipment can be made at sample locations.

Outside of the ship is a relatively good environment for wireless communication. Spectrum license issues, however, may restrict usage for ship-to-shore applications. The deck may include regions where other systems (e.g., radar) may cause interference. A site survey can quickly determine if any such systems would be problematic.

Between WiFi, WiMAX, and cellular technologies, there is no clear winner. One can choose a technology for the interior of the ship (and on deck) independent of the choice for ship-to-ship/ship-to-shore communication because they are independent networks connected to the wired backbone network.

WiFi is most likely the best choice for inside the ship, primarily because it is a proven technology and very cost effective. In some areas, such as large rooms, WiFi might not operate. Voice quality

over WiFi (e.g., VoIP over WiFi) has provided particular low quality in the past. Newer systems may provide better service due to better bandwidth and coverage.

WiMAX appears to be the best choice for ship-to-ship and ship-to-shore communication because of its high data rate and range. As WiMAX is in the early stages of adoption, it has not yet proven itself, as the other technologies have. One potential area of concern with WiMAX is spectrum availability, where each nation may have different regulations on frequency and power.

Cellular technologies (e.g., GSM/UMTS) are also possible. The next generation is expected to provide broadband data rates to mobile users. Security in cellular technologies is questionable due to small key sizes and potentially vulnerable cryptographic algorithms.

3.17.10 Conclusion

The requirements break into two parts. The first part is the individual end devices and system applications. These are included in the derived baseline that is used as a specification in this project. The other requirements are system wide, and are not addressed in a single place because the current design has each component separated, so each part has its own requirements. From the above sections on security, topology and wireless technologies, requirements covering the different systems need to be solidified. This converging of the multiple networks now needs to define requirements so individual packet types have set quality of server (QoS) defined. Even with in a single category like VoIP traffic there are multiple levels, of priority, to only mention one area.

In the derived baseline the individual device redundancy is covered, the application server and network component redundancy is not. The requirement for network and application server redundancy requirements need to be solidified as well.

In the area of mission critical systems, the Navy has always had fail-safe systems. For the internal communications system it has been the sound powered telephone system. This is another level higher then redundancy, by being a separate system that has no reliance on any part or power source of the internal communications system. To have this level of redundancy in a VoIP system a sound powered telephone system can be implemented in parallel to provide this higher level of redundancy. In most cases the standard practice for a data network relies on redundancy of equipment and connections between the hardware with very high levels of reliability and availability. Just adding equipment and network connections between switches and routers will not always result in a faster to recovery and more stability solution. Network analysis needs to be done with automated test programs like OPNet's SPGuru® to create and validate the design before it is purchased and installed on the vessel.

Each of the end devices need to be looked at to determine if VoIP solutions have been designed that match the requirements. The end device section discusses the changes that are required for the different end devices. In many cases a media gateway can be used as a converter. In some cases the right choice will be the media gateway, where the cost of development or the development cycle will be too long for the schedule to implement the move to VoIP. Each end device needs to be tested in a lab environment so the features can be verified with the chosen IP-PBX. Depending

on the method of security, changes to the SIP headers may be required to support tags like "Encrypt" so each end device can determine if it can connect to another end device, depending on the tag level of both devices.

In many cases it will not be possible to remove everything from a vessel and replace it with a complete system. In many cases only a single system or subsystem is being refitted at a time. This is very possible with an IP Packet based network and VoIP. The two systems can be combined with the use of media gateways to interface between the older TDM systems and the new VoIP system being installed. Depending on what is being refitted, it can be only an administrative phone system or a set portion of the vessel that has been damaged. The other reason for installing a hybrid system is to slowly move into the VoIP technologies in a controlled process, only replacing non-tactical end devices at first and then replacing tactical when the sailors and the commanding officers build up confidence in the technology. Depending on the presently installed TDM PBX, the manufacturer may have solutions that are used presently for the commercial customers to implement this hybrid solution. The other method is to use another manufacturer and use the media gateways between the two PBXs creating a connection between them.

The transition from TDM and segregated networks to VoIP and a converged network will be a process that will be done differently on each platform. Many reasons outside of the influence of this report will control the schedule and final technologies that will be finally used. It will be very important that the topology and security that is selected is tested and certified, so it is accepted and adopted across multiple platforms. Products in the Navy and groups like SPAWARS needs to be allied, like CANES, to have acceptance by all groups that can influence the final outcome.

3.18 Recommendations and Conceptual Design

This section explains why individual parts were included in this conceptual design. The design is vendor independent (unless otherwise noted); in the test bed design some components will be combined or separated depending on the vendor's solution. The number of end devices is limited, to show the different ones, but not the number of them for an individual platform. This design is fashioned after a submarine proposal that was developed and quoted for a friendly nation.

3.18.1 Infrastructure

The infrastructure must be designed to support the IP packet traffic for voice, video and data. Because there is no specification and we are not using defined vendor components a system analysis will not be done. Please reference Appendix C for an analysis of a representation network design.

3.18.2 Switches

3.18.2.1 Core Switches

The core switches connect the different major data centers in the vessel and maintain multiple connections between multiple core switches for survivability. In this design we have chosen to use 24 port PoE switches. The switches are connected using 2 different methods. The first method is a 10-gigabit stack link. This would be used if the units were stacked upon themselves as in a rack. The length is limited by this method, but the throughput is 10-gigabit and it is usually standard on switches. For switches that are in distributed racks a 10-gigabit fiber network connection is used. Each switch connects to the other core switches in a full mesh topology. Even thou the switches contain PoE ports, it is meant for support work and they are not expected to be used for end devices or access points. The end devices will be connected to the edge switches, in a star topology.

3.18.2.2 Edge Switches

The edge switches are the switches that the end devices connect to and are distributed throughout the vessel. They are distributed throughout the vessel where the runs to the individual end devices are short CAT 5 copper cables and the multimode fiber run to the core switches are longer. Each edge switch will connect to two different core switches, resulting in survivability if a single core switch or connection is damaged or fails. This will also allow for load balancing that would be determined by the analysis that is done during the design phase of the system.

3.18.2.3 Support Switches (not shown in diagram)

Support switches will be included in some racks were small switches are required to connect like data/security types together. The switches are non-managed and will only support a single VLAN. One place this will be used in between the SBC and the IP-PBX components.

3.18.3 Virtual Local Area Network (VLAN)

The uses of VLANs are two fold in this design. The first use of VLANs is to allow balancing of network traffic through multiple switches.. This results in no one single switch becoming a point of failure for a high percentage of traffic. The other use of the VLANs is to add security to the

network design. Each functional group of devices and servers will be located in their own VLAN group. Layer 3 filtering will be used to connect VLAN devices that require connecting to multiple VLANs. In this design we have created eight different groups:

- Video
- Administration
- Announcing
- Gateways
- VoIP Servers
- Workstations
- Data
- VoIP Devices

A tactical dual homed dedicated station with a softphone is shown bridging the VoIP Device and Data VLANs. In this case the unit has two network interface cards that connect to the different VLANs. For reliability this could be increased to four, two to each individual VLAN.

3.18.4 Wireless Network

The wireless network is two fold in this design. It will carry voice as well as data; it is an extension of the wired network that is handled by the network switches. Within the wireless network there are two different technologies that will be used. The first is WiFi for the internal communications. This technology is comprised of two major types of components. This is vendor determined, and each vendor's solution varies greatly. This design is shown as an Alcatel-Lucent WLAN design.

3.18.4.1 WiFi Wireless Controller

Wireless controller manages the individual access points (AP). In this design this unit is redundant, with two individual units that load balance unless one of them goes off-line then the other wireless controller controls all of the APs. It manages the power output of the AP as well as the security. Hand-offs between AP is not noticed by the wireless endpoints so they don't have to authenticate to each one. The power output and channels management allows the AP to not overlap, so no intensive site plan needs to be done initially and then continue to be updated as changes to the wireless network are made.

3.18.4.2 WiFi Access Points

The WiFi Access Points (AP) are located in any compartment that will require wireless access. If the room is large it may require more then one to cover the room. The controller manages the power output so there is minimal overlap as well as channel separation. For this type of controlled system the AP must be from the same manufacturer as the controller. If the design was done without a controller then any AP (from any vendor) could be used in any location. This would result in a site plan that would need to be extensive, as well as after being installed the individual areas would need to be measured and AP moved to even out the coverage. Because of this the use of the controller system makes sense. Some vendor's AP can be installed as dual homed devices allowing for survivability if a failure of an edge switch or network cable occurs.

3.18.4.3 WiMAX Access Points

This access point is different then the WiFi ones discussed above. This is used for the external communicates. Depending on the requirements and where the antenna will be mounted will

determine the types of antenna that will be required. For close range shore communications it will require it to be mounted high, this will cause issues with the roll of the vessel. This would only work for a surface vessel, since the signal will not transmit through water. To support the boat the antenna needs to be mounted lower so the range is limited and the affects of the rolling of the vessel would be reduced. The use of automatic focusing equipment can be used to direct the signal to the matching receiver, reducing the affects of the roll and pitch of the vessel.

3.18.5 Security, Protocols and Codexes

Security, protocols, and codexes may be completely separate from the vendor that is chosen or they may have the vendor's own preferred proprietary ones that are better. The use of open system ones will allow for future changes that don't tie the Navy into a single vendor. This will be important for the end devices that may not be purchased from the same vendor that supplies the infrastructure or internal communication system.

3.18.5.1 Security

There are several sections and appendixes that contain information about security. Security is divided into multiple components. The first is the infrastructure that requires either application layer or network layer implementation. Both methods have benefits and disadvantages, from the research done by Bell Labs. For this design concept we will go with network layer security. Network Layer security uses IP Security (IPSec) that can be added to IPv4 and is native to IPv6. This will require the end devices to also be aware of IPSec, which is not supported by many vendors currently. The session boarder controller (SBC) will encode/decode IPSec so the IP-PBX and supporting servers will not have to do it in software. The SBC encode/decode should be handled in optimized hardware instead of software to achieve improved performance. It also has to be handled at the administrator level, so some issues noted in Appendix I "VoIP Security Study "can be mitigated. This is handled with policies being created and followed, for the administrators of the network. Another area is that the main racks are secured with locks so individuals cannot access the servers. This also keeps individuals from cross connecting between secure and non-secure VLANs or physical networks. In Appendix M "Internet Protocol Telephony & Voice Over Internet Protocol Security Technical Implementation Guide" they discuss different network security configurations. In this conceptual design we have chosen the Voice Over Secure IP (VoSIP). This method defines that you secure the network and then the voice rides on top of the security.

3.18.5.2 Protocols

In the above topic the protocol for security was reviewed. This section, discussed some of the protocols that will be used other then the security ones for VoIP. The voice traffic will use SIP for the control signaling and RTP for the bearer. These two protocols are open system and are continually being improved with new functionality. There are many other protocols that will be used, but they are standard on the data networks.

3.18.5.3 Codexes

In the initial design G.711 will be used for the voice compending. G.711 packet size is larger but has good MOS scores when the packet loss is low. Because of the limited number of end devices in this conceptual design, this choice makes sense. In the final implementation a lower bit rate codex like G.729 should be used to compensate for the bandwidth issues and possible loss of packets in a production network environment. This will also reduce issues with the WiFi VoIP

bandwidth that is noted in the Appendix E "Shipboard Wireless Communication Study". There are many good low bit rate codexes, some of them are free to use and others like G.729 have to be licensed per end device. The switching between codexes is very CPU intensive so this needs to be evaluated if the use of more then one codex is used. Each end device must support the codex that is chosen and if there are multiple codexes there needs to be a device like a session border controller (SBC) to convert between them. This is made easier if the traffic passes between different networks.

3.18.6 Network Management System

Network management system is an important tool for managing the network and the components on it. In many cases the vendor that supplies the switches or the IP-PBX may have their own proprietary one that integrates tightly to their hardware components. There are also others that support multiple vendors' hardware, but they do not supply the same degree of control over the hardware. This tool allows configuration of the hardware from a single point as well as monitoring and fault detection. This technology was not evaluated in this study.

3.18.7 Network Resource Servers

For any network there are standard resource servers that need to be included. These resources were not reviewed in this study since they are standard on any network. There is some variation, depending on the network's use. I have included a few that are required for the VoIP network, but others may be required depending on the vendor and how the security is implemented. In this design a redundant server is shown as a domain backup for these services. These resources may be duplicated in both the VoIP VLAN and the Data VLAN, depending on how the infrastructure is developed and security policies are created.

3.18.7.1 Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a service that runs on a primary network server. This protocol allows devices on the network to request IP address that are available for assignment. Other parameters may also be included like default gateway, DNS and subnet mask. This allows for a dynamic addressing scheme so the administrator does not have to manually configure each device's IP configuration on the network.

3.18.7.2 Domain Name System

Domain Name System (DNS) tracks the hostnames of the individual devices on the network so the devices can be located with a human-readable name. Depending on the VoIP implementation used this may or may not be required for VoIP.

3.18.7.3 Trivial File Transfer Protocol

Trivial File Transfer Protocol (TFTP) is used by many devices to retrieve the configuration information that is required. For a phone this would be the SIP server address, extensions, and general configuration. Many COTS products can also get updated firmware and application code during the boot process from the configuration server. Depending on the device this may be done with other protocols HTTP or secure protocols. TFTP is inherently non-secure, but because of this, it will allow thousands of devices to access it with limited performance degradation.

3.18.7.4 Hypertext Transfer Protocol

Hypertext Transfer Protocol (HTTP) may be used for the configuration of devices like TFTP, as well for several other functions. Many IP-PBX systems use a web server for system configuration, configuration of individual accounts as well as voicemail configuration and collection. Several end devices contain web servers for configuration of themselves. In larger installation this method is not used, and should be disable since it can create a security hole in each device. The secure version SHTTP (RFC 2660) should be considered for a production system, depending on what is hosted on it.

3.18.7.5 Network-attached Storage

Network-attached storage (NAS) is part of networks for many reasons. For the VoIP installation there is several processes that will use storage. Configuration information will be offered by the TFTP or HTTP server but must be stored on the network. Depending on how this is done there may be a large number of files that are maintained. The voicemail also requires a place to store messages. A large consumer of the storage is the recording of voice calls and video. This process needs to be managed, because even the largest of NAS devices will be over run with this type of data if not carefully controlled and monitored. In many cases this storage is also backed up by an automated system, and having it contained in a single location eases the administrators job. The NAS is made up of multiple high capacity drives that are configured in some level of redundant array of independent drives (or disks) (RAID) that provides data reliability and I/O performance.

3.18.8 External Connections

External communications is outside the scope of this report. In the diagram we show connections for the different types but we don't get into security for each individual type. The encryption devices are not reference in this document. Each of the individual areas is covered in a high level review only.

3.18.9 Data

Data is handled in 2 different methods connecting to the external environment. In seaport, the connection is discussed in the Firewall section. Data is encrypted and sent through a satellite link while the vessel is underway. This link is a low bandwidth connection so limited amounts of data are transferred.

3.18.10 Voice

Voice has several different methods of being connected to the external environment. The satellite link is low bandwidth but can be used. It would be passed the same way as the data packets, but there would be some expected jitter from this method. The trip to and from the satellite adds a noticeable delay over the acceptable 150ms. While in port there are three different methods that can be used. The first is the firewall that will be discussed at the end of the data section. The use of media gateway is used to convert the VoIP to TDM, so it can be placed onto the PSTN. This method would have to be secured between the IP-PBX and the shore PBX before entering the PSTN. This would include analog phone lines as well as T1 PRI, both of these are common interfaces for the TDM network. Different seaports have different types of connection; this is why both methods are exposed on the vessel.

3.18.11 Video

Video is handled through the firewall as well. These packets can be transferred in batch mode to a single repository or reviewed from the video-processing server. The methods and security would have to be configured in the firewall. Video uses large amounts of bandwidth, so priority needs to be configured in the firewall for each type of packet and possible method of connection.

3.18.12 Firewall

IP packets that are transferred externally should be passed through the firewall, even the traffic being encrypted for the satellite link. The firewall is designed to be the wall between internal and external networks, a session border controller (SBC) may be required for processing the VoIP, depending on the firewall used and the security requirements. The WiMAX Access Point should also be placed on the outside of the firewall. If the WiMAX is only used for VoIP then the rules in the firewall should only allow that traffic from the WiMAX external antenna to pass through to the session boarder controller, in a VLAN or tunnel.

3.18.13 UPS

The uninterruptible power supplies (UPS) are used to maintain the equipment during times that vessel power is lost. The sizing of the units is done relative to load and the length of time required for the equipment to stay powered. This equipment varies depending on the time to load ratio and supply power. The grounding requirements on board a vessel are different so there are specially wired UPS that are developed for shipboard use. The two main uses for the UPS are in the nodes and the edge switches enclosures.

3.18.13.1 Node Racks

In the node racks there is a large power requirement that require a large UPS to maintain the racks power. Some of the equipment may require different requirements, so multiple UPS may be deployed to handle the different requirements.

3.18.13.2 Edge Switch

The edge switches are lower power consumers compared to the node racks. In this case a single power requirement only needs to be supported. In most cases a single switch will need to be powered, in some cases depending on the design there may be media gateway that also require power in the same enclosure. Because the IP-phones rely on the network, it must be kept up for an extended time, so each switch that carries VoIP needs to be protected by an UPS.

3.18.14 Internal Communications

The internal communication system is comprised of several components ranging from servers to small end devices. In this design the VoIP is based on SIP, even thou the design is vendor independent, there are chareristics from different vendors in the design. The different vendors will be looked at in more detail in the sections that discusses the test beds for phase two.

3.18.14.1 IP-PBX

The heart of the internal communications is the IP-PBX. This is comparable to the PBX of a TDM system. One major difference is that SIP is peer to peer for the bearer traffic where TDMs traffic passes through the PBX. In this design the IP-PBX is used to register the end devices and maintain presence of them. When a call is placed the IP-PBX will take the extension and match it to the end device that has registered and pass the IP address back to the requesting end device so it

can setup the session with the other end device. See the different sections on SIP for a more detailed explanation of the SIP protocol and how the IP-PBX operates in SIP. The requirements of encrypted/non-encrypted switches vary by platform. In this design both PBXs support encryption and are redundant. The redundancy could be removed by removing the SBC, and having an encrypted and a non-encrypted PBX.

3.18.14.2 Media Gateways

The media gateways have two uses in this design. The first was already covered in external communications is the connection to the external environment. This is with analog and/or a T1 PRI telephone line for when the vessel is at the dock. The other use is connection to systems that are not packet based like the sound powered telephones, traditional announcing system or a radio transmitter. Not shown on the diagram are smaller ones that can be used to connect older technology end devices to the packet-based network when required. This could be an analog device that is not cost affective to upgrade to VoIP.

3.18.14.3 Session Border Control

The session boarder controller can be defined as a peering or an access edge application. In this design the SBC hardware handles the IPSec encoding/decoding so the individual servers in the IP-PBX do not have to process IPSec directly. This reduces the amount of processing that is done by the servers, where the SBC handles it in optimized hardware instead of software. The equipment that is after the SBC needs to be physically protected since the packets will not be secured in this design when they leave the SBC. This is a design decision that is not a requirement. It was added to show a possible method. Review of the security sections would add more details to why this was done. The bearing audio can be forced to pass through the SBC. The design has a redundant SBC with the each IP-PBX in each node.

3.18.14.4 Voice Recording

The voice recording is located on the non-encrypted of the SBC so the packets are not encrypted so it can collect and save the call sessions without dealing with the encrypted packets. As noted above this is only one-way to achieve this. Using this method the bearing audio packets are forced to pass through the SBC in both directions instead of passing peer-to-peer. This creates a funnel in each node that is a weak link in the network chain, but makes the recording of the calls more centralized.

3.18.14.5 Voicemail

The voicemail is contained with in the IP-PBX in this design. The storage of the voicemail will be handled on the network-attached storage (NAS) where polices can be setup to restrict the access to only the tools that allow access to the voicemail.

3.18.15 Announcing System

The announcing system in this diagram is showing two different ways. The first method is an IP based system and the second is a non-packet design that requires a media gateway to be connected to the IP network. Even thou there are packet-based designs, they don't appear to match the derived baseline with all the features. It is still worth investigating this method since it adds many improvements for reduction in wiring as well as supporting equipment. Being a distributed system its amplifiers are contained in each speaker, allowing for reduction in housing of large amplifiers. This design also makes the speakers smart and allows the ability to add new functionality by the

change of firmware in the speakers. The other feature is the ability to dynamically change the speakers MC groups and allow it to be used by multiple groups. The microphone stations that are presently used on some vessels do not have a match in COTS. There are several design concepts that can be investigated in the test lab that may be able to use the already developed technology and just repackage it.
The non-packet based system is the same as implemented on many vessels today and uses the media gateway to convert the packets to audio that is then pushed through the amplifiers to the speaker strings. The microphone stations would not change from the current design used today.

3.18.15.1 Pager Server

The packet based system uses the pager server that can be loaded onto any server or be supplied in an application server chassis. There are currently a few manufacturers of this device in an application server, but the features don't match the derived baseline. The other option is to develop one that matches the requirements of the derived baseline. The benefit of this type of solution is the "speaker strings" are dynamic in nature allowing for changes in how the speakers are allocated to the MC groups, and speakers can be changed or added to multiple strings with only software changes and no rewiring. This could allow a single speaker to be in all the MC groups at the same time.

3.18.15.2 Speakers

The packet-based speakers have several advantages over the current ones used with the speaker string model. The speakers are smart in several ways, allowing for them to be added to multiple MC groups at the same time. The priority can also be manipulated at the speaker or the page server. Because it contains a circuit board and amplifier circuit, new functionality can be designed into them: The addition of a relay can be used to turn on a strobe light to signal an announcement. The ability to add the normalization of volume to the speaker instead of having to use external microphones with a single unit in the rack controls the volume of the full speaker string. This could allow it to be added to any single speaker that requires it and not the entire speaker string.

3.18.15.3 Phone Intercom

The phone intercom is another area that the packet based announcing system can possible interface to. There are issues with the intercom on phones, but as that is resolved, they can be added as speakers to a pager server that follows the different SIP drafts and specification. This could result in the reduction of required speakers in rooms that have at least a single speaker phone.

3.18.16 Video

Video on the vessel is used for surveillance of different compartments. This stream is either watched real time or is recorded for future review. The stored video is also transmitted off the vessel through the external interface for DoD review. In this design we have divided it into four components, but depending on the vendor this will vary.

3.18.16.1 Cameras

The camera are all IP based. There are several different manufacturers of camera and many different features. The high-resolution camera gives you the ability to zoom and pan through the image, and still maintain a high level of resolution. In some situations the need for an analog camera may be required, a converter could be used to convert the video analog output of the camera to IP packets.

3.18.16.2 Video Processor

The video processor is a server that manages the cameras and the video streams. It allows for configuration of the camera as well as defining the rates of the video stream and where it will be stored. It also hosts the ability to monitor a stream live or view a stream that has already been stored.

3.18.16.3 Video Storage

The video storage can be with the video processor, separate or combined with the voice storage server. The purpose of this server is to have high capacity storage that has some form of NAS.

3.18.16.4 Video Review

Video review is a combination of several components that are vendor dependant. Depending on how the vendor is architected the video system will determine the individual parts and where they are located. This is a generic explanation of a system. The video processor has a SHTTP application server that is running on it that allow internet browsers to connect to a URL that is exposes exclusively for the purpose of video review. The Internet browser may be required to first download an application that will allow the images and navigation to be done within the browser. In many of these review systems you can stop, reverse and continue to watch multiple streams independently of each other at the same time. Several of them will let you zoom and pan and then watch that resulting view as the video streams.

3.18.17 End Devices

The end device section covers devices that the end user uses. They range from standard phones to the microphone/speaker that is located in the dive chamber of some vessels. None of them were found directly in the COTS offerings, but parts of COTS offerings may be able to be used to manufacture end devices that match the derived baseline. Because of the design decision in this diagram each end device will need to support IPSec, for security at the network layer. Other security options could be implemented that would not require that all end points support IPSec.

3.18.17.1 Non-tactical Phones

The non-tactical phones are located and used during non-combat situations. The largest qualities of them are administrative phones; some vessels have many of these types, where other vessels may have none of them. The concept is a COTS phone that is hardened to take the required shock and vibration. In most cases the feature sets range from single line to multiple line with a display and without a display.

3.18.17.2 Communication Terminals

The communication terminal that is used on several vessels has no COTS product that can replace it. This product is used in tactical locations, where the sailor needs to have the ability during combat situations to process multiple calls at the same time, listening to them all simultaneously. The present solution is sold by a few Navy integration companies, many of them are divisions of L-3 Communications. Because of its tactical nature these units will probably be dual homed to multiple edge switches for survivability. Dual homed may be also required to support the security needs depending on the security topology required.

3.18.17.3 Portable Handsets

The portable handsets in this design are a replacement to the WICOMM radios that are traditionally used on Navy vessels. They will connect to the VoIP network through WiFi access points that would be spread out throughout the vessel. There are a few cellular phones that are watertight today, but no WiFi phone has been produced and marketed that was found that could be submerged. The ability to manufacture this type of phone is possible. When the manufacturers see a requirement for it, with quantities to support the manufacture costs, some phones may support WiMAX that would be used on the support boats, and be processed through the WiMAX access point. Since this is an emerging technology, they are expecting WiMAX phones to be available in the next couple years in mass production.

3.18.17.4 Softphones

The softphone is a software phone that doesn't have its own casing, but resides in a computer. The softphone uses the computer's speaker and microphone (output/input
) for its ability to interact with the user. This could be used where there is a phone and a computer, and the two tasks can be combined. The softphone can also reside on a laptop or hand held computer and be connected to the network by the wireless network. The security is inherited from the computer device that the softphone is installed on. A softphone can be integrated into a sailor's workstation, to make a seamless application instead of having to flip between multiple applications. The designated approving authority will be required to approve the use of a softphone, before it can be used on a Navy network.

3.18.17.5 Dedicated Stations

The dedicated station is a phone that has a specialized use, and is then customized to fulfill that requirement. In many cases these devices do not appear to be phones and may or may not have a handset connected to it. In the conceptual design we have included only one that is an emergency phone. The design of the phone should be from a base SIP phone that is modular in design allowing only the functionality that is required be exposed to the end user to reduce confusion on what the dedicated station is for.

3.18.17.5.1Dive Trunk (not shown)

This is a very specialized design that does not appear to be a phone. In the diver chamber there is a high-pressure speaker and microphone, with a selection switch for the direction of the audio path. This ties back to a phone that allows the person outside the chamber to hold a conversation with the individual in the dive trunk. It also allows for a conference to be setup between multiple parties and the dive chamber.

3.18.17.5.2Emergency Station

The emergency station looks more like a phone subset, with the phone receiver. The box has a power, in use light, and an on/off hook button. It is meant for only taking calls and can't be used to dial out. In many cases the call can be picked from the phone, so it never goes off hook and is able to take other calls. The PBX can be configured to queue calls on the extension.

3.18.18 Summary

This packet-based design will be used to create the design for the test beds for the selected vendors. A single network infrastructure will be chosen that will support the bandwidth requirements as well as allow simulation of multiple IP-PBXs so testing of security can also be done.

4 Phase 2 Recommendations

4.1 Introduction

To prove the concepts and designs covered in this report, a testing phase is required before integrated voice, video and data is moved to a vessel for shipboard testing. This testing phase should be broken into two different tests beds. The first is a more open test to verify feasibility and prove out concepts. Another part of this first test is to verify the different methods of securing the network and the performance degradation created by each one. Then the methods are layered together to complete a secured environment with separation between data and voice packets. Since security should be added much like an onion, each layer will add security and may result in degradation in performance; tests need to be done with each layer added to understand the ramifications of each layer. The second test bed before being placed on a vessel will be done at a sanctioned vessel lab. In this test a single topology, IP-PBX manufacturer, network switch manufacturer, and methodology for security will be tested. The result of this test will determine if it is ready for shipboard testing. In discussions with SPAWAR, their concept is to roll it out starting at administrative phones and hybrid it into the rest of the telephony framework. There are benefits to this approach but we believe the evaluation should quickly move to an integrated voice, video, and data IP implementation. Our focus in the first test bed is to make sure that the design that is placed into the sanctioned vessel lab is ready to go the distance and be able to be moved onto a vessel with a minimal amount of modification. This is not to say that the manufacturers will not change or there will not be a technology refresh, but the concepts proposed and evaluation will allow the implementation of an integrated voice, video and data conceptual design.

4.1.1 Objectives

- **Feasibility of Topology**

Does the topology support the requirements for bandwidth, and resilience for shipboard use?

- **Feasibility of Wireless Telephones**

Does wireless telephone communications have expectable quality of service?
Does the addition of data or video packets affect the quality of voice on the same access point?
Does wireless telephony replace WIFCOM with added features?

- **Feasibility of COTS Phones**

Can COTS phones comply with the environmental requirements for the U.S. Navy?
Do the COTS phones support the features needed on a U.S. Navy vessel?
Do the IP-PBX manufacturers phone support more features then the third party COTS phones?

- **Feasibility of Proprietary End Devices**

Can proprietary end devices be developed on Open System designs to fulfill the requirements of Red/Black, security performance, and SIP features?

- **Feasibility of IP-Announcing**

Does the IP-Announcing solution from COTS manufacturers fulfill the requirements for shipboard use?

- **Evaluate Improved GUI for Tactical Terminal**

Can the use of new GUI controls improve the layout and usability of the communication terminal?

- **Feasibility of Softphones Integration Into Consoles**

Does the softphone expose the flexibility to be integrated into a console to replace a hard phone?

- **Feasibility of SIP**

Does SIP support the required features for shipboard use?

- **Feasibility of Quality of Service (QoS)**

Can configuration allow voice traffic to maintain quality of service when the network is loaded with lower priority packets?

- **Feasibility of Security**

Does security degrade the over all performance of the network to make VoIP unusable on board ship?

- **Layer 2 (IPSec)**

Does Layer 2 security provide improved performance and implementation over Layer 3 security?

- **Layer 3**

Does Layer 3 security provide improved performance and implementation over Layer 2 security?

- **Feasibility of Handling Red/Black Communications**

Can Red/Black communications be determined by the end device and display the level of security within the SIP protocol?
Can it be displayed in any COTS end device?

4.1.2 Assumptions

This phase's test bed is small in size and has three different IP-PBX manufacturers represented. There are assumptions made on the onset that will need to be maintained to complete this phase of testing:

- Network analysis will not be performed on the topology of the network. Even though it is promoted in the report. It is felt that the analysis performed showed that for this small test bed there is no bandwidth issue. Because the topology will be changing to accommodate different switch configurations and VLANS for security and isolation of the IP-PBXs, the analysis would have to be continuously redone with little return.
- Security of the network will be evaluated for performance degradation, not for how secure the network is. There are many references in this report and STIGs that defined the different security methods.
- Wireless network ability to handle multiple clients will be assumed to be what the manufacture specifies.
- Wireless network ability to handle metal compartments will be assumed to be what the manufacturer specifies.

4.1.3 Test Bed Components Descriptions

4.1.3.1 Topology

The research showed that an inner network core of a Partial or Full Mesh with the edge being a Star topology was a resilient and well-distributed solution (Refer to Figure 4-1). One edge switch that will be configured as a Star will be included to hang off several of the end devices. The other end devices will be connected to the core network. This will allow the testing of network resilience and self-healing as one of the two connections from the edge switch is disconnected from the core network. Network analysis was done in the infrastructure Appendix C and should be done in the next test bed before it is placed into a sanctioned vessel lab.

4.1.3.2 IP-PBXs

There are five vendors' offerings on the current proposed test bed design. In the final design this will be reduced to three offerings. One from each group: Proprietary vendor doing SIP, SIP native solution, and an Open Source will be selected. Each of the ones listed have demonstrated functionality and are preferred vendors. The decisions will come down to how the vendor will support the test bed with reduced costs in purchase, support and training.

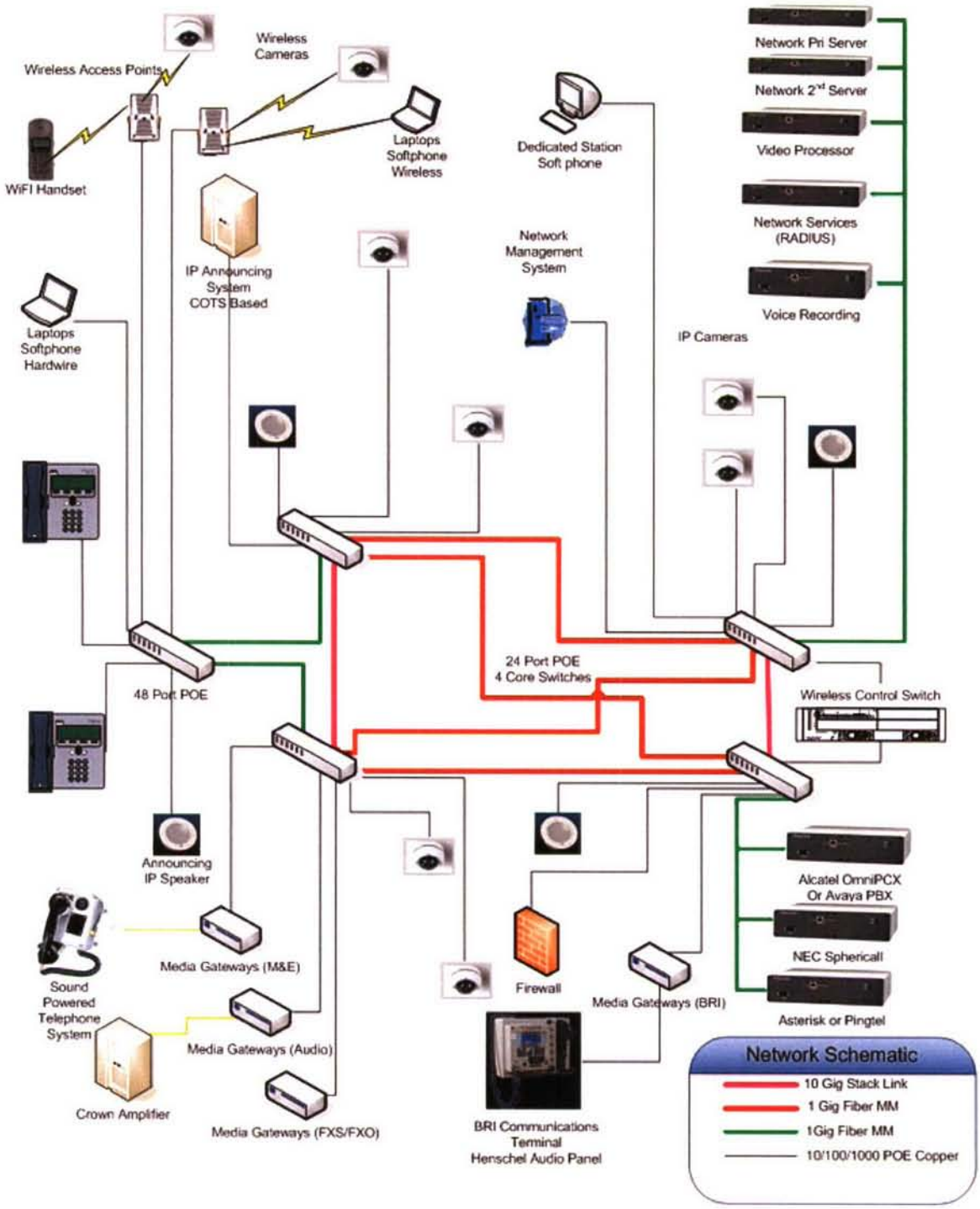


Figure 4-1. iACT Phase 2 Test Bed Design

4.1.3.3 Video

A complete video solution is shown on Figure 4-1. The purpose of having video is to emulate the streaming characteristics of the video, as well as the ability to separate it from the voice and data packets and to determine the degradation that will be caused. Two WiFi enabled cameras are included to see how the access points deal with video and voice packets passing through the access point. Two videophones will also be evaluated for functionality and interoperability with the different IP-PBXs.

4.1.3.4 Announcing

There will be two different announcing systems. The first will be a COTS IP-Announcing system. This will add multicast to the network traffic, as well as allow for separation using VLANs. The second method will be a traditional amplifier that will be connected through a media gateway. This will allow the test of a media gateway and determine how it will perform in this configuration. Again, an attempt to use VLANs and IPSec to see if this can be implemented with the media gateway will also be done.

4.1.3.5 Wireless

The implementation of the wireless will use the wireless controller to manage the individual access points. In this model the individual access points work and are seen by a wireless client as a single access point. Because of the controller, the installation of the wireless network is simplified, and no site review is required. The testing will involve quality of service for the wireless telephones and how they handle the hand off between multiple access points.

4.1.3.6 Supporting Servers

The VoIP servers require other network services that are on a network. These servers will supply these services. The servers may change as new requirements are generated and security is added to the network infrastructure. Two sets of standard services will be used so that one set is in the data network when the other set will supply the VoIP network with the same services. This is something that is recommended in several of the security papers from The Defense Information Systems Agency and The National Security Agency.

4.1.3.7 SIP Feasibility

The feasibility will be determined from the features that are stated in the SIP chapter of this report. The derived baselines will also be used to define the requirements for the feasibility tests. Each IP-PBX and end device (that relates to the IP-PBX) will be configured and tested. The initial tests will be done with a single IP-PBX and device, and then it will be redone with multiple end devices. The final tests will include multiple IP-PBXs where it makes sense to test between multiple PBXs.

4.1.3.8 VLANs

The configuration of the VLANs will be done in multiple stages to achieve different goals. First each IP-PBX will be configured, as required, in a single VLAN so testing for feasibility is not hindered by other IP-PBXs. As the testing proceeds VLANs will be used to separate different types of packets for security and performance. The final VLAN configuration will be designed around the Conceptual Packet Based Network that is represented in Section 5.29 Recommendations and Conceptual Design.

4.1.3.9 Security

Security will not be applied until the other initial testing is completed. It will be added in layers much like an onion. As each layer is added the degradation of the network will be measured from different statistics. The many papers referenced in this report cover how to do the security for DOD needs, but they do not touch on the issues of performance loss with the addition of different types of security. This is the area that will be focused on in the test bed.

4.1.4 Organization

The organization of the test bed will be finalized when the phase two proposal is finalized and a finite direction is defined. The first delivery of the phase two project is a Kickoff Meeting or Conference Call that will define the direction of the project. At that time the organization will be fitted to the requirements defined by that meeting. The description below is an overview of area to be covered to do a well-rounded review of VoIP for U.S. Navy vessels.

4.1.4.1 Define Components

Take the components in the test bed proposed design and get current quotes from the individual vendors. Training and support services will also need to be evaluated during this step. Individuals will be required to be trained on the major components so configuration can be done by internal engineering resources. Determine what will be purchased for phase two. The proposed design is larger than what the final design will be. The areas of reduction will be in the number of IP-PBXs; see the section on IP-PBX for more details on each one. The introduction of videowill produce load on the network allowing for the determination of what effect it has on the voice packets. This environment will allow for testing of a QoS configuration and packet separation with VLANS. The number of media gateways will be reduced to only the ones that have external devices to connect to that are part of this project. Ten and 50 Hertz navigational and wind data packets may also be added to the network traffic for the same reasons as the implementation of video traffic.

4.1.4.2 Purchase Components

After the selection process is completed, the individual components will be purchased from the vendors that quote the best prices to service level ratio with influence given to

small businesses. This process will be happening as internal engineering resources are being trained on the different components.

4.1.4.3 Setup All Components

The internal engineering resources that have been selected and trained will take the components and while working with the manufacturer or vendor install and test the individually components. This process will allow for the creation of the baseline configurations that the components can be returned to after each individual test.

4.1.4.4 Define Baseline

Before the systems are tested, a baseline configuration will be defined. This will allow for the different systems to be set back to a known state before each test or configuration change, so that a detailed configuration is always documented from a known state. There may be multiple baselines that are done as the system is configured. This will be determined, as required, but there will always be the initial baseline.

4.1.4.5 Evaluate Network Topology

The network evaluation will be in a couple different areas. The network management system will be used to determine how it can assist the engineering resources in the future tests. Depending on the manufacturer chosen, it may allow for control of the network switches, as well as IP-PBX and wireless network. The other part of the evaluation will be to review how the mesh network heals itself with different connections removed. This will not be an exhaustive evaluation, but will show how well spanning tree and other protocols handle separation and reconnection of network segments.

4.1.4.6 Evaluated IP-PBX SIP Features

Each individual IP-PBX will be evaluated for how it supports SIP natively. Manufacturers with proprietary protocol will also be evaluated and compared to the native SIP implementations.

4.1.4.7 Evaluate COTS Phones

The different COTS phones that are purchased will be physically examined for their ability to survive the environment that they would be exposed to on a U.S. Navy vessel. This examination will be done in a way so the phones will not be damaged and can be used for the other evaluations. Some of the phones will be used to determine if they can be repackaged into hardened cases that will allow them to pass the environmental challenges of being used on U.S. Navy vessels.

4.1.4.8 Evaluate GUI Controls

The creation of GUI will be done in the same form facture as the current tactical terminals. Usability will be evaluated with the different control layouts. This evaluation will only be skin deep, and no functionality will be under the buttons other than the switching between different screens. A touch screen will be fitted to the screen so the evaluation will involve the use of the touch screen for usability of the new layouts. Voice will be looked at as an alternative to the touch screen in a non-software research. A complete review of development of voice is larger then this test bed can support.

4.1.4.9 Evaluate IP-Announcing

There are a few COTS based IP-Announcing systems that are in the market place. The system will be evaluated against the announcing derived baseline, as well as the traffic created during an announcement. The use of VLANs will be used for isolation of the multicast packets.

4.1.4.10 Evaluate Media Gateways

Four different media gateways are shown on the test bed. As the design is completed and the interfacing is determined the number of gateways may vary. The interface to Sound Powered Telephones and announcing amplifiers are the two main ones that will need to be tested. This may require some external circuit to adapt the media gateway output to the external device. Then programming of the units will be done so calls can be placed.. The BRI gateway will be used to interface to an existing Audio Panel that L3 Henschel manufactures and will loan to the iACT program. This will demonstrate the connectivity of the other manufacturers of the communication terminals.

4.1.4.11 Evaluate Wireless network

The wireless network will be evaluated in several different ways. The wireless network will need to support both voice and data. The wireless network shall have the ability for the moving client to transverse access points without dropping connection, and the ability to continue a call during the hand off to other access point. When multiple clients connect to an access point will it hand off clients or degrade as the clients are added to the access point? The testing of the access points in metal rooms will not be part of this evaluation and the recommendations of the chosen vendor will need to be looked at for this functional area. If the manufacturer has done any testing, the results will be requested and included in the final report.

4.1.4.12 Evaluate Softphones

Some of the IP-PBX manufacturers have softphones, where others do not. Softphones will be evaluated if they support SIP natively. wxCommunicator will be evaluated. Minisip will not be evaluated as defined in the Open Source sections. Because it was not able to be compiled on Windows and could not place a call on Linux. .

4.1.4.13 Evaluate video

Video will be evaluated on its use of bandwidth, and how it affects other packets on the network. It can be setup several different ways; a wrong configuration can create performance and security issues. It also allows for the network evaluation in the area of configuring VLANs and priority tags that will allow for evaluation of performance of the other packets. The two videophones will be configured and evaluated on a single IP-PBX for ease of setup, quality of image and the bandwidth characteristics. A comparison of the quality of voice service to the quality of video service will be performed for the individual videophones, as well as for the effects it has on other phones on the network.

4.1.4.14 Add 50 and 10 Hz Data Simulators

The use of simulators for added multicast packet traffic will be used for the next several tasks. A Navigation Sensor System Interface (NAVSSI) Navigation Data simulator, which outputs data at a 50 Hz rate, will be added. There are two simulators, a forward and aft unit. A MORIAH Wind System (MWS) is a digital Wind Simulator which generates output at a 10 Hz rate. The last simulator will be the Ships Control Display System (SCDS) that also generates output data at a 10 Hz rate.

4.1.4.15 Add VLANs to the Network

Each group of components will be placed into different VLAN groups and Layer 3 filtering will be used to combine the groups as required. This will result in quality of service improvements, but may also result in degraded network performance due to Layer 3 switching delays.

4.1.4.16 Add IP Separation to the Network

Each group of components will be placed into different IP address groups and Layer 3 filtering will be used to combine the groups, as required. This will result in quality of service improvements, but may also result in degraded network performance due to Layer 3 switching delays.

4.1.4.17 Add Security Layer 2

Layer 2 security will involve the implementation of IPSec and VPN tunneling. This will allow for testing of the delays created. Evaluation of end devices and IP-PBX manufacturers support for this will also be reviewed. Depending on what is purchased and supported by IP-PBX vendors, a session border controller may be used in the network to do the translation before the IP-PBX and supporting servers. In this mode the end devices will be required to support the Layer 2 security.

4.1.4.18 Add Security Layer 3

Layer 3 security will involve the implementation of different security protocols at Layer 3 (ie., Transport Layer Security (TLS) and SRTP). This will allow for testing of the

delays created. Evaluation of end devices and IP-PBX manufacturers support for this will also be reviewed. Depending on what is purchased and supported by IP-PBX vendors, a session border controller may be used in the network to do the translation before the IP-PBX and supporting servers. In this mode the end devices will be required to support the Layer 3 security.

4.1.4.19 Evaluate Red/Black Communications

The evaluation of Red/Black communications will be a paper evaluation. Testing on the bed will be performed as well . The first evaluation will be can an end device be connected to two IP-PBXs at the same time? Then, can two calls be conferenced together from the independent switches? This may be a function of the end device more than the IP-PBXs. If time allows, evaluation of the concept of adding the security level to the SIP header will be looked at and tested in the softphone only.

4.1.4.20 Evaluate Security, Red/Black and Multiple IP-PBX

Now that each individual piece of security has been evaluated in a vacuum, start to put together the onion and determine the degradation of performance of the voice packets. This will be done in stages as each layer is added and a set group of features are evaluated. As stated above, this is for degradation of performance and not the ability to secure the network infrastructure from attack.

4.1.4.21 Evaluate Dual vs. Single Homed Device

This evaluation will work with the different network protocols to see if a VoIP device will maintain connection when a single leg of a dual homed device is lost. It will be evaluated if the configuration allows for the call to be maintained with minimal disruption of the voice path during loss and reconnection of a single leg.

4.1.4.22 Select Architecture for Next Test/ Create Baseline

Taking the results from the testing done on the test bed, the best-rounded components that would make up a complete system will be placed into an architecture that will be documented for the next round of testing in the next phase of iACT. This architecture will be presented in a diagram form that will allow for the first steps of creating a final design that would be taken to a sanctioned vessel test lab for evaluation. This design should then go to a place, such as Bell Labs network group, for analysis of the proposed architecture It can then be purchased with the known bandwidth capabilities for the move from the lab to an actual vessel test.

4.1.5 Measuring Methods

A measurement tool will allow the determination on how security and topology changes effect the network. Two areas will be looked at. Performance of the packets in the network would be related to bandwidth issues, as well as bottleneck issues. The next area of measurement is how the quality of voice is effected. Different methods of evaluation are being evaluated for the test bed. This can be done with a software measurement system or by having individuals listening and defining the quality.

4.1.6 Conclusion

The test bed will be dynamic in nature. It will change as results are turned back into the project, molding the project to fulfill the question of feasibility of VoIP on U.S. Navy vessels. The testing done here will allow a design that will compliment the need of the U.S. Navy in forming an IP packet network that will carry voice, data, and video into the testing on board a vessel. This project does not design end devices for the implementation. Testing of COTs products will be performed to determine if the end devices that are designed for the U.S. Navy on SIP will support the requirements that the U.S. Navy currently has. The testing will show where enhancement can be found in the new IP packet network.

This project will define the future direction of the U.S. Navy in the integration of voice, video and data for vessels of the future. This will show the feasibilities learned about implementing integration of voice, video and data, in the areas of IP-PBX, COTS products, Encryption methods, and network fault recovery.

This page intentionally left blank.

References

[1] iSTAT, In-Stat: VoIP Security: Preparing for the evolving threat, September 2006.

[2] The Internet Society, Network Working Group, "SIP: Session Initiation Protocol", Request For Comments 3261, June 2002. , http://www.ietf.org/rfc/rfc3261.txt, July 6, 2007.

[3] The Internet Society, Network Working Group, "Communications Resource Priority for the Session Initiation Protocol (SIP)", Request For Comments 4412, February 2006.

[4] The Internet Society, Network Working Group, "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events", Request For Comments 4411, February 2006.

[5] *Light Reading, VoIP Reliability, June 2004*
http://www.lightreading.com/document.asp?doc_id=53864&page_number=4.

[6] Recommended IP Telephony Architecture, National Security Agency's Systems and Network Attack Center (SNAC), http://www.nsa.gov/snac/voip/I332-009R-2006.pdf, September 12, 2007.

[7] Developed by DISA for the DOD, "IPT & VoIP STIG, V2R2 21 April 2006, Internet Protocol Telephony & Voice Over Internet Protocol, Security Technical Implementation Guide V2R2".

[8] Developed by DISA for the DOD, "Network Infrastructure, Security Technical Implementation Guide V6R4.

[9] Security Guidance for Deploying IP Telephony Systems, National Security Agency's Systems and Network Attack Center (SNAC), http://www.nsa.gov/snac/voip/I332-016R-2005.PDF, September 12, 2007.

[10] Das, K. P., Hubbart, J., and T. Rumland, "Intelligent Advanced Communications - Network Infrastructure," April 2, 2007.

[11] Recommendation H.323, International Telecommunications Union http://www.itu.int/rec/T-REC-H.323/e, July 16, 2007.

[12] Session Initiation Protocol - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Session_Initiation_Protocol, July 16, 2007.

[13] The Opportunity: Pervasive Computing - Indiana University
http://www.indiana.edu/~ovpit/ipcres/index_4.html, July 16, 2007.

[14] The Internet Society, Network Working Group, "SIP: Session Initiation Protocol", Request For Comments 2543, March 1999, (Obsolete). RFC 2543, http://www.ietf.org/rfc/rfc2543.txt, July 6, 2007.

[15] The Internet Society, Network Working Group, "Models for Multi Party Conferencing in SIP", Internet Draft draft-rosenberg-sip-conferencing-models-00, November 2000.

[16] The Internet Society, Network Working Group, "Basic Network Media Services with SIP", Request For Comments 4240, December 2005.

[17] The Internet Society, Network Working Group, "An Approach to Call Park/Retrieve Using SIP", Internet Draft draft-procter-sipping-call-park-extension-00, April; 2004.

[18] CyberData, Pager Server http://www.cyberdata.net/products/voip/voip-pagingserver.html, September 24, 2007.

[19] Raytheon, ARA-1, http://www.jps.com/page/view/213, September 24, 2007.

[20] K. S. Vallerio, L. Zhong, and N. K. Jhu, "Energy-Efficient Graphical User Interface Design".

[21] D. Kuhn, T. Walsh, and S. Fries, "Security Considerations for Voice Over IP Systems", Recommendations of the National Institute of Standards and Technology, Special Publication 800-58, January 2005.

[22] Dan York, CISSP "VoIP Security: How Secure is your IP Phone".

[23] http://iase.disa.mil/stigs/index.html, "Security Technical Implementation Guides (STIGS) and Supporting Documents" August 29, 2007.

[24] Developed by DISA for the DOD, "Enclave Security Technical Implementation Guide," Version 3, Release 2, July 28, 2005.

[25] Developed by DISA for the DOD, "Defense Switched Network Security Technical Implementation Guide," Version 2, Release 3, April 30, 2006.

[26] Developed by DISA for the DOD, "UNIX Security Technical Implementation Guide," Version 5, Release 1, March 28, 2006.

[27] D. Kuhn, T. Walsh, and S. Fries, "Security Considerations for Voice Over IP Systems", Recommendations of the National Institute of Standards and Technology, Special Publication 800-58, January 2005.

[28] Federal Information Processing Standards Publication, "Security Requirements for Cryptographic Modules", FIPS 140-2, May 25, 2001.

[29] International Standards Organization, "Information Technology–Security Techniques– Evaluation Criteria for IT Security, Part 1", ISO/IEC 15408-1, 2nd edition, October 10, 2005.

[30] Telcordia, "Generic Requirements for Network Element/Network System (NE/NS) Security", GR-815-CORE Issue 2, March 2002.

[31] Chairman of the Joint Chiefs of Staff Instruction, "Policy for Department of Defense Voice Networks", CJCSI 6215.01B, September 23, 2001.

[32] Chairman of the Joint Chiefs of Staff Instruction, "Information Assurance (IA) and Computer Network Defense (CND)", CJCSI 6510.01D, June 15, 2004.

[33] Chairman of the Joint Chiefs of Staff Instruction, "Defense Information System Network (DISN): Policy, Responsibilities and Processes," CJCSI 6211.02B, July 31, 2003.

[34] Ken Coar, "The open source definition," July 24, 2006, june 27, 2007. "http://www.opensource.org/docs/definition.php"

[35] Eric S. Raymond, "The Cathedral and the Bazaar" "http://www.free-soft.org/literature/papers/esr/cathedral-bazaar/" , September 25, 2007.

[36] Blane Warrene, "Navigating Open Source Licensing," March 9, 2005, June 27, 2007. "http://www.sitepoint.com/article/open-source-licensing"

[37] John Koenig, "Seven open source business strategies for competitive advantage," May 13, 2004, June 27, 2007 "http://www.itmanagersjournal.com/feature/314"

[38] LGS Innovations, LLC, "Intelligent Advanced Communications –VoIP Security Study", May 4, 2007.

[39] M. A. Padlipsky, "A Perspective on the ARPANET Reference Model," RFC 871, September 1982.

[40] International Organization for Standards/International Electrotechnical Commission, ISO/IEC 7498-1, 7498-2, 7498-3, and 7498-4, "Open Systems Interconnection: Basic Reference Model," available from www.iso.org .

[41] International Organization for Standards/International Electrotechnical Commission, ISO/IEC 14496-10, "Coding of audio-visual objects – Part 10: Advanced Video Coding," and 14496-10/FDAmd1, "Support for color spaces and aspect ratio definitions," available from www.iso.org.

[42] International Telecommunication Union, ITU-T Recommendation H.261, "Video codec for audiovisual services at p x 64 kbit/s", http://www.itu.int/rec/T-REC-H.261-199303-I/en .

[43]] International Telecommunication Union, ITU-T Recommendation H.263, "Video coding for low bit rate communication", http://www.itu.int/rec/T-REC-H.263-200501-I/en .

[44] International Telecommunication Union, ITU-T Recommendation H.264, "Advanced video coding for generic audiovisual services", http://www.itu.int/rec/T-REC-H.264-200503-I/en.

[45] International Telecommunication Union, ITU-T Recommendation H.264 (2005) Amendment 1 (06/06), "Support of additional color spaces and removal of the High 4:4:4 Profile," http://www.itu.int/rec/T-REC-H.264-200606-I!Amd1/en.

[46] International Telecommunication Union, ITU-T Recommendation G.711, "Pulse code modulation (PCM) of voice frequencies", http://www.itu.int/rec/T-REC-G.711/en .

[47] International Telecommunication Union, ITU-T Recommendation G.726, "40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)", http://www.itu.int/rec/T-REC-G.726/en.

[48] International Telecommunication Union, ITU-T Recommendation G.722, "7KHz audio-coding within 64 kbit/s", http://www.itu.int/rec/T-REC-G.722/en.

[49] International Telecommunication Union, ITU-T Recommendation G.722.1, "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss", http://www.itu.int/rec/T-REC-G.722.1/en .

[50] International Telecommunication Union, ITU-T Recommendation G.722.2, "Wideband coding of speech at around 16 kbit/s using Adaptive Multi-Rate Wideband (AMR-WB)," http://www.itu.int/rec/T-REC-G.722.2/en.

[51] International Telecommunication Union, ITU-T Recommendation G.728, "Coding of speech at 16 kbit/s using low-delay code excited linear prediction", http://www.itu.int/rec/T-REC-G.728/en .

[52] International Telecommunication Union, ITU-T Recommendation G.723.1, "Dual rate speech coder for multimedia communication transmitting at 5.3 and 6.3 kbit/s", http://www.itu.int/rec/T-REC-G.723.1-200605-P/en.

[53] International Telecommunication Union, ITU-T Recommendation G.729, "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)," (Status Pre-published), January 2007, http://www.itu.int/rec/T-REC-G.729/en.

[54] International Telecommunication Union, ITU-T Recommendations G.729 Annex A, "Reduced Complexity 8 kbit/s CS-ACELP speech codec", (Status- superseded), http://www.itu.int/rec/T-REC-G.729-199611-S!AnnA/en.

[55] International Telecommunication Union, ITU-T Recommendations G.729 Annex B, "A silence compression scheme for G.729 optimized for terminals conforming to Recommendation V.70", (Status- superseded), http://www.itu.int/rec/T-REC-G.729-199610-S!AnnB/en.

[56] International Telecommunication Union, ITU-T Recommendation G.729.1, "G.729.1 : G.729 based Embedded Variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729," (Status - In force), May 2006, http://www.itu.int/rec/T-REC-G.729.1/en

[57] Herlein, G., Morlat, S., Jean-Marc, J., Hardiman, R., and P. Kerr, "RTP Payload Format for the Speex Codec," draft-herlein-speex-rtp-profile, April 4, 2005.

[58] Andersen, S., Duric, A., Astrom, H., Hagen, R., Kleijn, W., and J. Linden, "Internet Low Bit Rate Codec (iLBC)," RFC 3951, December 2004.

[59] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation protocol (SIP) for asserted Identity within Trusted Networks", RFC 3325, November 2002.

[60] VoIPForo.com, http://www.en.voipforo.com/H323/H323_example.php September 25, 2007.

[61] VoIPForo.com, http://www.en.voipforo.com/SIP/SIP_example.php September 25, 2007.

[62] VoIPForo.com, http://www.en.voipforo.com/H323vsSIP.php September 25, 2007.

[63] Freshmeat.net : About, http://freshmeat.net/about/, July 6, 2007.

[64] Asterisk: The Open Source Telephony Platform | About, http://www.asterisk.or/about, July 2, 2007.

[65] Wiki CallWeaver, http://www.callweaver.org/wiki/CallWeaver, July 5, 2007.

[66] FreeSwitch – Communication Consolidation, http://www.freeswitch.org/, July 5, 2007.

[67] Comparing sipX with Asterisk – SIPfoundary sipx, The Open Source SIP PBX for linux – Calvia, http://sipx-wiki.calivia.com/index.php/Comparing_sipX_with_Asterisk, July 5, 2007.

[68] Yate – Main – Homepage, http://yate.null.ro/pmwiki/, July 5, 2007.

[69] Ekiga ~ Free Your Speech, http://www.ekiga.org, July 2, 2007.

[70] Kphone, http://sourceforge.net/projects/kphone/, July 2, 2007.

[71] Minisip, http://www.minisip.org, July 2, 2007.

[72] Zap! – The Mozilla SIP Client, http://www.croczilla.com/zap, July 5, 2007.

[73] The eXtended oslibrary, http://savannah.nongnu.org/projects/exosip, July 2, 2007.

[74] Jain-sip, Java API for SIP Signalling, https://jain-sip.dev.java.net/, July 5, 2007.

[75] OpenSourceSIP: OSS – Open Source SIP, http://www.opensourcesip.org:8080/jiveforums/opensipstack.jsp, July 2, 2007.

[76] The GNU oSIP Library, http://www.gnu.org/software/osip, July 2, 2007.

[77] Vox Gratia FAQ, http://www.voxgratia.org/docs/faq.html, July 5, 2007.

[78] PJSIP – Open Source Embedded SIP Stack and Media Stack, July 5, 2007.

[79] Resip Overview – Resiprocate, http://www.resiprocate.org/Resip_Overview, July 5, 2007.

[80] Sofia-SIP Library, http://sofia-sip.sourceforge.net/, July 3, 2007.

[81] OpenSourceSIP: OSS – Open Source SIP, http://www.opensourcesip.org:8080/jiveforums/downloads.jsp, July 2, 2007.

[82] Mobicents.org – The Open Source VoIP Middleware Platform, http://www.mobicents.org, July 2, 2007.

[83] Home – Open Source SIP Server, http://www.openser.org/, July 5, 2007.

[84] About Sip Express Router, http://www.iptel.org/ser/, July 5, 2007.

[85] J.G. Andrews, A. Ghosh, and R. Muhamed, *Fundamentals of WiMAX: Understanding Broadband Wireless Networking*, Prentice Hall, 2007.

[86] G.J. Foschini and M.J. Gans, "On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas," *Wireless Personal Communications, Kluwer Academic Publishers*, Vol. 6, No. 3, pp 311–335, March 1998.

[87] A. Goldsmith, S. Ali Jafar, H. Jindal, and S. Vishwanath, "Fundamental Capacity of MIMO Channels," *IEEE Journal on Selected Areas in Communication*, Vol. 21, No, 5, pp 684–702, June 2003.

[88] J. Winters, "Understanding MIMO," http://www.wirelessnetdesignline.com/showArticle.jhtml?articleID=161500272.

[89] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.

[90] N. Borisov, I. Goldberg, D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," *7th Annual international Conference on Mobile Computing and Networking–MobiCom '01*, pp 180-189, 2001.

[91] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," *Selected Areas in Cryptography: 8th Annual International Workshop*, pp 1–24, August 2001.

[92] J.R. Walker, "Unsafe at any key size; an analysis of the WEP encapsulation," IEEE Document 802.11-00/362, October 2000.

[93] J.R. Rao, P. Rohatgi, H. Scherzer and S. Tinguely, "Partitioning Attacks: Or how to Rapidly Clone Some GSM Cards," *IEEE Symposium on Security and Privacy*, May 2002.

[94] D. Wagner, I. Goldberg, M. Briceno, "GSM Cloning," April 1998, http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.

[95] E. Barkan, E. Biham, and B. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," *Advances in Cryptology–CRYPTO 2003*, vol. 2729/2003, pp. 600–616, October 2003.

[96] C. Wingert and M. Naidu, "CDMA 1xRTT Security Overview," Qualcomm Whitepaper, August 2002.

[97] News Release, "Sprint Nextel Announces 4G Wireless Broadband Initiative with Intel, Motorola and Samsung," August 8, 2006.

[98] K. S. Vallerio, L. Zhong, and N. K. Jhu, "Energy-Efficient Graphical User Interface Design".

[99] J. Polk, "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events RFC 4411".

[100] H. Schultzrinne, and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP) RFC 4412.

[101] Cisco Systems "Understanding, Preventing and Defending Against Layer 2 Attacks Session SEC-2002 http://www.cisco.com/networkers/nw04/presos/docs/SEC-2002.pdf.

[102] F. Robles. "The VoIP Dilemma", SANS Institute, http://www.sans.org/rr/whitepapers/voip/1452.php.

[103] VQIPSA, "VoIP Security and Privacy Threat Taxonomy".

[104] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120–126, February 1978.

[105] Federal Information Processing Standards Publication, "Digital Signature Standard (DSS)," FIPS 186, May 19, 1994.

[106] R. Rivest, "The MD5 Message-Digest Algorithm," IETF RFC 1321, April 1992.

[107] Federal Information Processing Standards Publication, "Secure Hash Standard," FIPS 180-2, April 17, 1995.

[108] Federal Information Processing Standards Publication, "Data Encryption Standard (DES)," FIPS 46-3, October 25, 1999.

[109] Federal Information Processing Standards Publication, "Advanced Encryption Standard (AES)," FIPS 197, November 26, 2001.

[110] International Telecommunication Union (ITU-T) X.509 "Information technology – Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks," August 2005 (revised).

[111] DoD Instruction, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," DoDI 8520.2, April 1, 2004.

[112] DoD, "X.509 Certificate Policy for the United States Department of Defense," Version 9.0, February 9, 2005.

[113] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," IETF RFC 2246, January 1999.

[114] E. Rescorla, "HTTP Over TLS," IETF RFC 2818, May 2000.

[115] R. Housley, W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC 2459, January 1999.

[116] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," IETF RFC 3711, March 2004.

[117] M. Euchner, "HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY)," IETF RFC 4650, September 2006.

[118] J. Arkko, E. Carrara, F. Lindholm, M. Naslund and K. Norrman, "MIKEY: Multimedia Internet KEYing," IETF RFC 3830, August 2004.

[119] S. Kent, K. Seo, "Security Architecture for the Internet Protocol," IETF RFC 4301, December 2005.

[120] S. Kent, "IP Authentication Header," IETF RFC 4302, December 2005.

[121] S. Kent, "IP Encapsulating Security Payload (ESP)," IETF RFC 4303, December 2005.

[122] J. Schiller, "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)," IETF RFC 4307, December 2005.

[123] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," IETF RFC 4306, December 2005.

[124] H. Orman, "The OAKLEY Key Determination Protocol," IETF RFC 2412, November 1998.

[125] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. 22, No. 6, pp. 644–654, November 1976.

[126] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," IETF RFC 2409, November 1998.

[127] F. Andreasen, M. Baugher and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams," IETF RFC 4568, July 2006.

[128] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Ipv6 Network Architecture Protection," draft-vandevelde-v6ops-nap-01, January 24, 2005.

[129] W. Eddy, "Comparison of IPv4 andIPv6 Header Overhead," draft-eddy-ipv6-overhead-00, May 8, 2006.

[130] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," IETF RFC 3711, March 2004.

[131] F. Andreasen, M. Baugher and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams," IETF RFC 4568, July 2006.

[132] J. Arkko, E. Carrara, F. Lindholm, M. Naslund and K. Norrman, "MIKEY: Multimedia Internet KEYing," IETF RFC 3830, August 2004.

[133] DISA, "Department of Defense Voice Networks Generic Switching Center Requirements (GSCR)," September 8, 2003 (Errata Change 2, December 14, 2006).